Hyper-connectivity: Intricacies of national and international cyber securities.

Maurice Dawson

Submitted in partial fulfillment of the award of Doctor of Philosophy by Prior Output at London Metropolitan University

PART I

August 2017

Statement of Originality

This narrative commentary along with the research outputs listed in Appendix A has been submitted in partial fulfillment of the requirements for the award of Ph.D. by Prior Output at London Metropolitan University. Both the commentary and the outputs are the sole work of the candidate. No part of this submission, including outputs, narrative, footnotes, and appendices, has previously been submitted for award elsewhere.

Table of Contents

List of Figures

List of Tables

Abstract

This thesis examined the three core themes: the role of education in cyber security, the role of technology in cyber security, and the role of policy in cyber security, the areas in which the papers are published. The associated works are published in referred journals, peer reviewed book chapters, and conference proceedings. Research can be found in the following outlets: 1. Security Solutions for Hyperconnectivity and the Internet of Things; 2. Developing Next-Generation Countermeasures for Homeland Security Threat Prevention; 3. New Threats and Countermeasures in Digital Crime and Cyber Terrorism; 4. International Journal of Business Continuity and Risk Management; 5. Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning; 6. Information Security in Diverse Computing Environments; 7. Technology, Innovation, and Enterprise Transformation; 8. Journal of Information Systems Technology and Planning; 9. Encyclopedia of Information Science and Technology. The shortcomings and gaps in cyber security research is the research focus on hyperconnectivity of people and technology to include the policies that provide the standards for security hardened systems. Prior research on cyber and homeland security reviewed the three core themes separately rather than jointly. This study examined the research gaps within cyber security as it relates to core themes in an effort to develop stronger policies, education programs, and hardened technologies for cyber security use. This work illustrates how cyber security can be broken into these three core areas and used together to address issues such as developing training environments for teaching real cyber security events. It will further show the correlations between technologies and policies for system Certification & Accreditation (C&A). Finally, it will offer insights on how cyber security can be used to maintain security for international and national security. The overall results of the study provide guidance on how to create an ubiquitous learning

(U-Learning) environment to teach cyber security concepts, craft polices that affect secure computing, and examines the effects on national and international security. The overall research has been improving the role of cyber security in education, technology, and policy.

Acknowledgments

This submission would not have been possible without the guidance of my supervisor, Professor Hassan Kazemian. I am also thankful for the support from my colleagues at the University of Missouri - St. Louis. I am indebted to the students whom I have had the pleasure of teaching at the Clarence M. Mitchell, Jr. School of Engineering at Morgan State University, University of the Gambia, the Faculty of Computational Mathematics and Informatics at South Ural State University, College of Business Administration and Public Affairs at Alabama A&M University, the University of Tennessee Space Institute, and the College of Business Administration at the University of Missouri - St. Louis.

The opportunities to serve as a Visiting Professor at University of the Gambia, University of Nairobi, Pontificia Universidad Catolica Madre y Maestra, and the Polytechnic University of Puerto Rico has allowed for me to gain insights on the use of technology in other regions of the world. For this I am thankful for these opportunities to serve as a visiting faculty member in the named universities. I would like to thank the Fulbright Program, United States Department of State Bureau of Educational and Cultural Affairs, Winrock International, and the International Studies and Programs (ISP) Department at the University of Missouri - St. Louis for providing funding to carry out projects technology focused projects.

Lastly, submission is dedicated to the memory of Juanita Dawson. I also dedicate this submission to my children Amayah Claire Dawson, Maurice Elijah Dawson, and Kingsley Jediah Dawson.

1.0 Thesis Overview

1.1 Introduction

This research brings together three key elements in cyber security which are education, policy, and technologies. The education review provides insight on innovative ways to teach cyber security coursework to include discussing the accrediting bodies for programs related to Information Technologies (IT) or computer science. Further reviewed are the policies, tools, and techniques that can be brought forward in cyber security education. Concepts such as simulation, U-Learning, virtualization, and engineering standards are explored. The policy section reviews multiple directives, standards, mandates, laws, and best practices. These include policies from the Department of Defense (DoD), National Institute of Standards and Technology (NIST), United States (U.S.) military, and more. These policies provide the baseline for further guidance and direction for organizations to set their own policies. The technologies portion of the literature review brings in data about emerging technologies such as those that include Internet enabled devices. Mobile phones, Operating Systems (OS), software, and other devices are reviewed as they relate to cyber security.

1.2 Research Problem

This study focused on increasing the understanding on how to address cyber security in a holistic nature that can be replicated in multiple countries for ensuring national and international security. The research question states: What is a framework that provides the intricacies of national and international cyber securities?

1.3 Motivations

The motivation behind this research is the global need for countries to address growing concerns for Information Systems (IS). As newer devices strive for Internet connectivity, and the use of the web increases we become part of a hyperconnected society. Thus, it is essential to understand how to address these new threats and how society needs to be shaped in order to mitigate any risk, and recover securely from a cyber attack.

1.4 Contribution to Knowledge

The research provided in the literature needed to create a customized framework development that includes education, policy, and technology. Figure 1.1 displays the Mission Framework that was created by reviewing the education, policy, and technology of that specific entity. The specific entity can be a country, organization, or group of institutions.

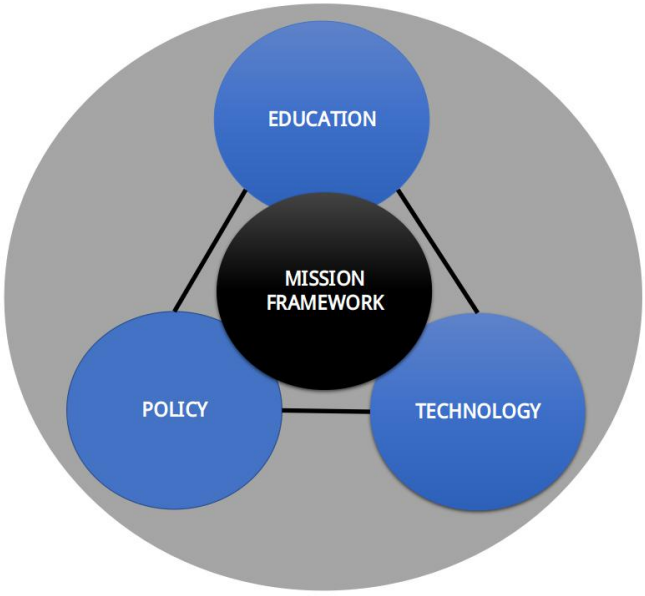


Figure 1.1: Mission Framework

1.5 Overview of Ph.D. Thesis

This thesis covered three themes which are broken down into separate chapters. The first of these chapters covered establishing cyber security education programs. The next chapter covered the role of policy in cyber security, and the final chapter covered the role of technology in cyber security.

2.0 Establishing Cyber Security Educational Programs

2.1 Introduction

Understanding how cyber security is effective in education is essential when building a rigorous program to meet the demands to be secure, and also participate in an offensive manner if that is the organization's mission. These can range from university education to professional certification to meet the workforce requirement of a government organization. Understanding the requirements for the core technology program such as regional, national, or program specific accreditation is a method to ensure there are identified benchmarks that are being met. Institutions need to develop, train, update, and retire curriculum to meet the needs of the workforce. This chapter provides guidelines, practices, and methods for developing programs.

Every university technology related program developed has its own accreditation standards that drive the program development ranging from systems engineering to computer science. The Accreditation Board for Engineering and Technology (ABET), Inc., is a non-governmental organization that accredits computer science, engineering, and engineering technology degree programs. Most of the accredited programs are in the U.S.; however, there are international schools that have this accreditation as well. Over 3,000 programs are accredited in more than 20

countries. ABET is a federation of 32 societies such as the National Society of Professional Engineers (NSPE), Institute of Electrical and Electronic Engineers (IEEE), International Council of Systems Engineering (INCOSE), and more.

ABET provides a good standard that institutions can use to measure their program and strive to build for compliance. Also, this accrediting body can be used as a measurement criteria for international programs collaborating. Institutions can jointly develop their program using the ABET engineering criteria as a baseline. When it comes to the ABET professional skills it is essential that they are not only taught appropriately but accessible (Shuman, Besterfield-Sacre, & McGourty, 2005). This will allow for a continued measurement to occur between institutions internationally. ABET has Mutual Recognition Agreements (MRA) which are also known as accords. The current MRAs are the following: the bilateral agreement between Engineers Canada and ABET for engineering programs, the multilateral Washington Accord for engineering programs, the multilateral Seoul Accord for computing programs, the multilateral Sydney Accord for bachelor degree level engineering technology programs, and the multilateral Dublin Accord for associate degree level engineering technician programs (Phillips, Peterson, & Abrele, 2000). MRAs have even been viewed in North America as being beneficial in shaping educational policies (Sá & Gaviria, 2011). MRAs are one of the policy instruments employed in global and regional trade agreements to facility the mobility of skilled labor (Sá & Gaviria, 2011). In 1997 American Society for Engineering Education (ASSE) and IEEE launched the International Conference on Engineering Education (ICEE) to focus on global issues in engineering accreditation (Tovar, & Castro, 2007).

When discussing STEM programs, it is essential to discuss those with a focus on cyber security. The National Security Agency (NSA) and Department of Homeland Security (DHS) have addressed harmonized security education by creating the Centers for Academic Excellence (CAE). As of 2016, only 8 states do not have CAEs within them. Both Washington, D.C. and Puerto Rico have at least one CAE. This number of accredited programs does not include the ongoing re-accreditation effort to gain Cyber Defense (CD) designation. Of those states and territories, the state with the most CAEs is Texas with 16 total institutions that have accreditation. The number of states with only one institution that boasts a CAE is 13. Approximately 25 states have 3 institutions that meet the CAE criteria. One can visit the NSA CAE page to gain details into the number of CAEs per state, territory, institutional focus on cyber defense education at the 4 year or 2 year, and cyber research. In total, there are 162 CAEs out of 4,495 total institutions according to the U.S. Census (Department of Education, 2014). This number represents only 3.6% institutions that hold this accreditation.

As of 2016 there is no such global standard for cyber security education accreditation as the majority of countries that have standards set in place are developed nations such as the U.S., U.K., Canada, and Australia. The NSA only accredits institutions that are within the U.S. The National Initiative on Cyber Security Education (NICE) Framework has three main goals which are the following: raise the level of awareness in the nation about risks in cyber space, prepare individuals for entering the cyber security workforce, and promote competitiveness in the current cyber security workforce (Shoemaker, Kohnke, & Sigler, 2016). However, in South Africa there has been emerging research looking at what developed nations have done for developing cyber security education (Kortjan, 2013). This could be party in a response to released Wikileak Cables

regarding the state of cyber security in this nation. The International Federation for Information Processing (IFIP) Technical Committee (TC11) on Information Security and Privacy Protection in Processing Systems host an international conference to address these matters; however, the IFIP created the International Professional Practice Partnership (IPS) to standardize IS and Information Technology (IT). IFIP has a long history dating to the 90s demonstrating the assistance of sharing IT goals and the continued need for building IT education (Marshall, & Ruohonen, 1998). Other factors are that a standard for the NSA and DHS means that these organizations would need the ability to look into the detail of foreign programs. Since the Intelligence Community (IC) are the ones that are developing these standards with the guidance of experts then it is best that this knowledge remains in the states and territories. Thus, the need for detailed global standards becomes an issue as you have federal agencies providing what is required for them to have the program recognized. These university programs have become a method to align institutions closer to what is needed by the various IC members to be successful in cyber warfare, and defend critical infrastructure.

2.2 Technology and Knowledge Sharing

The use of technology in cyber security programs is vital in bridging partnerships. Technology costs can be an issue because developing countries may have extremely small budgets due to lack of investment or low exchange rate of national currency. A method of performing this internationally at a low cost to all institutions can occur with Open Source Software (OSS), and cloud computing. For working with developing institutions who do not have access to major research databases, then Open Access (OA) is a research model to be implemented for sharing research information.

OSS is software that provides the source code and allows developers to modify or enhance (Dawson & Al Saeed, 2012). OSS also provides faculty members the ability to dissect source code and prepare students for low-level software development. OSS could enhance the STEM environment by infusing multiple applications that can be developed, analyzed, and used as part of the curriculum (Dawson, Wright, & Onyegbula, 2015). Thus Linux provides the ability for students to perform low level code analysis. Table 2.1: Linux Distributions and Uses, provides a list of Linux distributions and associated uses.

Table 2.1: Linux Distributions and Uses

Linux Distributions	**Description and Potential Use**	**Packet Management System**
Ubuntu	One of the most popular Linux OSs developed to be a complete OS that can be an easily replacement for other comparable OSs.	Debian-based
Edubuntu	OS targeted for grades k-12. Contained in the OS are tons of software applications that are useful to those who are education majors.	Debian-based
Damn Small Linux	This OS is designed as a small OS to be utilized on older hardware. This OS is great for institutions that have old computers and want to revitalize them for use. OS is also great for VMs as DSL requires a low amount of memory	Knoppix-based
BackTrack	OS based on Ubuntu for digital forensics and penetration testing. Great tool for students majoring in technology fields. As cyber security is becoming a hot topic around the world, this tool provides students the ability to learn from over thirty software applications that aid in penetration testing and more.	Debian-based
Kali Linux	OS based BackTrack that is a continuation of the popular penetration testing distribution.	Debian-based
Red Hat Enterprise Linux	This OS serves as the standard for many enterprise data centers. OS was developed by Red Hat and targeted for commercial use. Red Hat has a policy against making nonfree software available for the system through supplementary distribution channels. This is	RPM-based

	different and why this OS is listed as an exception in terms of OSS.	
Fedora	This OS is supported by the Fedora Project and sponsored by Red Hat. This OS provides a great resource for learning Red Hat Enterprise Language (RHEL). As there are thousands of jobs requiring expertise specifically with Red Hat, this OS is a great tool to prepare students for employment in IT. Fedora has over six Fedora Spins such as Design-suite, Scientific-KDE, Robotics, Electronic-lab, Games, and more.	RPM-based
CentOS	This OS derived entirely from RHEL. The source code is developed from Red Hat which allows a student to learn RHEL with a small number of differences. CentOS can be used for teaching IT students on how to setup, administer, and secure a server.	RPM-based
SUSE Linux	OS is of German origin with most of its development in Europe. Novell purchased the SUSE brand and trademarks.	Debian-based
Xubuntu	Xubuntu is based upon Ubuntu; however, it uses the light weight Xfce desktop environment.	Debian-based
Ubuntu Studio	This OS is derived from Ubuntu. This OS is developed specifically for multimedia production such as audio, video, and graphics. Departments for multimedia could use this OS for multimedia instruction and the development of projects. Since many of the tools for multimedia production are expensive this alleviates large license costs for institutions.	Debian-based
Lubuntu	OS is based on Ubuntu and uses the LXDE desktop environment. It replaces Ubuntu's Unity shell and GNOME desktop.	Debian-based
Chromium OS	An open source light weight OS that is targeted for netbooks and mobile devices.	Portage-based

2.3 Simulation

It is important to develop training environments that mimic the real world so that students have the ability to practice learned skills. Simulation allows for the imitation of a real world scenario or systems. This can be accomplished using software technology such as virtual worlds. Simulation can come in the form of training, education, video games, modeling, low fidelity prototypes, and usability. Simulation can use learning objects and incorporate other modern day technologies such as Google Glass for increasing teaching effectiveness. Additionally, accreditation bodies require such environments to replicate hands on experience that would be gained from industry experience such as apprenticeships. Thus having simulations allows for this requirement to be met, and improve the overall experience of the learner.

2.3 Ubiquitious Learning

U-Learning, supported by the revolutionary and abundant digital resources, is viewed as an effective learning approach for situating students in real-life and relevant learning environments that supports and promotes a variety of learning needs. U-Learning involves applying ubiquitous technologies in the enhancement of education strategies and models. Embedded Internet-based devices that we use in our daily life can present a supportive environment for U-Learning. The rise in Internet availability and accessibility has truly made a significant number of learning resources and options available to today's students at all levels of education. U-Learning has the unique power of providing educational resources in a manner that is flexible, calm, and seamless due to its

pervasive and persistent model (Martinez-Maldonado, Clayphan, Muñoz-Cristóbal, Prieto, Rodríguez-Triana, & Kay, 2013). U-Learning aims at removing educational and learning physical barriers by utilizing the advancements in technology. The ubiquitous learning has become more than a technology phenomenon and a prominent vision that strives to revolutionize the educational landscape and present technology-driven educational settings, because it thrives on the concept and idea of making a variety of educational and learning assets available to students, creates new and varied learning environments, customizes learning, and enables the realization of a series of training activities from anywhere, anytime, and from any device (Durán, Álvarez & Únzaga, 2014).

Ubiquitous and pervasive learning environments offer students unique possibilities for team work and collaboration both face-to-face and remotely (Neto, deSouza, & Gomes, 2016). These environments include an array of modern and innovative technologies at different stages of adoption: interactive whiteboards are already available in many classrooms; interactive tabletops are just starting to be introduced in schools (Kharrufa et al, 2013), and handheld devices are already used by students and teachers in the form of smart-phones or tablets.

2.4 U-Learning Space and Design

Many studies in the past have investigated the effectiveness of deploying different learning and teaching styles with different U-Learning environments to determine which strategy produces the best learning outcomes for students with different learning needs. It is important to note that when developing a u-Learning space, the developer must take into consideration the outcome of the existing learning theories regarding best practices, such as a structured relationship between

information and learners' understanding in educational settings (Jones & Jo, 2004; Sung, 2009). This helps to prevent learning being isolated from a meaningful context. For example, if a student understands why and how something happens rather than just being told that it is true, then the information is more relevant and, therefore, is more meaningful to the student. The rationale for this action is how the pedagogical information is included; and why is the inclusion of interactive learning allowing students to create knowledge from what they perceive (Ogata & Yano, 2012).

2.5 Ubiquitous Computing

As computers become ubiquitous, they capture our attention and daily activity, which allows them to infiltrate into the background. Ubiquitous computing, however, includes computing devices such as smartphones, tablets, cameras, and other digital gadgets. Integrating ubiquitous computing into ubiquitous learning promotes the interaction between students and their digital gadgets to become connected with the manifold digital embedded devices and/or services (Möller, Haas, & Vakilzadian, 2013). Therefore, in a ubiquitous learning settings or environment, students have the unique ability of exploring the ubiquitous space built and powered by ubiquitous and mobile technology to interact with the various embedded digital devices and/or services. Thus, ubiquitous learning has the potential to create a sustainable and persistent learning and education environment that is barrier free and adapts to varying student learning needs.

Students have the advantage and ability of deciding which learning approache best fits their learning needs and they are able to customize the environment to best fit their specifying situation (Martinez-Maldonado & Kay, 2013). In the U-Learning space, sharing information and knowledge between learners and mobile devices becomes a reality and contributes to creating a learning

environment where learners can access, share, and distribute knowledge anytime and anywhere and therefore we become a more powerful society by connecting people, ideas, and knowledge. With U-Learning, we are able to create an available and accessible learning community utilizing mobile technology that makes learning attainable, traceable, and identifiable (Möller, Haas, & Vakilzadian, 2013).

2.6 Learning Objects

Learning objects allow for educational content to be broken down into smaller pieces that can be reused in various learning environments (Boss & Krauss, 2007). Learning objects are grounded in the object oriented paradigm of computer science (Wiley, 2000). These are digital resources uniquely identified and metatagged that can be used to support learning. Provided is a new and innovative method to reuse technologies in the learning environment. Thus learning objects (LSTC, 2000a) leads other candidates for the next generation of instructional design.

The IEEE Learning Technology Standards Committee (LTSC) System Interoperability in Education and Training has a couple of research projects actively working on an augmented reality learning experience model. This new standard will include technologies such as wearables (LSTC, 2000b). In virtual worlds these objects can be given a 3 Dimensional (3-D) representation which allows users to interact with these objects. Also, behavioral tasks and indicators can be observed with 3-D learning objects (Vincenti, 2010).

2.7 Enhancing The Stem Environment

When discussing teaching tools one must consider all the OSS applications that can be used to improve Science, Technology, Engineering, and Mathematics (STEM) fields such as systems engineering (Dawson, Al Saeed, Wright, & Onyegbula, 2015). OSS provides the ability to create many technical items at a low cost and view source code of the software application (Dawson & Al Saeed, 2012). It is essential to take advantage of these tools and applications as many institutions of learning are having budget problems. These items allow for any institution to be competitive in instruction regardless of location. When thinking about U-Learning the virtual environment is key in the marketplace for low fidelity prototyping.

2.8 Virtualization

In terms of virtualization there are tools available to create a virtual version of a system. In terms of educational resources this provides a method for institutions to train on Virtual Machines (VMs). This allows a university to teach students complex techniques to computer science, engineering IT students such as networking, software assurance, secure programming, system administration, and Information Assurance (IA). There are multiple types of virtualization such as hardware, desktop, memory, storage, data, and network. For institutions that would like the opportunity to provide a cloud like environment, tools such as Oracle Virtual Box and VMware Player provide that ability; however, it should be noted that new Linux distributions running that require GNOME 3 will have issues running on older hardware. With older hardware as a constraint, there are bare minimal Linux distributions such as Puppy Linux and Damn Small Linux (DSL). VMs provide the ability for a student to experiment with hundreds of OSs without installing or uninstalling the base OS. As faculty members, we have used VMware software as well as Oracle Virtual Box as effective tools to host Linux as well as Windows operating systems; the results have been impressive in that

students were able to better grasp the theories and principles presented in class because they had the opportunity to tinker with all the inner workings of those OSs. This approach also helped researchers save invaluable time and resources that would have otherwise been needed for installing and un-installing all those OSs.

Additionally, this allows for the creation of baseline OS images for classes. For example, an engineering course would have an OS created with all the software, case studies, and labs preloaded. This baseline OS for software engineering would have development tools, static code analysis tools, debugging tools, case studies, eBooks, links to online course management tool, etc. This would allow an institution to have an image ready for every class to ensure consistency, and that the students have all required tools needed. In the case of a more technical course such as software engineering, the students would have a baseline OS image with all the programming software, the Integrated Development Environment (IDE), quality testing tools, and labs preloaded. In considering virtual environments, the image can include the necessary installation software or preloaded software to immediately start work in the U-Learning environment.

An example is that a U.S. based researcher can create an image with all the tools and associated source code loaded on a prebuilt OS. The U.S. researcher can export these items to a foreign counterpart via a VDI so that the incoming party can perform research on the same image. Another example: there is a class in two different countries; however, all students must use the same tools. A downloadable VDI provides all students the same tools and installed software to work on.

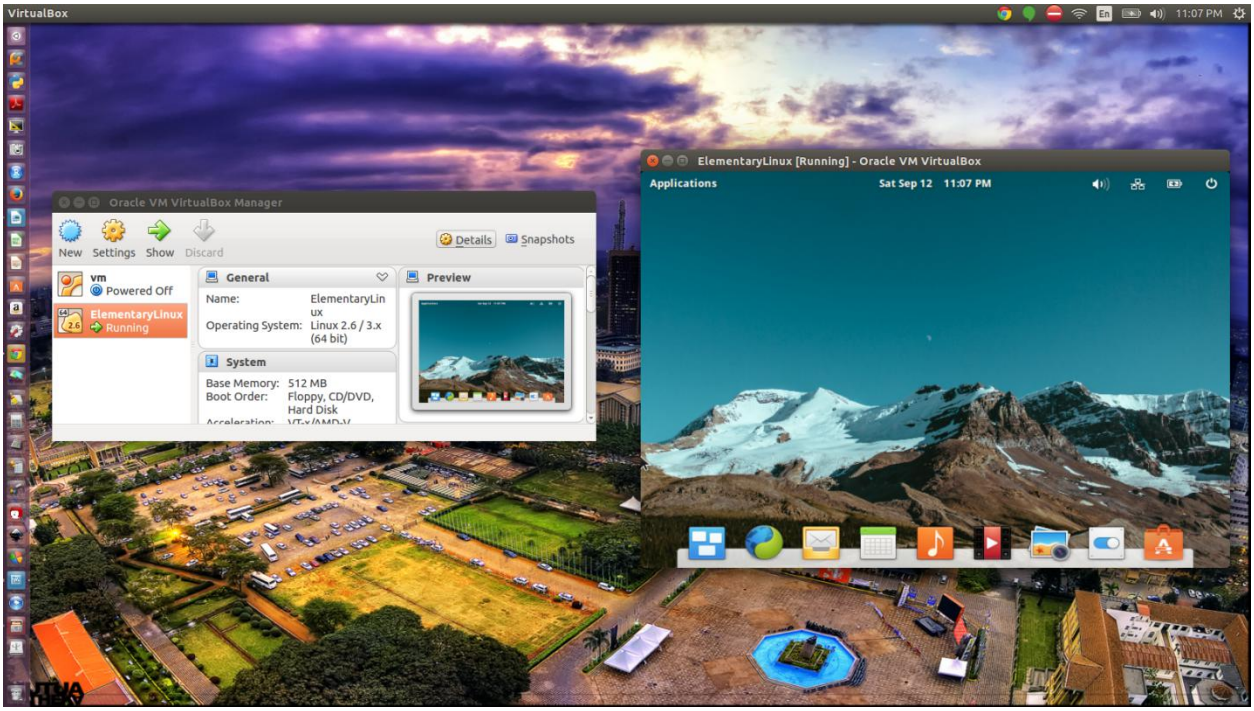


Figure 2.1: Oracle VirtualBox Running on Ubuntu Desktop

2.9 Software Engineering Standards

With the development of programs, it is important to understand current standards and their applicability to engineering. This allows professors to develop environments according to standards that are being used in industry. Learners get early exposure to these standards that they will be using upon graduation. All the items below in Table 2.2: List of IEEE Software Standards can be applied to a virtual project to limit the virtual environment for development. These software standards can be used as conditions or requirements that must be met while developing the projects. If a project is a secure web server then the professor states that upon delivery of this project the following artifacts need to be delivered with project. During a group project IEEE Std 1028-2008 can be stated as a requirement for all group reviews and code walk throughs.

Table 2.2: List of IEEE Software Standards

IEEE Standard	**Name of Standard**	**Additional Info & Citation**
IEEE Standard Glossary of Software Engineering Terminology	IEEE Standard Glossary of Software Engineering Terminology	A glossary that contains the vocabulary for the software engineering domain (IEEE Standards Coordinating Committee, 1990)
IEEE Std 730-2002	IEEE Standard for Software Quality Assurance Plans	This particular standard specifies the format and content of Software Quality Assurance plans (Lee et al, 2005).
IEEE Std 830-1998	IEEE Recommended Practice for Software Requirements Specifications	This document recommends the content and characteristics of a Software Requirements Specification (IEEE Computer Society, 1998).
IEEE Std 1028-2008	IEEE Standard for Software Reviews	This standard defines five types of software reviews and procedures for their execution. The five review types include management reviews, technical reviews, inspections, walk-throughs, and audits (Westfall,

		2008).
IEEE Std 1062-1998	IEEE Recommended Practice for Software Acquisition	This document recommends a set of useful practices that can be selected and applied during software acquisition (IEEE Standards Association, 1998).
IEEE Std 1074-2006	IEEE Standard for Developing Software Life Cycle Processes	This standard describes an approach for the definition of software life cycle processes (Hawker, 2009).
IEEE Std 1220-2005 (ISO/IEC 26702)	IEEE Standard for the Application and Management of the Systems Engineering Process	This standard is listed in a literature survey on international standards for systems requirements engineering (Scheider & Berenbach, 2013).
IEEE Std 1233-1998	IEEE Guide for Developing System Requirements Specifications	This standard provides guidance on the development of a System Requirements Specification, covering the identification, organization, presentation, and modification of requirements (Moore, 1998). It also provides guidance on the characteristics and qualities of

		requirements such as objective or threshold requirements specification.
IEEE Std 1362-1998 (Reaffirmed 2007)	IEEE Guide for Information Technology-- System Definition-- Concept of Operations (ConOps) Document	This document provides guidance on the format and content of a ConOps document, describing characteristics of a proposed system from the users' viewpoint.
IEEE Std 132-1998	IEEE Guide-- Adoption of PMI Standard-- A Guide to the Project Management Body of Knowledge	The third edition of the PMBOK is recognized as an international standard which is the IEEE Std 132-1998 (Ahlemann et al, 2009).
IEEE Std 1517-1999	IEEE Standard for Information Technology— Software Life Cycle Processes— Reuse Processes	The standard that provides life cycle processes for reuse of software (Moore, 1998).
ISO 9001:2000	Quality Management Systems-- Requirements	This standard has been debated upon in relation to the impact of quality management (Martinez-Costa, 2009).
EEE/EIA 12207-2008	Systems and Software Engineering - Software Life Cycle Processes	An international standard to establish common framework for software life cycle processes. This is applicable to

		software products and the acquisition of systems.
IEEE/EIA 12207.1-1996	Industry Implementation of International Standard ISO/IEC 12207:1995, Standard for Information Technology-- Software Life Cycle Processes--Life Cycle Data	It is essential to know the basic relation between primary parties in the form of something that is binding. In this contract the requirements will be specified as well the life cycle process model which will be used.
ISO/IEC 90003	Software and Systems Engineering-- Guidelines for the Application of ISO 9001:2000 to Computer Software	This standard provides guidance for organizations in the application of ISO 9001:2000 to the acquisition, supply, development, operation and maintenance of computer software.

The education review provides insight on innovative ways to teach cyber security coursework to include discussing the accrediting bodies for programs related to Information Technologies (IT) or computer science. Further reviewed are the policies, tools, and techniques that can be brought forward in cyber security education. Concepts such as simulation, U-Learning, virtualization, and engineering standards are explored. The policy section reviews multiple directives, standards, mandates, laws, and best practices. These include policies from the DoD, NIST, United States military, and more. These policies provide the baseline for further guidance and direction for

organizations setting their own rules. The technologies portion brings in data about emerging technologies such as those that include Internet enabled devices. Mobile phones, OSs, software, and other devices are reviewed as they relate to cyber security.

2.10 Academic Contribution

Figure 2.1 shows the Education portion of Mission Framework developed by conducting research. This portion of the framework looks at K-12, university, professional certification, executive education, and training. Each of these methods of education relies upon independent accrediting bodies. These accrediting bodies provide standards, education, and training. For example, the American National Standards Institute (ANSI), and the ISO 17024:2012 are to be used as the standard for professional certifications. This allows an entity to set minimum standards for the selection or the development of education and training for cyber security.

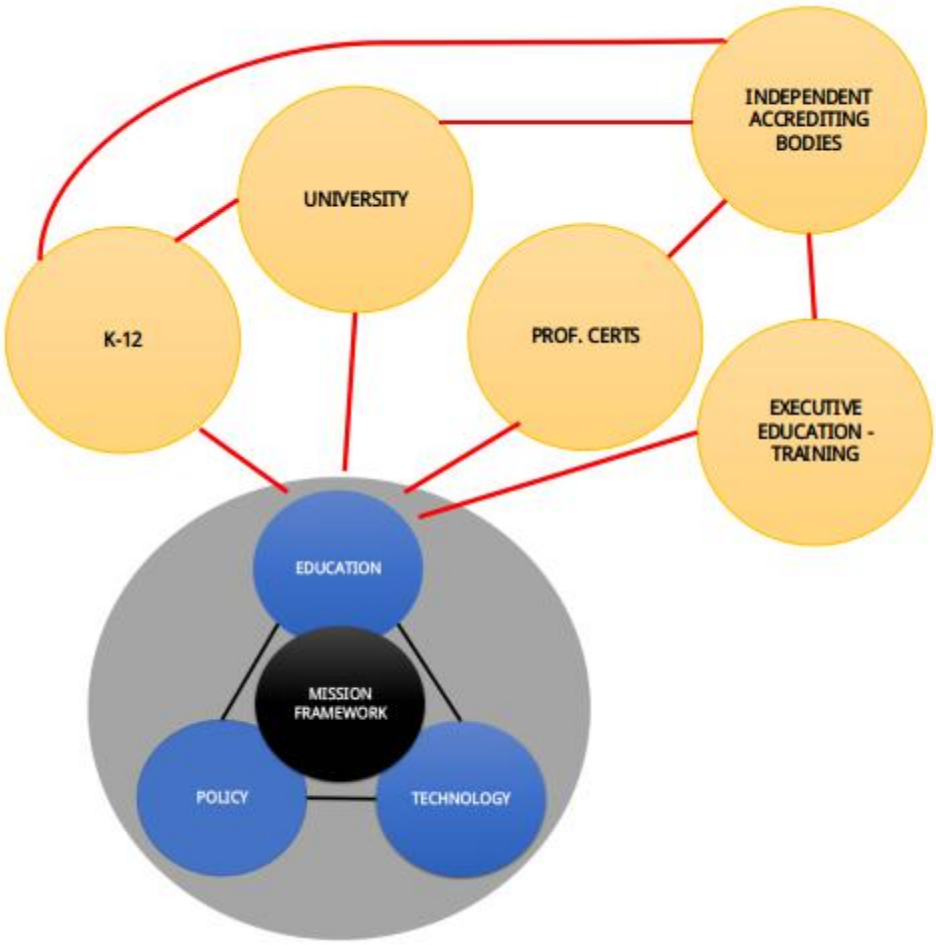


Figure 2.2: Mission Framework – Education

3.0 Cyber Security Policies, Laws, Directives, and Mandates

3.1 Laws and Policies to Combat Terrorism

The events of 9/11 not only changed policies within the U.S., but also changed the policies of other countries regarding how they treat and combat terrorism. The United Nations (U.N.) altered Article 51 of the U.N. charter. This article allows members of the U.N. to take necessary measures

to protect themselves against an armed attack to ensure international peace and security. The United Kingdom (U.K.) enacted the Prevention of Terrorism Act 2005 and the Counter-Terrorism Act 2008 which was issued by Parliament. The first act was created to detain individuals who were suspected in acts of terrorism. This act was intended to replace the Anti-terrorism, Crime and Security Act 2001 as it was deemed unlawful. These acts seem to mirror those created in the U.S. to monitor potential terrorists. The U.K. also shared their information with the U.S. for coordinating individuals that may be of risk.

In the U.S., the methods for national security were enhanced to ensure no threats occur on U.S. soil. These changes include enhanced security in all ports of entry. The signing of the Homeland Security Act of 2002 (HS Act) (Public Law 07-296) created an organization that received funding and lots of resources for monitoring the security posture of this country. Additional changes include enhanced monitoring of citizens and residents within the country to prevent terrorist activities by the mention of keywords, e.g. bomb, terrorism, explosive, or Al Qaeda.

The USA Patriot Act was signed into law by President George W. Bush in 2001 after September 11, 2001 (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This act was created in response to the event of 9/11 and provided government agencies increased abilities. These increased abilities provided the government rights to search various communications such as email, telephone records, medical records, and more of those who were thought to be perpetrators of terrorist acts (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This allowed law enforcement to have the upper hand in being proactive to stopping potential acts against U.S. soil. In the 2011 year, President Obama signed an extension on the USA Patriot Act. This act has received criticism from the public

due to the potential to be misused or abused by those in power. This act has allowed government agencies to intrude on constitutional rights. The Protecting Cyberspace as a National Asset Act of 2010 was an act that also amends Title 11 of the Homeland Security Act of 2002. This act enhanced security and resiliency of the cyber and communication infrastructure within the U.S. This act is important as the President declared that any cyber aggression would be considered an act of war. This is also important as Estonia's entire digital infrastructure was taken down by hackers who supported the former Soviet rule. This type of attack could be damaging to the infrastructure in the U.S.- causing loss of power for days or more which could result in death.

Israel is a country with some of the most stringent policies towards national and international security. This nation requires all citizens to serve in the military and includes multiple checkpoints throughout the country to ensure security. Israel has utilized stringent checks in airports long before 9/11; however, now they have implemented additional measures to ensure the nation's security as they are surrounded by countries that have tried to invade before. Israel has also deployed more Unmanned Air Vehicles (UAVs), and Unmanned Ground Vehicles (UGVs) to patrol the border in the event a threat to the border occurs.

The Protecting Cyberspace as a National Asset Act of 2010 was an act that also amends Title 11 of the Homeland Security Act of 2002. This act enhanced security and resiliency of the cyber and communication infrastructure within the U.S. This act is important as the President declared that any cyber aggression would be considered an act of war. This is also important as Estonia's entire digital infrastructure was taken down by hackers who supported the former Soviet rule. This type of attack could be damaging to the infrastructure in the U.S., causing loss of power for days or

more which could result in death. In an area, such as the Huntsville Metro, there could be multiple nuclear facility meltdowns, loss of lSR capabilities, and loss of communication to the war fighter that the US is supporting.

Additional changes from this act include the ability to carry out a research and development program to improve cyber security infrastructure. At the moment, all government organizations must comply with the Federal Information Security Management Act (FlSMA) of 2002. This act has shown many holes within the U.S. cyber security infrastructure, including in those organizations that are leads. This act provides DHS the ability to carry out the duties described in the Protecting Cyberspace as a National Asset Act of 2010.

3.2 Stuxnet Worm

During the fall of 20 l 0 many headlines declared that Stuxnet was the game-changer in terms of cyber warfare (Denning, 2012). This malicious worm was complex and designed to target only a specific system. This worm had the ability to detect location, system type, and more. And this worm only attacked the system if it met specific parameters that were designed in the code. Stuxnet tampered directly with software in a programmable logic controller (PLC) that controlled the centrifuges at Natanz. This tampering ultimately caused a disruption in the Iranian nuclear program.

3.3 America's Homeland Security Preparing for Cyber Warfare

The DHS is concerned with cyber-attacks on infrastructure such as supervisory control and data acquisition (SCADA) systems. SCADA systems are the systems that autonomously monitor and adjust switching among other processes within critical infrastructures such as nuclear plants, and power grids. DHS is worried about these systems as they are unmanned frequently and remotely accessed. As they are remotely accessed, this could allow anyone to take control of assets to critical infrastructure remotely. There have been increasing mandates and directives to ensure any system deployed meets stringent requirements. As the Stuxnet worm has become a reality, future attacks could be malicious code directly targeting specific locations of critical infrastructure.

3.4 DIACAP for Systems Level Development & Deployment

The Department of Defense Information Assurance Certification & Accreditation Process (DIACAP) is the process that the DoD utilizes to ensure that risk management is applied to Automated Information Systems (AIS). DIACAP is the standard process that all services utilize to ensure that all DoD systems maintain IA posture throughout the system's life cycle. DIACAP is the replacement of the Department of Defense Information Technology Security Certification & Accreditation Process (DITSCAP). Figure 3.1: DIACAP Stages (Department of Defense 2007) displays the process which includes five key steps (Department of Defense, 2007). The first step is to initiate and plan the IA C&A process. The second step is to implement and validate the assigned IA controls. The third step is to make the certification determination and accreditation decision. The fourth step is to maintain authorization to operate and conduct reviews. The final step is to decommission the system.

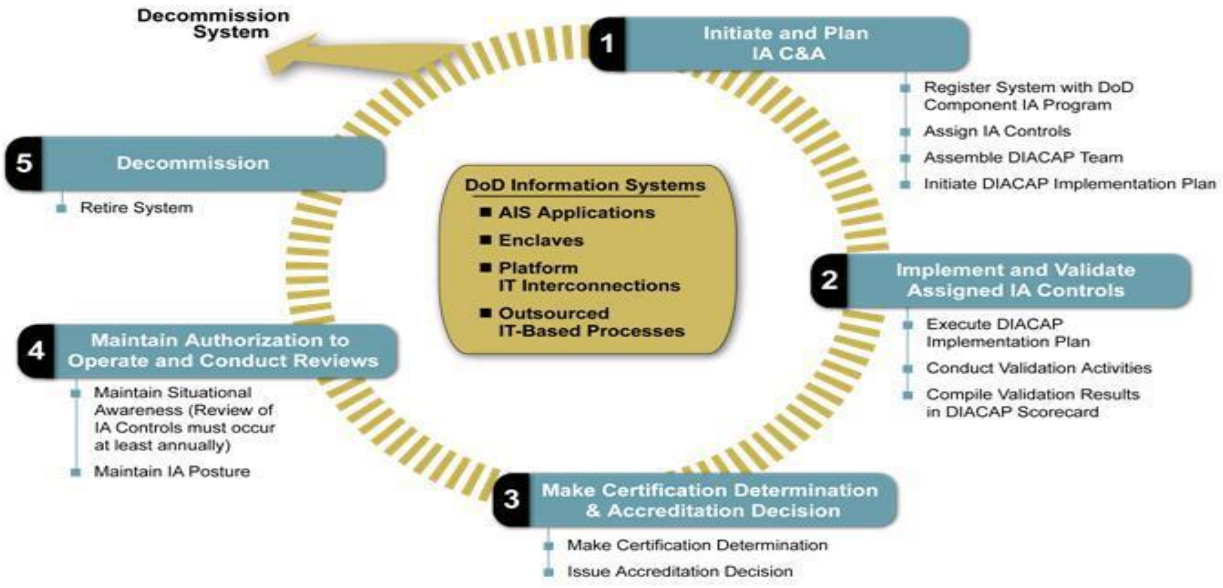


Figure 3.1: DIACAP Stages (Department of Defense 2007)

The DIACAP process incorporates multiple artifacts to capture system data, network connections, data classification, and more.

- Plan of Actions & Milestones (POA&M). See Appendix E
- DIACAP Scorecard. See Appendix F.
- Systems Identification Plan (SIP). See Appendix G.
- DIACAP Implementation Plan (DIP). See Appendix H.

3.5 Common Criteria Certification Process for Technology Products

The Common Criteria (CC), an internationally approved set of security standards, provides a clear and reliable evaluation of the security capabilities of IT products (CCEVS, 2008). By providing an independent assessment of a product's ability to meet security standards, the CC gives customers more confidence in the security of products and leads to more informed decisions (CCEVS, 2008).

Security-conscious customers, such as the U.S. Federal Government, are increasingly requiring CC certification as a determining factor in purchasing decisions (CCEVS, 2008). Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings. The international scope of the CC, currently adopted by fourteen nations, allows users from other countries to purchase IT products with the same level of confidence, since certification is recognized across all complying nations. Evaluating a product with respect to security requires identification of the customer's security needs and an assessment of the capabilities of the product. The CC aids customers in both these processes through two key components: protection profiles and evaluation assurance levels (CCEVS, 2008).

The CC is the process that replaced the Orange Book. The CC has Evaluated Assurance Levels (EAL) 1 through 7 (Troy, 1999) as displayed in Figure 3.2: Common Criteria EAL Levels. EAL products 1 through 4 may be used and certified in any of the participating countries, but EAL 5 through 7 must be certified by the country's national security agency. For example, United States' national agency is the National Security Agency and United Kingdom's national agency is the Communication Electronics Security Group (CESG). By all accounts, the NSA's Orange Book program, in which the NSA forced vendors through prolonged product testing at Ft. Meade, MD., was a dismal failure. The government's failure to buy Orange-Book-tested products, which were often out of date after years of testing, was a blow to vendors that invested huge sums in the Orange Book Evaluations.

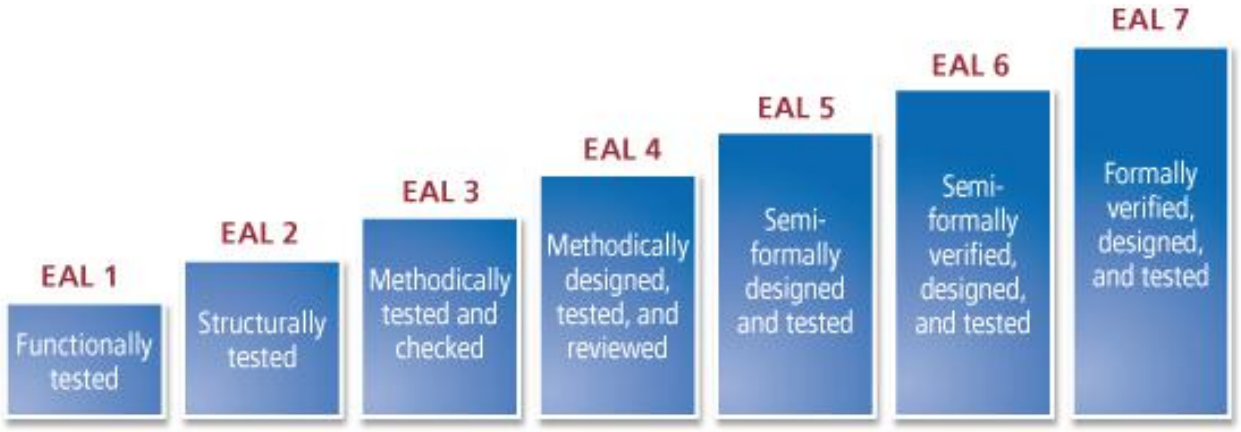


Figure 3.2: Common Criteria EAL Levels

A Protection Profile (PP) defines a standard set of security requirements for a specific type of product, e.g. OSs, databases, firewalls, etc. (CCEVS, 2008). These profiles form the basis for the CC evaluation. By listing required security features for product families, the Common Criteria allows products to state conformity to a relevant PP. During CC evaluation, the product is tested against a specific PP, providing reliable verification of the security capabilities of the product. Since technology enabled products can be linked to specific protection profiles, customers can compile a list of critical security features by examining the details of a relevant PP. In addition, since the CC certification verifies that a product meets the requirements of a PP, customers can rapidly assess the product's ability to meet their security needs, and compare the security capabilities of any validated products.

A Security Target (ST) contains the IT security objectives and requirements of a specific identified TOE and defines the functional and assurance measures offered by that TOE to meet stated requirements. Unlike the PP, ST is more product-specific as it is used as a basis for agreement between developers, evaluators and sometimes consumers on the TOE security properties. ST

answers the question of "What do I have to offer?" from the point of view of product vendors, developers, or integrators. The content of an ST is an extension to that of a PP. The additional information is TOE Summary Specification (TSS) and statement of conformance to one PP or more. The TSS describes TOE security functions and its assurance measures. Any PP conformance claims must be complete as no partial conformant is permitted for CC evaluation. The underlying requirement is such that an ST has a clear, complete and unambiguous content. This is to ensure ST evaluation can be carried out.

TOE is an enabled technology product or system, which is subject to an evaluation (CCEVS, 2008). TOE includes all material like documentation and administrator guides that are delivered with it. TOE might not be a full system or product as it could be referring to only a particular module or part of it. The security features in a TOE would be corresponding to the requirements as claimed in a ST in the case of a vendor. It could also be addressing the requirements put forth by a PP from a consumer point of view.

3.6 US Navy IA Processes

The Department of the Navy begins its IA program with a definition of roles and responsibilities within the organization. Daryl Edgar's article depicts the need for a security compliance program (Dodson-Edgars, 2002). His survey found, "Companies with a compliance program have the opportunity to greatly reduce penalties for violations of almost all federal statutes. Companies are expected to exercise due diligence and be innovative in designing and implementing their own security programs" (Dodson-Edgars, 2002). This practice is vital to successful network defense and avoids liability for failing to exercise due care and diligence in protecting Navy assets and

national security. All DoN entities must adhere to Secretary of the Navy (SECNAV) instruction 5239.1, the Navy IA Program Guideline. Under this instruction, the DoN Chief Information Office (CIO) is responsible for developing and disseminating the DoN's IA strategy and policy and coordinating IA within the DoN and with other DoD commands. The DoN CIO is also in charge of evaluating Navy enterprise and system level IA posture and performance and reporting to the SECNAV on the effectiveness of DoN IA activities. Under SECNAV 5239.1, the DoN CIO reports directly to the Secretary of the Navy and has the responsibility to ensure compliance with applicable IA requirements including the development and maintenance of a department-wide IA Program.

The Navy Deputy Chief Information Officer for Policy and Integration is designated as the Department of the Navy Senior Information Assurance Officer (DoN Senior IA Officer). The DoN CIO focuses its efforts on the development of IA policy, strategy, tools, and oversight (Department of the Navy, 2005). The DoN Information Management vision is to provide a joint environment that delivers information dominance to the United States Navy (USN). The DoN CIO achieves that vision by ensuring that all personnel have the full and best use of world-leading information technology assets at their disposal. The DoD IA Strategic Plan is a joint, enterprise-wide effort to identify the major goals and objectives of DoN-wide IA efforts. The major goals of the DoN IA strategy are:

- Protect Information (Department of the Navy, 2005)
- Defend Systems and Networks (Department of the Navy, 2005)

- Provide Integrated IA Situational Awareness/IA Command and Control(Department of the Navy, 2005)
- Transform and Enable IA Capabilities (Department of the Navy, 2005)
- Create an IA-empowered Workforce (Department of the Navy, 2005)

The DoN achieves its IA goals by deploying a team-centric approach. Each team is responsible for specific tasks to ensure IA practices are enforced and implemented correctly. The following outlines and describes each DoN IA team member:

- DoN Deputy CIOs. This team implements and enforces policies, standards, and procedures to ensure the DoN complies with DoD statutes, regulations, and directives.
- Chief of Naval Operations. The Chief of Naval Operations (CNO) is responsible for developing and implementing IA-related programs and controls, ensuring that IA is incorporated throughout the system development lifecycle, assigning designated approval authorities (DAAs), providing enterprise-wide vulnerability mitigation solutions, and providing an incident reporting.
- Designated Approving Authority (DAA). The DAA is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. DAAs accredit IT system security postures throughout the system development lifecycle, and in accordance with risk-management principles.
- Certification Authority. The Certification Authority (CA) is the official responsible for performing the comprehensive evaluation of the technical and non-technical security features and safeguards of an IT system, application, or network. This evaluation is made

in support of the accreditation process to establish the extent that a particular design and implementation meets information assurance requirements. The CA is responsible for managing the certification process.

- Program Manager. The Program Manager (PM) is the person who owns the business process and controls the funding for the system. The PM is the individual with overall responsibility for the system/application.
- IA Manager. The Information Assurance Manager (IAM) is responsible for the IA program within a command, site, system, or enclave. The IAM is accountable to the local IA command authority and DAA for ensuring the security of an IT system, and that it is approved, operated, and maintained throughout its life cycle in accordance with IT system security certification and accreditation documentation.
- IA Officers. IA Officers (IAOs) are responsible to an IAM for ensuring the appropriate operational IA posture is maintained for a command, organization, site, system, or enclave. IAOs assist in creating accreditation packages. They implement and enforce system level IA controls in accordance with program and policy guidance.

3.7 Risk Assessment Process

Once the roles and responsibilities are defined, the next step is identifying the risks involved in DoN operations. The DoN deploys an effective risk management program to address the need for identifying potential problems before they occur so that the organization can plan risk-handling activities and invoke them as needed across the life of the product or project. The DoN's risk management program is a continuous, forward-looking process that is an important part of military and technical management processes. The DoN risk program is implemented into three sectors:

1. Risk Management Methodology
2. Identifying and Analyzing Risks
3. Handling Identified Risks

To begin identifying and analyzing risks, the DoN executes risk assessments of enterprise systems. Stephen Cobb, contributing author of the *Computer Security Handbook, 4th Edition*, defines risk assessments as: "Evaluation involving imagining what could go wrong, then estimating the chances of it actually happening. For each of the possible problems, the question of probability needs to be considered. In this way, the problems and their potential costs can be prioritized and an appropriate plan of action developed" (Cobb, 2006). Executing risk assessments is a vital task to the successful implementation of an effective information assurance program. The United States Government Accountability Office (USGAO) highlights this importance during an analysis of information security practices of leading organizations: "Risk assessments provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected" (Brock, 1999). The DoN's risk assessment methodology helps identify, prioritize, mitigate, and manage risk.

3.8 Risk Assessment Methodology

The Navy risk assessment methodology was developed by the Space and Naval Warfare Systems Center (SPAWAR). SPAWAR is the inventing, acquisition, and development command for new

technology within the DoN (SPAWAR, 2002). The purpose of the SPAWAR risk management document is to define a process that will assist project managers to develop and execute a plan to identify project risks as early as possible and to periodically reassess and manage those risks (Cobb, 2007).

The first step in the DoN risk assessment process is identifying risks. A peer group is created for assessing risks against criticality. This group includes developer staff, government oversight, certification authority, and validation personnel. The peer group reviews system concept of operations, system requirements, schedules, and cost documents. After review, this team identifies the risks associated with developing, administering, deploying, and maintaining the system being evaluated. With the risks of the program identified, the next step is a deeper analysis of the identified risks. Peer group members amplify risks by noting the Program Area, Affected Phases, Risk Area, and Control source. The peer group reaches a consensus on each risk and assigns a team member responsibility for the mitigation of risk (Cobb, 2007).

The next process step is to prioritize the risks into Probability, Impact, and Impact Time Frames for each risk. This task is accomplished with use of SPAWAR's risk allocation software, Risk Radar. A Risk Radar report is generated which is analyzed and adjusted by the system's risk group members. With risks prioritized, the risk board can research process improvement possibilities for the system and begin the next step in the risk assessment process, which is defining risk avoidance alternatives. Peer group meetings are held to determine what actions or decisions could be made that reduce the probability and/or severity of impact of key risks. Residual risk, which could not be avoided, is analyzed to determine what risks are candidates for the development of a mitigation

strategy. While all risks are discussed, risks with medium and high exposure ratings are the serious candidates for development of mitigation strategies. Mitigation strategies include possible delays in development, extra cost, and possible loss of features or overall system performance. The next step in the process is developing a disaster recovery plan or system contingency plans for identified medium and high risks.

3.9 Disaster Recovery Plans

The DoN recognizes that risks and vulnerabilities have a likelihood of being exploited. In many cases, the last line of defense is the Navy disaster recovery plan. *The Disaster Recovery Journal* defines a DRP as a, "management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort (*Disaster Recovery Journal*, 2009). A review of standard Department of Navy DRP will reveal insight into whether these plans perform their desired functions effectively.

3.10 System Contingency Plans

The DoN, which views disaster recovery of information systems as a vital role to mission success, develops their DRPs as System Contingency Plans (SCP). The SCP is developed in accordance with Navy directives OPNAVINST 5239.1C and SECNAVINST 5239.3 and primarily directed towards all DoN systems. The contingency plan satisfies the requirements of DoDI 8500.2 IA Control CODP-3 Disaster and Recovery Planning, which states that a disaster plan exists that provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. Disaster recovery

procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.

In addition to the SCP, commands often reference the System Operational Sequencing System (SOSS) for contingency planning of non-security related casualties. This document defines procedures for systems equipment initialization and restoration. It is used as a response to system casualties including equipment failure and power loss. Contingency plans are tested monthly and quarterly to ensure that AIS controls are effective and function reliably during service interruptions. SCPs address plausible situations/conditions that must be recognized and understood by the commands to ensure DoN System integrity is never compromised. SCP recommends a course of action to be taken when dealing with events that could interfere with normal DoN Enterprise operations. The SCP discusses actions required to rapidly restore mechanisms soon after their functionality is interrupted. Actions within the SCP are recommendations only and are always subordinate to approved command procedures/policies. DoN enterprise users/maintainers are encouraged to identify additional scenarios and recovery actions, and include them in local command contingency planning and training activities.

3.11 SCP Scope

The SCP is applicable to all DoN enterprises equipped surface ships and shore installations. The plan provides the DoN team and security administrators with information that will assist them in the maintenance of information processed by the enterprise in case of emergency. The security contingency plan is a supplement to and subordinate to the ship's existing contingency plan. The SCP assumes that installation sites have approved a site contingency plan prepared in accordance

with prevailing requirements. The shipboard plans explain the procedures to be followed in case of emergencies that could be encountered by a naval combat vessel. The shipboard contingency plan serves to inform users of overall emergency procedures. The assets referred within the SCP are treated as critical processes. The SCP uses responsibilities, strategies, and situations that may be encountered to breakdown key elements within contingency process. The situations are based on risk resulting from possible unresolved threats from the site and system's business impact analysis and risk assessment.

3.12 SCP Responsibilities

Secure and safe operation of the DoN Enterprise system is the primary responsibility of the operators. The operators are required to notify the system administrator when suspected events arise which can compromise system functionality. The security administrator has the responsibility to assure that all classified aspects of the system are protected from compromise including the loading of unauthorized information to the system. This responsibility extends to occasions when normal system operation is interrupted. Assistance from the essential personnel is identified, as often other administrators are required because of the additional system operational capabilities possessed by this individual.

3.13 SCP Strategy/Methodology

The first responsibility of the DoN during execution of the SCP is the safety of the personnel. To that end, the SCP is subordinated to the shipboard contingency (or emergency) plan; however, the individuals responsible for control of classified material are also responsible for the prevention of

the compromise of that material. That responsibility encompasses various DoN Systems because they store classified information in the form of storage media such as removable hard disk drives. The primary strategy to protect the classified assets of the DoN enterprise is the use of physical protection. This is accomplished by providing a secure environment for housing the system. Access is limited to individuals with the proper security clearance or under escort by properly cleared individuals and is controlled at the door.

3.14 Action Plan

Action plans lay out procedures for revival of systems after an outage has occurred. The action plan in five main categories:

- Category 1: Physical Damage. This section refers to risks associated with the physical protection and availability of systems. Recovery actions include supplemental locking mechanisms or the stationing of an appropriately cleared individual in the area.
- Category 2: System Failure. System failures may be as simple as loss of a component or as drastic as the failure of the main processors or the loss of power to the system. Failures could affect or degrade the capabilities of the system as well as interfering with the mission.
- Category 3: Security Violations. Security violations can occur from a number of different circumstances, such as an administrator's misuse of privileges or an unauthorized user attempting to gain access.

- Category 4: Backup Operations. Backup operations as applied to this contingency plan represent maintaining copies of specific data and system information that can be used in the event the system must be re-installed.
- Category 5: Restoration of lost services is only one step of the response process used by the DoN. Investigation into how the event occurred, the assailant mission, the source, and the attack used are needed to ensure future attempts using the same signature are unsuccessful.

The ease of committing crimes using computers has prompted the DoN to develop procedures for the investigation and prosecution of computer crime against the U.S. Navy. Traditional law enforcement practices are not adequate to handle the capture and prosecution of these electronic criminals.

The DoN networks hold classified information about our country's offensive and defensive weapons systems and other information critical to national security. This makes DoN networks a high value target for hackers and cyber terrorists. Once an attempt to penetrate a DoN network or system has occurred, a set of practices and procedures is needed to acquire the evidence needed to prosecute these offenders, forensics is this practice. Judy Robbins defines forensics as, "The application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud" (Robbins, 2006).

The DoN benefits from their internal investigative unit, the Naval Criminal Investigative Service (NCIS). NCIS created a special investigative division named Computer Crime Investigation Group (CCIG) to resolve investigations involving computer hardware and/or software. The CCIG has merged, as all Defense Criminal Investigative Organizations (DCIOs) have, with the Department of Defense Cyber Crime Center (DC3). The DC3, in conjunction with the CCIG, has responsibility for investigating computer misdeeds for the DoN. To perform this intense investigation, it is important for the DoN as well as the DC3 to employ qualified personnel and keep these employees abreast of the newest evidence gathering and investigative procedures.

The DoN utilizes vulnerability assessments as the foundation for developing security programs for new and current systems deployed within its enterprise. A vulnerability assessment is the first step needed for system certification under DIACAP. The purpose of the DIACAP is for the DoD to certify and accredit information systems through an enterprise process for identifying, implementing, and managing IA capabilities and services. IA capabilities and services are expressed as IA controls. IA controls are maintained through a DoD-wide Configuration Control and Management (CCM) process that considers the architecture and risk assessments that are conducted at DoD-wide, Mission Area (MA), DoD Component, and IS levels (Department of Defense, 2007). Once the vulnerability assessments are completed, the DoN commands deploy security assets to defend and/or mitigate identified vulnerabilities. One of the weapons deployed in the security battlefront is the Intrusion Detection System (IDS). An examination of the methodology used by the DoN for their assessments and how IDSs play a vital role in this organization's network defense will expose their effectiveness in ensuring solid information assurance.

3.15 IA Vulnerability Assessment and Methodology

The DoN's methodology for vulnerability assessment was created in a joint effort from the Defense Information Systems Agency and the Department of Energy. Vulnerability assessments are authorized by local commands developing new systems or current systems which are in need of re-certification under DIACAP rules. Systems under development are required to be certified within a year of deployment and, upon certification, are required to hold yearly assessments to address new threats. The DoN methodology describes 10 elements or areas of concern during the assessment:

1. Network architecture. This element provides an analysis of the information assurance features of the information network(s) associated with the organization's critical information systems. Information examined should include network topology and connectivity (including subnets), principal information assets, interface and communication protocols, function and linkage of major software and hardware components (especially those associated with information security such as intrusion detectors), and policies and procedures that govern security features of the network (Department of Energy, 2002).
2. Threat environment. This element includes a characterization of threats, identification of trends in these threats, and ways in which vulnerabilities are exploited. To the extent possible, characterization of the threat environment should be localized, that is, within the organization's service area (Department of Energy, 2002).
3. Penetration testing. The purpose of network penetration testing is to utilize active scanning and penetration tools to identify vulnerabilities that a determined adversary could easily

exploit. Penetration testing can be customized to meet the specific needs and concerns of the command (Department of Energy, 2002).

4. Physical security. The purpose of physical security assessment is to examine and evaluate the systems in place (or being planned) and to identify potential improvements in this area for the sites evaluated. This includes access controls, barriers, locks and keys, badges and passes (Department of Energy, 2002).
5. Physical asset analysis. The purpose of the physical asset analysis is to examine the systems and physical operational assets to ascertain whether vulnerabilities exist (Department of Energy, 2002).
6. Operations security. The OPSEC assessment reviews the processes and practices employed for denying adversary access to sensitive and nonsensitive information that might inappropriately aid or abet an individual's or organization's disproportionate influence over system operation (Department of Energy, 2002).
7. Policies and procedures. The objective of the policies and procedures assessment task is to develop a comprehensive understanding of how a facility protects its critical assets through the development and implementation of those documents (Department of Energy, 2002).
8. Impact analysis. The purpose of the impact analysis is to help estimate the impact that outages could have on a command. Outages in electric power, natural gas, and oil can have significant financial and external consequences to a command (Department of Energy, 2002).
9. Infrastructure inter-dependencies. The purpose of the infrastructure inter-dependencies assessment is to examine and evaluate the infrastructures (internal and external) that

support critical facility functions, along with their associated inter-dependencies and vulnerabilities (Department of Energy, 2002).

10. Risk characterization. Risk characterization provides a framework for prioritizing recommendations across all task areas. The recommendations for each task area are judged against a set of criteria to help prioritize the recommendations and assist the organization in determining the appropriate course of action. It provides a framework for assessing vulnerabilities, threats, and potential impacts (Department of Energy, 2002).

These 10 elements combine to give the DoN a complete analysis of their security vulnerabilities and priority of mitigation. One of the steps of mitigation will include the deployment of security resources to combat threats identified during the assessment. One of the main tools used by the DoN is intrusion detection systems.

3.16 IA Enabled Product Review: Intrusion Detection Systems

An IDS monitors network traffic, monitors for suspicious activity, and alerts the system or network administrator. IDS respond to malicious traffic by taking action, such as blocking the user or source IP address from accessing the network or notifying network management for further action. The DoN deploys mostly Network IDSs, which scan all inbound and outbound traffic from strategic perimeter points on the network. For critical systems, Host IDSs (HIDS) are installed. HIDS run on individual hosts or devices on the network. They monitor the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. DoN IDSs are administered locally and monitored by the Navy's Network Information Operations Command (NIOC), which gathers the DoN security information to predict the Navy's

overall security posture. Attacks against the U.S. military have dramatically increased within the past few years. With countries now using cyber warfare to conduct information theft, espionage, and denial of service attacks, the DoN must stay ahead of its adversaries by deploying the latest technology to fight new challenges on the road ahead.

3.17 Risk Management Framework

The Risk Management Framework (RMF) is a framework created by the NIST to address risk management (NIST, 2012). The RMF uses the risk based approach to security control selection and specification considering effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders (EO), policies, standards, or regulations. There are six RMF categorization steps that serve as the basis for this NIST guidance (NIST, 2012). Step 1: Categorize. The system is assessed and categorized based on an impact analysis. Step 2: Select. Chose which during this period the systems is given a baseline set of security controls that are to be addressed in the design. Step 3: Implement. During this step the controls selected in Step 2 are deployed within the system to include the associated environment of operation. Step 4: Assess. The controls implemented are assessed to see if they are working as intended, and that the desired outcome meets the security requirements for the system. Step 5: Authorize. Get authority for the system to operate based upon an acceptable decision upon the acceptable risk for the system. Step 6: Monitor. Continually assess the security control of the system on an ongoing basis. This can include annual security checks to review compliance.

4.0 Cyber Security Issues in Technological Devices

Secure computing is essential as environments continue to become intertwined and

hyperconnected. As the Internet of Things (IoT), Web of Things (WoT), and the Internet of Everything (IoE) dominate the landscape of technological platforms, protecting these complicated networks is important. The everyday person who wishes to have more devices that allow the ability to be connected needs to be aware of what threats they could potentially be exposing themselves to. Additionally, the unknowing consumer of everyday products needs to be aware of what it means to have sensors, Radio Frequency IDentification (RFID), Bluetooth, and WiFi enabled products. This submission explores how Availability, Integrity, and Confidentiality (AIC) can be applied to IoT, WoT, and IoE with consideration for the application of these architectures in the defense sector.

The next era of computing will be outside of the traditional desktop (Gubbi, Buyya, Marusic, & Palaniwami, 2013). When you consider Bring Your Own Device (BYOB) as a radical step, imagine using a device such as a refrigerator that contains an embedded computing device to track the quantity of groceries within. This embedded device would allow access to email, weather, and other devices that allow connectivity through WiFi, or some Application Programming Interface (API) to a web based application. Thus, the data collected would be weather, thermostat cooling patterns, foods purchased, the cost of items per month, average consumption, and more. This massive amount of data that can also be collected means there must be a large place where this data is stored. At the moment, organizations such as Cisco Systems and others are pushing for WoT and IoT but none has a plan for ensuring IA posture is maintained during various modes of operation.

Thus with these connected environments maintaining anonymity in times of high surveillance (Haro & Dawson, 2016). The use of items such as Kali Linux, The Onion Router (TOR), and cryptography allow for a user to remain under the watchful eye (Dawson & Haro, 2017).

4.1 Virtualization and Cloud Computing

Virtualization is a technology that can allow individuals to develop virtualized images of their computing environments. Included is the creation of an OS, server, storage, and network resources. This allows for the ability to emulate hard disks in 1 of 3 different disk image formats. The first format is Virtual Disk Image (VDI) which is a VirtualBox specific format (Oracle, 2013). The second format is Virtual Machine Disk (VMDK) that is an open format used by VMWare products (Oracle, 2013). The third format is Virtual Hard Disk (VHD) that represents a virtual Hard Disk Drive (HDD) containing items that would be found on a physical HDD (Oracle, 2013).

Cloud computing is based on concepts of virtualization, distributed computing, networking, and is underpinned in the latest Web and software technologies (Vouk, 2008). A useful definition of cloud computing is that it is a way of delivering applications as services over the Internet as well as a way of providing for the hardware and system software that act as platforms for these applications and services (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, & Zaharia, 2009). Cloud is also used to refer to a network of computers that are linked together and distribute processing capacity and applications to different systems (Johnson, Levine, & Smith, 2009). Cloud computing lets organizations add on to their IT and computing capacity without having to invest in new architecture, software or hardware, or in training and developing personnel (Glotzbach, Mordkovich,& Radwan, 2008). A cloud environment could prove to be a cost effective implementation of which would allow for scalability if these right tools are utilized. Figure 2 provides an overview of how a VM environment looks. The hardware is loaded with the selected OS platform. The OS platform can be Linux, Mac, Solaris, or Windows. Once the OS is loaded onto the hardware then the hypervisor is loaded. The hypervisor allows for multiple VMs to be hosted. The VMs act independently from the OS platform. This environment allows for testing,

development, and integration of new OSs. When constructing the VM environment it is important to think about the overall architecture which includes the hypervisor (Sailer, Jaeger, Valdez, Caceres, Perez, Berger, & van Doorn, 2005). There are two distinct types of hypervisors which are Type 1 and Type 2. The Type 1 hypervisor runs directly on the system's hardware to control the hardware to include managing the guest OS. An example of this would be XenServer or VM ware ESXi. The Type 2 hypervisor runs within the OS environment with the hypervisor layer as an appliance that is accessed through an application such as Oracle VirtualBox.

Cloud computing provides services that are available over the Internet or the intranet and the customers can access them using their computers or even mobile devices like the PDAs or phones. Cloud computing also makes it possible for the employees of the organization to access the services from diverse locations instead of being the second application software layer. The guest OSs runs on the third layer above the hardware.

Cloud computing is therefore characterized by on-demand availability of the service and on the concept of self service. The cloud computing services are to be automated so that there is little interaction of the service provider or the service users. In cloud computing, the service provider pools resources and makes them available to different customers while these customers do not concern themselves about how and where the resources are getting pooled from.

Cloud computing provides flexibility in terms of elasticity and scalability, meaning that the services can be increased or decreased on need basis and in an automated manner without the intervention of the IT personnel. As such, organizations that deploy cloud computing do not have

to buy additional computing resources if they expect an increase in demand. The organizations also do not have to fear redundant resources as the cloud services are paid for only on the basis of usage (Kundra, 2010).The automation and the freeing of the IT personnel from the task of managing, updating and maintaining the IT systems means that organizational resources are freed up and there are additional benefits of using the resources for other business related needs. In addition to the benefits of automation, cloud computing also means that there is no requirement for the customers to go for selection of resources from individual service providers or for getting certifications from them.

The cloud computing service provider provides a pool of diverse service in a ready to use form that the customers simply have to access and start using (Kundra, 2010). Cloud computing also leads to a reduced information technology overhead for the end-user, as the service provider takes the responsibility of maintaining, managing, developing and integrating the systems and the services that the end-users use. Also, as the resources are pooled, it means that fewer organizations or departments are using their own resources and hence there is a tremendous scope for energy and power savings (Kundra, 2010). Cloud Computing, being managed and provided for by the service provider is managed in a highly professional manner that ensures that there are no or minimum service outages and the problems if any are rectified immediately. The service providers, being experts and professionals in their field, are better equipped with the resources and facilities to ensure that the service is provided without any disruption (Kundra, 2010). Cloud computing leads to reduced costs as the services may be shared by many organizations and thus reduce the cost of access and maintenance. The services are also paid for based on need, and organizations can better plan their IT budgets and tailor it to their specific requirements. It is also cost effective as it is

easier to quantify and measure the usage of the services and thus it is easy to track the revenue and costs associated with that particular service (Kundra, 2010).

4.2 Hyperconnectivity

Hyperconnectivity is a growing trend that is driving cyber security experts to develop new security architectures for multiple platforms such as mobile devices, laptops, and even wearable displays (Dawson, Omar, Abramson, & Bessette, 2014). The future of both national and international security relies on complex countermeasures to ensure that a proper security posture is maintained during this state of hyperconnectivity. To protect these systems from the exploitation of vulnerabilities, it is essential to understand current and future threats to include the instructions, laws, policies, mandates, and directives that drive their need to be secured. It is imperative to understand the potential security-related threats with the use of social media, mobile devices, virtual worlds, augmented reality, and mixed reality.

In an article published by *Forbes*, a contributor describes the concept of hyperconnectivity in six different scenarios (Ranadivé, 2013). These events range from energy to hospitality. In healthcare, for example, there would be real time monitoring through wrist monitors that the medical staff could monitor to get instantaneous, real-time feeds on patients. They would be able to foresee problems before they occur or receive alerts during various events. Imagine a pregnant woman that is having early complications who could be monitored first through a wristband that delivers real-time patient information wirelessly.

When discussing hyperconnectivity, it is necessary to examine systems of systems concepts. Systems of systems is a collection of systems tied together to create a more complex system

(Popper, Bankes, Callaway, & DeLaurentis, 2004). When thinking about the possibilities of hyperconnectivity the Personal Area Network (PAN) is an excellent example as it allows multiple technologies to be interconnected with soil ware applications. The Google Glass has the potential to all Global Positioning System (GPS), social media, digital terrain overlays, and synchronization with other devices. This increases the complexity of the system as it becomes part of larger systems which multiplies the number of potential vulnerabilities.

4.3 Internet of Things

IoT is a global infrastructure for information society enabling services by interconnecting physical and virtual things based on existing and evolving interoperable Information Communication Technologies (ICT) (International Telecommunication Union, 2012). Gartner has developed a figure which displays the hype cycle of emerging technologies. This hype circle shows the expectations on the y-axis and time on the x-axis. This is displayed in Figure 4.1: Gartner 2014 Hype Cycle of Emerging Technologies (Gartner, 2014). The time shown is the innovation trigger, the peak of inflated expectations, the trough of disillusionment, slope of enlightenment, and plateau of productivity (Gartner, 2014). What the figure fails to provide is anything associated with security about the technologies identified. The figure simply shows the cycle of emerging technologies with time corresponding to

expectations.

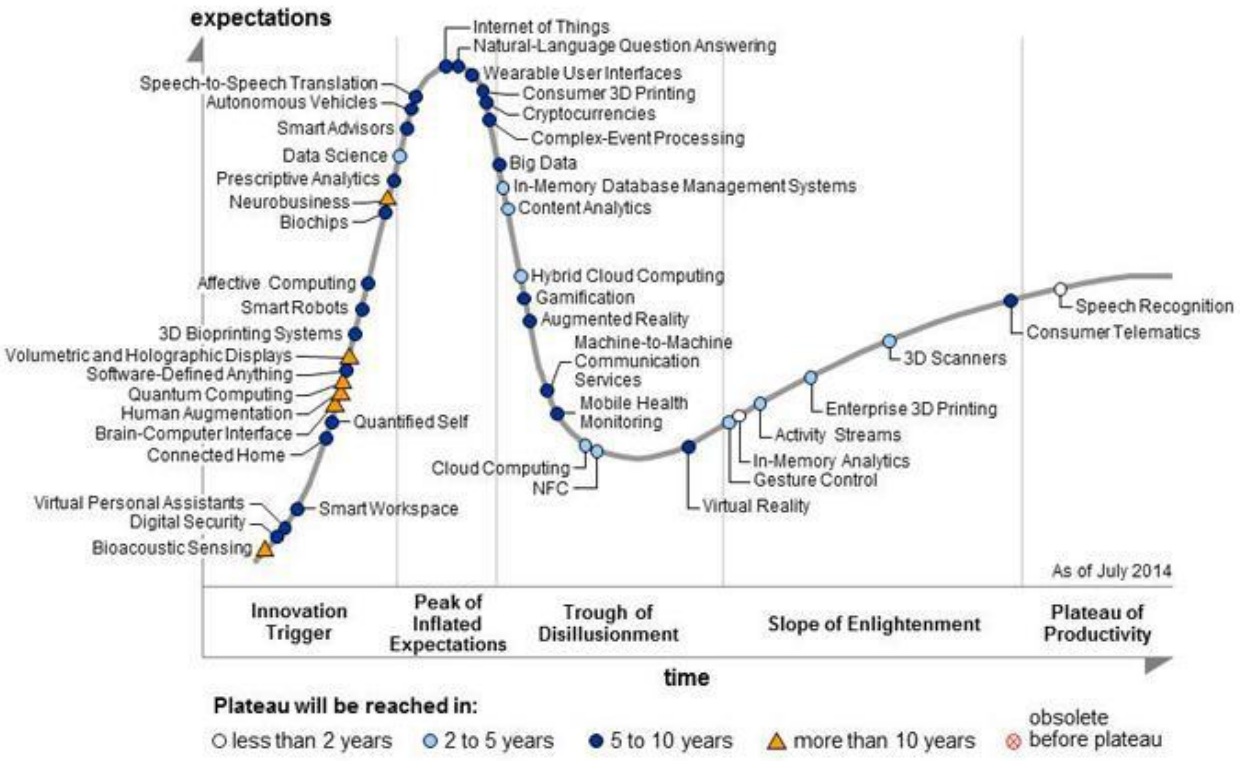


Figure 4.1: Gartner 2014 Hype Cycle of Emerging Technologies (Gartner, 2014)

4.4 Web of Things

The WoT is a continued vision that describes concepts where everyday objects are fully integrated into the World Wide Web (WWW). This concept focused on embedded computing devices that enable communication with the WWW. The devices can run from refrigerators to mobile devices integrated with the Web through an API (Guinard & Trifa, 2009). The Social WoT offers opportunities to use social connections and underlying social graphs to share digital artifacts (Guinard, 2011). This would help bridge a gap between social networks and networks of objects transforming communication. Figure 4.2: Building the Web of Things displays the WoT architecture and the detailed layers it is comprised of.

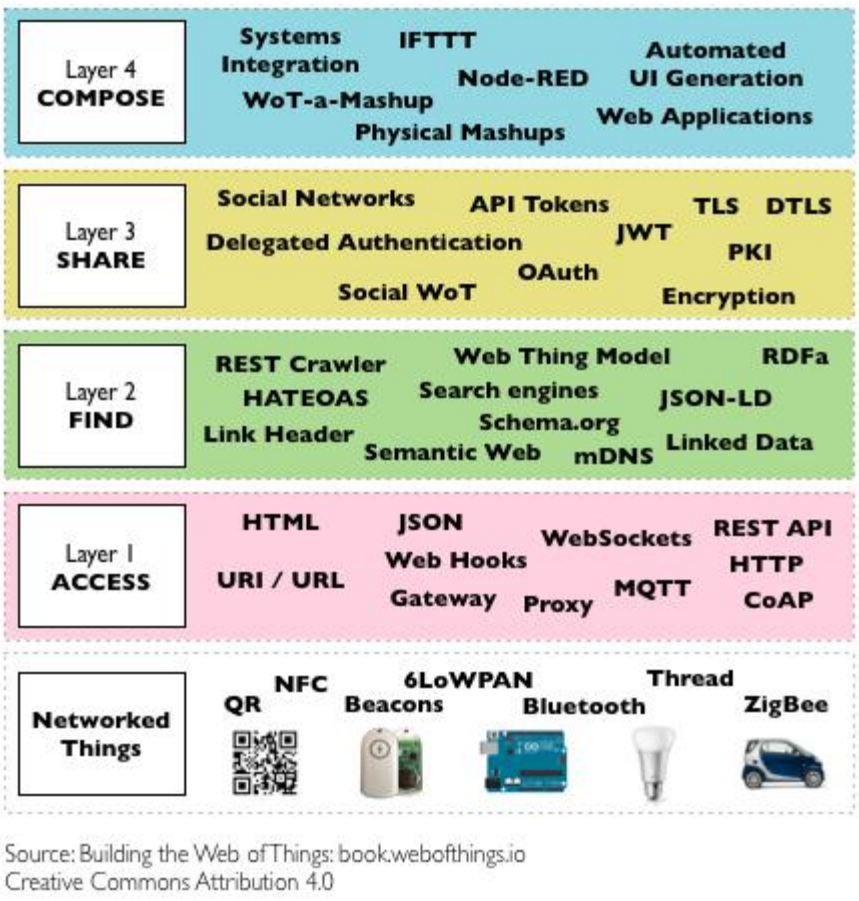


Figure 4.2: Building the Web of Things

This bridge between social connections and basic things could allow for a plethora of data that can be analyzed unlike before. When looking at the networked things, you can see that multiple technologies can be enabled in WoT. When looking at Layer 1, you can immediately see items that cause problems. For examples, Hyper Text Markup Language (HTML) and JavaScript Object Notation (JSON) contain known vulnerabilities. In current social networks, geolocation provides individuals exact location; however, anyone that develops an application using this API can tweak items providing even more granularity of its users. Even without modification of Tweets, only adding the location will provide details such as neighborhood, city, state, or country. This

publication information can be used to start an analysis. In iOS version 6.26+ and Android version 5.55+ precise location can be shared if elected to do so. Also, third party applications or websites may share specific Tweet locations as well.

Various social media accounts provide the ability to associate a location. This position over time can provide trends of sites visited with time/date stamps. This can be used to start developing a full analysis on Tweeting trends from particular locations, frequency of location visits, and content analysis through text mining. Exchange Image File Format (EXIF) data is a standard that specifies the formats for images, sounds, and ancillary tags used by digital cameras. The EXIF digital image standard defines the following: the basic structure of digital image data files, labels and JPEG marker segments the conventional uses, and how to define and management format versions (Tešić, 2005). Research has been conducted on how to efficiently extract EXIF data for prosecuting those involved in child pornography (Alvarex, 2004).

In Layer 3, some of these concerns can be addressed in Figure 4.2. In this layer, controls can be made for the ability to share content. Content can be tagged with a severity and classification to have a security feature added automatically. If the data were Personal Identifiable Information (PII) then the data would have encryption and access controls that only allow certain individuals to obtain it. That data could be sent wirelessly over a Bluetooth enabled device or a medical beacon. The types of encryption to be used would depend on if the data is in transit or if the data is in rest. Other factors would include the type of data being secured, and implementation to prevent over using cryptographic keys (Bellovin & Housley, 2005).

4.5 Internet of Everything

The IoE consists of four groupings, which are data, things, people, and process (Bradley, Barbier, & Handler, 2013). IoE leverages data as a means to make more insightful decisions. IoT plays a significant role in the things of IoE as this is the network of physical devices and objects connected to the Internet for decisions making. The IoE connects people in more valuable and relevant ways. The process is the last part which is delivering the correct information to the right entity at the right time.

Researchers at Cisco Systems estimate that over 99 percent of physical devices are still unconnected and that there is a market of $14.4 trillion. This white paper urges business leaders to transform their organizations based on key learnings to be competitive for the future (Evans, 2012). IoE is comprised of four key things, which are people, data, and things built on the process. Figure 4.3 displays these four key things in relation to connections. The model IoE is made up of three types of connections: People to Machine (P2M), Machine to Machine (M2), and People to People (P2P).

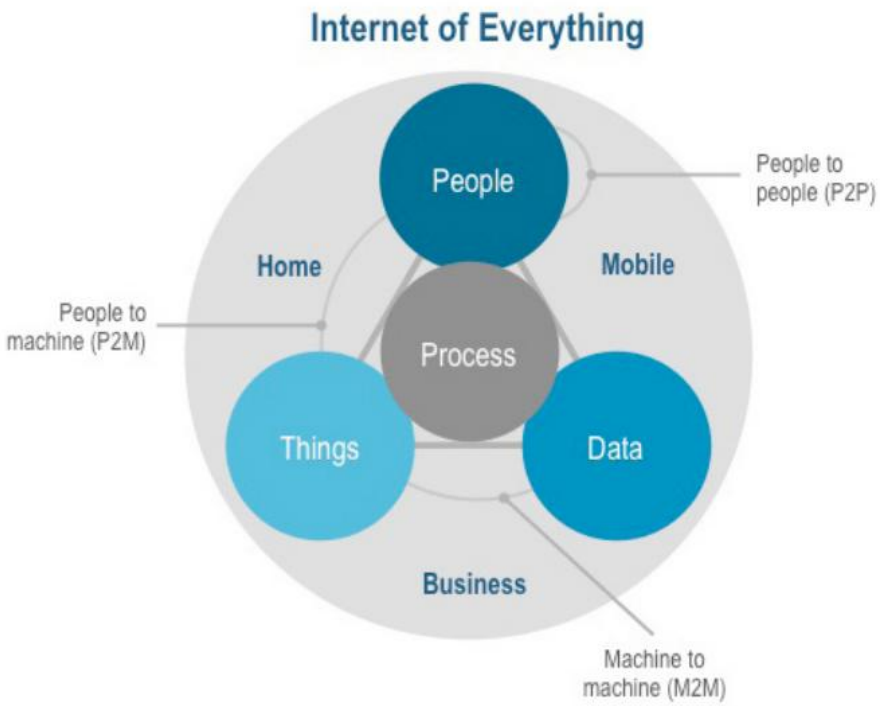


Figure 4.3: The What, Where, and How of the Internet of Everything (Cisco IBSG, 2012)

4.6 Body Hacking and Enhancement

One of the newest trends in staying connected is human enhancement through body hacking (Nortol, 2007). This involves individuals placing RFID chips into their bodies. These RFID components are associated with unique ID numbers that can be used for unlocking doors, logistical tracking, embedded electronics, e-government, and more. The use for e-government would allow interaction between government and outside groups through the connected body parts. A health organization could monitor the status of a group through embedded chips or other devices connected to an individual or group.

The issues surrounding body hacking is the lack of security controls associated with making these

mods. Early in this chapter hyperconnectivity, IoT, and IoE was discussed to provide an overview of these various technological concepts. When adding more connectivity to systems, the complexity increases, thus it becomes more difficult to effectively protect from potential threats. Items such a pacemakers have already been proven to be hackable (Kirk, 2012; Richardson, n.d.).

The report "Enhanced Warfighters: Risk, Ethics, and Policy" (2013) that was prepared for The Greenwall Foundation discusses the findings of using technology for soldiers. As other technologies are emerging within the United States (U.S.) military sector so are robotics, Artificial Intelligence (AI), human enhancement technologies, other cyber capabilities. The issues surrounding human enhancement technologies among other items are the operational, ethical, and legal implications (Mehlman, Lin, P., & Abney, 2013). Regarding risks, those identified are about the technology falling into the wrong hands allowing for reverse engineering. Reverse engineering would allow non-friendlies to develop similar technologies on their own to rival those found on the warfighters.

4.7 Security and Privacy

As a new wave of Internet-enabled technologies arrives, it is imperative to understand fully the security and privacy concerns (Thierer, 2015). Understanding these concerns also means understanding how to appropriately apply IA controls to systems. Addressing security objectives appropriately will allow for risks to be mitigated. This means following the principles of security to ensure IA posture is achieved.

All of these connected devices using proven standards, policies, and guidance can help with the

ease of integrating these technologies into everyday life. Currently, there is a lack of guidance for securing IoT, IoE, and WoT as a cohesive unit; however, there is appropriate documentation available through the NIST, Federal Information Processing Systems (FIPS), DoD, Institute of Electronic and Electrical Engineers (IEEE), International Organization for Standardization (ISO), Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and more. It will be key for the security engineer to understand how to protect these devices individually and then understand how the devices become more vulnerable when connected. Mobile devices would need to be hardened with appropriate security controls (Dawson, Wright, & Omar, 2016; Omar & Dawson, 2013).

Encryption would need to be on devices that have IoT capabilities such as refrigerators, televisions, or smart watches. This would allow the protection of data in transit and at rest. The recommended guidance would be to use an approved public algorithm and not a weak algorithm. The classification of weak and strong algorithm change over time, thus it is important to keep abreast of the changes in cryptography algorithms (Bellovin & Steven, 2005). Access controls would need to be placed to ensure that other users of the hyperconnected systems to do not have the ability to elevate privileges through lateral movement within a network. The NSA already has substantial items providing cryptography as they have been using this form of data security since the end of the 1970s (Newman & Pickholtz, 1986).

Commercial entities that provide services and host data identified as having information regarding state information should require that only approved products be used (Caddy, 2011). And organizations should be required to follow similar workforce requirements so that individuals who are implementing crypto system must be licensed or certified as security engineers to ensure only qualified personnel are designing these system architectures (McNulty, 2005).

With the potential threats of cyber terrorism affecting national and international security, the importance of security is elevated to greater heights (Dawson, Omar, & Abramson, 2015). New threats against national infrastructure and digital crime are making researchers consider new methods of handling cyber incidents (Dawson, & Omar, 2015). It is imperative that if the government or commercial sectors want to make use of these new technological Internet and Web-enabled architectures that they are prepared to battle new threats. Technological threats need to be accessed individually, but when those threats are through connected applications or systems, then a joint assessment has to be done with the new configuration. Once this new configuration has been established, which includes the operating environment, then a discovery of threats has to occur. After this discovery, appropriate mitigations to the systems applied, and risks accepted. Next, the developer of the technology continuously monitors remaining risks to ensure the criticality level does not rise. As commercial systems do not review the complete operating environment, such as the location change, it will be imperative that this is examined so that consumers are safer when operating devices to different places.Currently, DoD is using limited

IoT to be more efficient in combat. New battlefield technology includes helmets that provide a Heads Up Display (HUDs) to provide GPS battle mapping to integrate with other technologies that provide real-time tracking of the battlefield. A potential example includes the ability to control UAVs through sensors tied to platoon leaders rather than the use of a Universal Ground Control System (UGCS) or Portable Ground Control System (PGCS). IoT, IoE, and WoT can place the control of tactical devices directly in the hands of those soldiers who are a front line during combat missions. In years to come, body enhancement with RFIDs and other sensors could provide situational awareness data to the soldiers and those that lead them. This data can be analyzed to maximize the effectiveness of troop movement, target location, and other activities deemed key to the mission of the military.

Secure computing is essential as technological environments continue to become intertwined and hyperconnected. The policies to properly secure these new environments must also be explored as many of the security controls found within guidance such as the DoD focuses on singular systems and components (Dawson Jr, Crespo, & Brewster, 2013).

There needs to be the creation of new cyber security controls that review embedded sensors, body modifications, and devices that fully take advantage of Internet-enabled technologies. With the emergence of these technologies, the possibilities are endless; however, there will be new vulnerabilities unexplored. The current guidance provided by NIST does not cover these needed

items. A working group needs to be created that looks at the impacts of these items in the commercial, and federal spaces to associate proper risk ratings to the needed controls. Similar to the database that serves as a repository for software vulnerabilities the same needs to be created for new controls. And since these controls alter significantly when coupled with other technologies that system needs to be dynamic, allowing for changing associated weights to include providing new vulnerabilities based upon any reconfiguration.

4.8 Issues with Android Phones and Other Mobile Devices

Smartphones are becoming a more integrated and prevalent part of people's daily lives due to their highly powerful computational capabilities, such as email applications, online banking, online shopping, and bill paying. With this fast adoption of smartphones, imminent security threats arise while communicating sensitive, personally identifiable information (PII), such as bank account numbers and credit card numbers used when handling and performing those advanced tasks (Wong, 2005; Brown, 2009). Traditional attacks (worms, viruses, and Trojan horses) caused privacy violations and disruptions of critical software applications (e.g., deleting lists of contact numbers and personal data). Malware attacks on smartphones were generally "proof of concept" attempts to break through the phone's system and cause damage (Omar & Dawson, 2013). However, the new generation of smartphone malware attacks has increased in sophistication and is designed to cause severe financial losses (caused by identity theft) and disruption of critical software applications (Bose, 2008). Because smartphones are becoming more diverse in providing general purpose services (i.e., instant messaging and music), the effect of malware could be

extended to include draining batteries, incurring additional charges, and bringing down network capabilities and services (Xie, Zhang, Chaugule, Jaeger, & Zhu, 2009).

Smartphones are rapidly becoming enriched with confidential and sensitive personal information, such as bank account information and credit card numbers, because of the functionality and powerful computational capabilities built into those mobile devices. Cyber criminals, in turn, launch attacks especially designed to target smartphones, exploiting vulnerabilities and deficiencies in current defense strategies built into smartphones' operating systems. Bhattacharya (2008) indicated that because of skill and resource constraints, businesses are ill-prepared to combat emerging cyber threats; this claim is true for smartphones as well, given the fact that those mobile devices are even less equipped with necessary protections, such as antivirus and malware protection software. Some services and features, such as Bluetooth and SMS, create attack vectors unique to smartphones and thus expand the attack surface. For example, in December 2004, a Trojan horse was disguised in a video game and was intended to be a "proof of concept," which signaled the risks associated with smartphones that could potentially compromise the integrity and confidentiality of personal information contained in smartphones. Attackers can easily take advantage of those services provided by smartphones and subvert their primary purpose because they can use Bluetooth and SMS services to launch attacks by installing software that can disable virus protection and spread via Bluetooth unbeknownst to smartphone users.

With the development of features and services for smartphones, security measures deployed are currently not commensurate because those services and features, such as MMS and Bluetooth, are driven by market and user demands, meaning that companies are more inclined to provide more

entertainment features than security solutions. In turn, this further increases vulnerabilities and opens doors for hackers to deploy attacks on smartphones. Furthermore, Mulliner & Miller (2009) argue that the operating systems of smartphones allow the installation of third-party software applications, coupled with the increase in processing power as well as the storage capacity. Scenarios like this pose worse security challenges because hackers could exploit those vulnerabilities, which are further compounded by users' lack of security awareness. Smartphone attackers are becoming more adept in designing and launching attacks by applying attack techniques already implemented on desktop and laptop computers; smartphones' enhanced features, such as music players and video games, produce easy-to exploit targets by sending seemingly benign files via music or video game applications to users and luring them into downloading such files. Becher, Freiling, and Leider (2007) indicated that attackers could exploit such vulnerabilities to spread worms autonomously into smartphones. Therefore, hackers usually use a combination of technical expertise along with some social engineering techniques to trap users into accepting and downloading benign applications, which are used later to execute malicious code and affect critical applications running on smartphones.

Android's core components, such as Linux and connectivity media, are vulnerable to attacks through which personal and confidential information is likely to be compromised. Android's threats are further amplified by the fact that users are limited to using their smartphones for basic services and functions, such as email and SMS/MMS. Users lack the programming mind-set to protect their Android smartphones and stay current with the latest security software updates. This gives hackers an edge to target Android smartphones in the hope of gaining unauthorized access to disable core services (email and web browsing); abuse costly services (i.e., sending MMS/SMS

and making calls to high-rate numbers); eavesdrop on calls; and most importantly compromise sensitive information to be sold for a price. Android's open-source nature further increases security vulnerabilities because attackers can easily exploit this feature to modify the core applications and install malicious software, which could be used to compromise Android-based smartphones and ultimately cause disruption and monetary loss.

4.9 Challenges with a Mobile Browser

One cyber security challenge for mobile devices is the screen size. For example, web address bars (which appear once the user clicks on the browser app) disappear after a few seconds on a smartphone because of the small screen size (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is usually the first line of defense for cyber security. Checking the Uniform Resource Locator (URL) of a website is the first way users can insure that they are at a legitimate website. Moreover, SSL certificates for a website are usually more difficult to find on a mobile phone browser (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This adds another gap in security for mobile devices. Furthermore, the touch-screen attribute of mobile phones can be cause for concern when dealing with cyber attackers. Traynor states that the way elements are placed on a page and users' actions are all opportunities to implant an attack. An illustration of this is seen when an attacker creates an attractive display content (i.e. an advertisement for an app or a link to a social media app) in which the malicious link is carefully hidden underneath a legitimate image. Unfortunately, once the user clicks the image they can be redirected to the malicious content via the link (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012).

4.10 Common Mobile OS, IOS, and Linux

Apple debuted iOS, or iPhone OS, in 2007, with the inception of the iPhone to the cell phone market (Barrera & Van Oorschot, 2011). Presently, the iOS platform not only runs on iPhone but also iPod Touch and iPad (Barrera & Van Oorschot, 2011). Apple developers specifically write apps to run on all iOS devices. Apple's iOS popularity stems from an easy user interface, including "onscreen interactive menus, 2D and 3D graphics, location services, and core OS functionality such as threads and network sockets" (Barrera & Van Oorschot, 2011).

Apple utilizes various techniques to ensure that the security and quality of their applications are not compromised by malicious cyber attackers. Unlike Android's OS, iOS prevents third-party apps from accessing external data by utilizing a "sandbox mechanism" (Barrera & Van Oorschot, 2011). This mechanism employs policy files that restrict access to certain device features and data (Barrera & Van Oorschot, 2011). App developers use registered APIs to restrict apps from accessing protected resources (Barrera & Van Oorschot, 2011). Finally, Apple approves every iOS app developers create. The approval process has not been published by Apple; however, it is believed that "the company employs both automated and manual verification of submitted apps" (Barrera & Van Oorschot, 2011). Once Apple approves a potential app, Apple "digitally signs it and releases it" to the App Store (Barrera & Van Oorschot, 2011). Ultimately, Apple has the final say pertaining to which apps are available for download in the App Store – "apps that Apple hasn't digitally signed can't run on the device" (Barrera & Van Oorschot, 2011).

Linux is a Unix like OS that is built on the Linux kernel developed by Linus Torvalds with thousands of software engineers. As of 2012 there are over two hundred active Linux distributions.

The majority of the kernel and associated packages are free and OSS. This type of software provides a license which allows users the right to use, copy, study, change, and improve the software as the source code is made available. Providing source code allows developers or engineers to understand the inner workings of development. Imagine being able to study Mac or Windows by viewing all the source code to replicate similar developments. This exercise is great for a developer to learn low level coding techniques, design, integrate, and implement. This is also a great method for penetration testing with the ability to test all available back doors within the software.

In terms of associated cost, the majority of Linux distributions are free; however, some distributions require a cost for updates or assistance that related to specific needs such as OS modifications for server hosting. In software, there is a packet management system that automates the process of installing, configuring, upgrading, and removing software packages from an OS. In the Linux OS builds, the most common packet management systems are Debian, Red Hat Package Manager (RPM), Knoppix, and netpkg. The most popular Linux distributions for mobile use are Android IOS and Ubuntu.

4.11 Malware Attacks on Smartphone OS

Along with this, malware that targets smartphone operating systems is constantly evolving. An example of this is seen with "Zeus-in-the-Mobile" (ZitMo), a specific form of malware common to the Android operating system. ZitMo targeted Android users' bank apps; it attempted to bypass the banking two-factor authentication, steal credentials, and gain access to users' bank accounts, and

ultimately money (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is just one form of cyber-attacks that IT professionals are trying to prevent from occurring.

Lastly, it is believed that mobile devices will be the new vector for targeting network and critical systems (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). According to the report, mobile devices are an excellent way to spread malware because phones are great storage devices. A hypothetical example of a cyber-attack against a company's network is seen when malware is implanted in a smartphone. For example, a clever cyber attacker can write code to remotely control wireless connectivity technology and plant malware on the mobile phone. If that same phone is connected to a corporate network, i.e. the user is charging the phone on the company's computer, the malware can now attack the company's network. IT professionals want to prevent attacks like that from occurring because the economic consequences of such an event would be catastrophic. Ultimately, it is imperative that a national security standard is created for mobile devices in order to protect personal data.

4.12 Android Platform

According to Shabtai et al. (2010), Android is an open-source application execution environment that includes an operating system, application framework, and core applications. Android was designed and released originally by Android Inc. to provide a user-friendly, open, and easy-to-use mobile-based development environment. This open-source mobile development framework is user-centric because it provides a variety of developments, tools, and features. However, this open-development feature also poses challenges to securing sensitive user data and protecting users from malicious attacks, such as phishing applications that are usually sent to users to trick

them into providing their financial information and credentials while accessing malicious websites that look the same as the legitimate banking sites.

The Android operating system was first released in October, 2008 by T-Mobile 1G, and soon major telecommunications companies (such as T-Mobile) in both the U.S. and Europe adopted it because of its rich capabilities exemplified by core applications (i.e., email, web browsing, and MMS), entertainment features, and services, such as camera and Bluetooth. This has also led to Android's popularity amongst developers due to the open-source nature of Android, which offers the capability of developing and programming rich applications at the lowest level of Android's operating system. Since its initial release in 2008, Android has undergone many releases, the last being Android 2.2; this latest version of the Android platform brings many new and existing features and technologies to make both users and developers productive. Some of the new services and applications included in the new version aim at increasing speed (CPU is about 2-5 times faster), performance, and browsing (using version 8 engine that provides 2-3 times faster java script heavy page load). This new version also offers improved security features by allowing users to unlock their device using a password policy and the ability to wipe data from devices in case of theft or loss.

4.13 Android Security Model

Android is a multi-process system where each application (and parts of the system) runs its own process. The standard Linux facilities enforce security between applications and the system at the process level; those applications are assigned by users and group IDs. Applications are restricted in what they can perform by a permission mechanism, called permission labels, that uses an access

control to control what applications can be performed. This permission mechanism is fine-grained in that it even controls what operations a particular process can perform (Shabtai et al., 2010). The permission labels are part of a security policy that is used to restrict access to each component within an application. Android uses security policies to determine whether to grant or deny permissions to applications installed on Android OS.

Those security policies suffer from shortcomings in that they cannot specify to which application rights or permissions are given because they rely on users and the operating system to make that guess. They are therefore taking the risk of permitting applications with malicious intentions to access confidential data on the phone. Ongtang, McLaughlin, Enck, and McDaniel (2009) best described this security shortcoming by their hypothetical example of "PayPal service built on Android. Applications such as browsers, email clients, software marketplaces, music players, etc. use the PayPal service to purchase goods. The PayPal service in this case is an application that asserts permissions that must be granted to the other applications that use its interfaces" (Ontang, McLaughlin, Enck, & McDaniel, 2009). In this hypothetical scenario, it is unknown whether the PayPal application is legitimate or not because there is no way to determine whether this is the actual PayPal service application or another malicious program. Again, Android lacks security measures to determine and enforce how, when, where, and to whom permissions are granted.

4.14 Android's Security

Android uses permission mechanisms to determine what users can do in applications; this is achieved via the manifest permission that grants permissions to applications independently, which in turn, allows applications to run independently from each other as well as from the operating

system. This could be a good security feature since the operations being run by one application cannot interfere or otherwise impact operations within other applications. For example, users sending email messages will not be allowed (by default) to perform any operation within an application (such as reading a file from another application) that could adversely impact the email application (Developers, n.d). Applications achieve that by using the "sandbox" concept, where each application is given the basic functions needed to run its own process; however, if the sandbox does not provide the needed functions to run a process, then the application can interfere with the operations of another process and request the needed functions to run a process. This capability of allowing applications to request permissions outside of their sandbox capabilities could be harmful to Android mobile devices because it opens a window of opportunity for malware to exploit the privilege of accessing sensitive data on Android handsets and thus install malicious software (Vennon, 2010).

4.15 Attack Vectors and Infections Mechanisms Bluetooth

This is a wireless communication protocol used for short-range (about 10 meters) transmissions at 2.4 G.H.z. Bluetooth is one of the most widely used and preferred attack techniques for infecting smartphones because by pairing Bluetooth-enabled devices, hackers have the capability to access infected phones' critical applications and files, such as email, contact lists, pictures, and any other private data stored in the smartphone. Bluetooth-enabled smartphones are prone to various kinds of attacks due to security implementation flaws that exist in current security specifications. For example, Wong (2005) reveals that when two Bluetooth-enabled devices communicate after establishing a trusted relationship, all the credential information is left on both devices, even after the session is ended. This implementation hole allows potential hackers to have full access to the

device, without the owner's knowledge or consent, based on the previously established trust relationship; attackers then can access confidential data stored on smartphones and manipulate it. The only way smartphone users would be able to detect such security flaws is to observe the Bluetooth icon indicating an established Bluetooth connection; otherwise, attackers will have unauthorized access to the victim's smartphone. This security shortcoming, along with other security flaws found in Bluetooth security architecture, such as device-based authentication rather than user-based authentication, make smartphones vulnerable to direct attacks and threaten privacy and critical personal information.

4.16 MMS/SMS

Multimedia message service and short message service are both communication protocols that have become widely used and adopted by smartphone users as the standard for fast and convenient communications. Although it might seem unrealistic to think that hackers would ever be interested in targeting MMS/SMS, recent studies have shown that MMS/SMS can contain confidential information that is exposed to attacks due to lack of security services not provided by the cellular network. SMS suffers from exploitable vulnerabilities, such as lack of mutual authentication methods and non-repudiation. An SMS that is sent from a sender to a receiver cannot be mutually authenticated by both parties, which opens doors for hackers to exploit. Also, senders who send SMS cannot be held accountable for their sent SMS because there is no mechanism that could be implemented to ensure the sender's true identity. The weak security implementation of SMS can also be used as an attack mechanism by hackers, where an arbitrary computer can be used to inject SMSs into the network, thus exposing smartphones to risks. In addition, SMSs are susceptible to

man-in-the middle attacks while they are being transmitted over the air. Therefore, attackers are increasingly relying on MMS/SMS as an effective attack vector (Lockefeer, 2010).

4.17 File Injection and Downloadable Applications

Malware authors constantly develop new and innovative ways for attacking smartphones; sending benign files that contain malicious code and downloadable applications has proven to be a successful attack mechanism adopted by hackers. What makes such attack vectors effective is the fact that they come in the form of legitimate applications, luring smartphone users to disclose their private and financial information. For instance, in January 2010, a group of malicious writers calling themselves "09Droid" developed an application that specifically targeted Google Android phones and mobile banking institutions. The application contained the phrase "happy banking" on the summary statement that each application uses to advertise itself to potential users. The attack tempted users to purchase the mobile banking application from the Android Market in order to log on to their mobile banking accounts. While doing so, users would have to reveal their account numbers and passwords, which would then be sent to the authors of the malicious program (Morrison, 2010). This kind of well-crafted attack underscores the powerful capabilities of emerging attacks and the attackers; they target banking institutions and credit unions and use their logos to lure naive smartphone owners into giving their confidential information to applications that look identical to as the legitimate ones.

4.18 Open Source Intelligence

The intelligence field of Open Source Intelligence (OSINT) relies on data that is freely available on the public domain to conduct an analysis. OSINT is conducted by collecting data in an overt manner. OSINT has been defined by the United States (U.S.) Department of Defense (DoD) and the U.S. Director of National Intelligence (DNI) as analysis produced from publicly available information that is collected, exploited, and disseminated for the purpose of addressing a specific intelligence requirement (National Defense Authorization Act for Fiscal Year 2006). In Subtitle D – Intelligence – Related Matters SEC. 931., 932., and 933 findings by Congress for the DoD strategy for open source intelligence are displayed (National Defense Authorization Act for Fiscal Year 2006). These findings provide a base of the importance of OSINT as it relates to intelligence.

Cyber espionage or cyber spying is yet another method of cyber warfare. This method allows for the ability to obtain secrets without the permission of the data owner. The rise in cyber espionage is yet another reason governments must improve the cyber security infrastructure. With the freely available contents of the WWW providing intimate details about it users, this platform provides a way for individuals, groups, or nation states to take advantage of this rich information.

Cyber security is becoming the cornerstone of national security policies in many countries around the world as it is an interest to many stakeholders, including utilities, regulators, energy markets, government entities, and even those that wish to exploit the cyber infrastructure. Cyber warfare is quickly becoming the method of warfare and the tool of military strategists. Additionally, it is has become a tool for governments to aid or exploit for their own personal benefits. For cyber terrorists there has been an overwhelming abundance of new tools and technologies available that have allowed criminal acts to occur virtually anywhere in the world.

4.19 Open Source Intelligence and Tools

OSINT, which is one of several sub-intelligence collection disciplines, is intelligence collected from publicly available sources. Publicly available sources can be but are not limited to newspapers, magazines, industry newsletters, online forums, social media, and web queries. OSINT is the opposite of what is known to many as covert intelligence or intelligence gathered through classified means; however, OSINT does not mean that the information in the publicly available domain does not have a classified value. It only means that we all have access to it, but the associated labels of combined information still remain secret or tied to another unknown data classification per the associated agency.

OSS can be defined as software that is made available in source code form. This is important as this source code may fall under the General Public License (GPL) which is a widely used free software license that is managed under the GNU Not Linux (GNU) Project (Dawson et al, 2014). There are currently thousands of active projects on sites such as SourceForge that provide access to innovative tools that make OSINT techniques relatively painless. Chinese and Australian researchers have reviewed the many OSS applications available for data mining and published an extensive review discussing findings (Chen, et al, 2007). These researchers note issues such as usability, maintainability, and stability as an issue (Chen et al, 2007); however, OSS applications such as the R programming language, also identified as GNU S, has become one of the most powerful tools among statisticians in industry and academia. These tools can provide the ability to do data mining.

4.20 Geolocation

Twitter allows geolocation tags in Tweets through a geotagging feature in the Twitter API (Twitter). Twitter provides terms of Twitter's Developing policy regarding aggregation, caching, and storing of geographic information (Twitter, 2014); However, anyone that develops an application using this API can tweak items, which would provide even more granularity of its users. Even without modification of Tweets, simply adding the location will provide details such as neighborhood, city, state, or country. This publication information can be used to start an analysis. In iOS version 6.26+ and Android version 5.55+ precise location can be shared if elected to do so. Also, third party applications or websites may share precise Tweet locations as well.

Personal Twitter accounts provide the ability to associate a specific location with each tweet [See Figure 4.4]. This location over time can provide trends of locations visited with time/date stamps. This can be used to start developing a full analysis on Tweeting trends from particular locations, frequency of location visits, and content analysis through text mining.

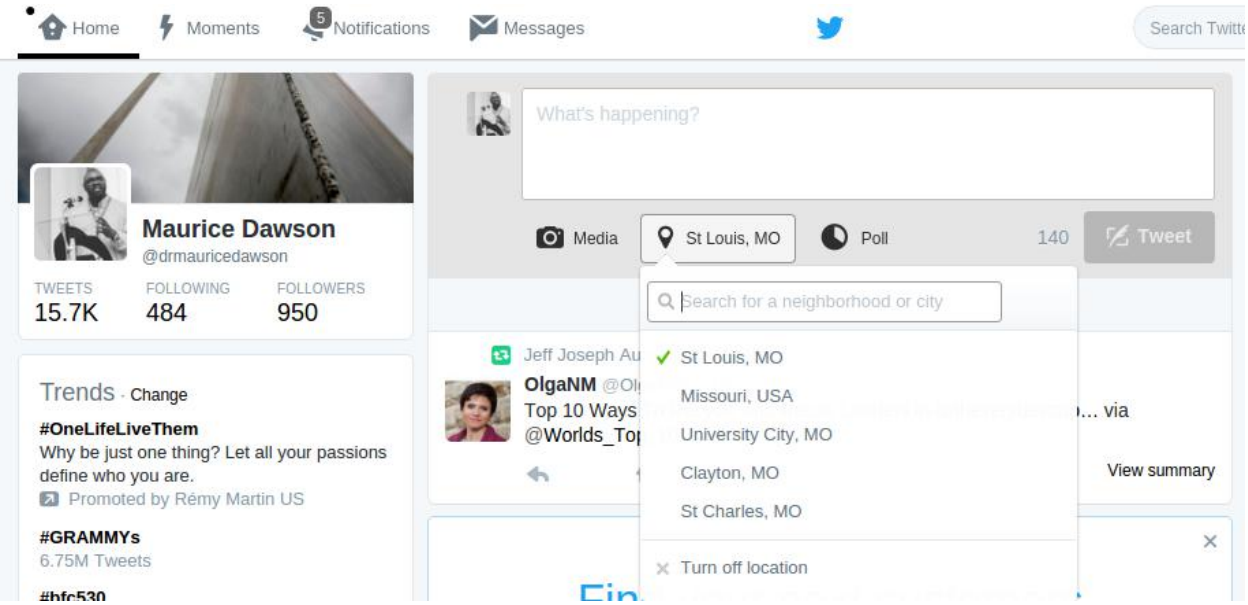


Figure 4.4: Twitter location example EXIF

EXIF data is a standard that specifies the formats for images, sounds, and ancillary tags used by digital cameras. The EXIF digital image standard specifies the following: the basic structure of digital image data files, tags and JPEG marker segments the standard uses, and how to define and manage format versions (Tešić, 2005). Research has been conducted on how to effectively extract EXIF data for prosecuting those involved in child pornography (Alvarex, 2004). Figure 4.5: Twitter Gambia photo example is the photo that was used with the selected application to extract data contained in the photo.

Figure 4.5: Twitter Gambia photo example

Extracting EXIF data using the ImageMagick application is rather simple in Debian based Linux OS. First the following command is ran: sudo apt-get install imagemagick. Then the following command is ran to extract the EXIF data: identify -verbose /usr/share/backgrounds/sample_exif.jpg | grep "exif:" The EXIF data output is displayed below [See Figure 4.6].

```
exif:ApertureValue: 128/32
exif:ColorSpace: 1
exif:ComponentsConfiguration: 1, 2, 3, 0
exif:CompressedBitsPerPixel: 3/1
exif:Compression: 6
exif:CustomRendered: 0
exif:DateTime: 2014:03:19 12:24:44
exif:DateTimeDigitized: 2014:03:19 12:24:44
exif:DateTimeOriginal: 2014:03:19 12:24:44
exif:DigitalZoomRatio: 3648/3648
exif:ExifImageLength: 1200
exif:ExifImageWidth: 1600
exif:ExifOffset: 240
exif:ExifVersion: 48, 50, 50, 49
exif:ExposureBiasValue: 0/3
exif:ExposureMode: 0
exif:ExposureTime: 1/1000
exif:FileSource: 3
exif:Flash: 16
exif:FlashPixVersion: 48, 49, 48, 48
exif:FNumber: 40/10
exif:FocalLength: 5000/1000
exif:FocalPlaneResolutionUnit: 2
exif:FocalPlaneXResolution: 1600000/241
exif:FocalPlaneYResolution: 1200000/181
exif:ImageDescription:
exif:InteroperabilityIndex: R98
exif:InteroperabilityOffset: 3244
exif:InteroperabilityVersion: 48, 49, 48, 48
exif:ISOSpeedRatings: 80
exif:JPEGInterchangeFormat: 5108
exif:JPEGInterchangeFormatLength: 3816
exif:Make: Canon
```

Figure 4.6: EXIF Data Output

The data that is provided includes date and time of photo taken, camera used, and other properties that allow for more detail analysis over time. There are more programs that allow viewing of

EXIF data than ImageMagick. This include applications that can be added to the Chrome browser and Firefox browser, as well as downloadable applications.

Google+, Twitter, Facebook and other social media sites allow for intelligence analysis of publicly shared data (Cleveland, Jackson, & Dawson, 2016). Understanding the personality traits as it relates to social engineering can provide a means of controlling this deception susceptibility. For example, an individual that continuously posts photos without removing geolocation tags is providing the information needed to create a pattern analysis over time. Figure 4.7 shows the types of data contained in a photo such as latitude, longitude, date, camera, lens, and more.

Figure 4.7: Instagram Photo EXIF Data Extraction

Knowing the camera and lens an individual could narrow down to the the make and model of a mobile device. With the date of the photo taken the mobile OS can be determined by release years associated with date. From here they can look up associated vulnerabilities or default settings that may allow them to exploit device features (Enck, Ongtang, & McDaniel, 2009). However, the mining of open source data can still provide valuable information that is captured in various state and federal databases. With the photo location, the GPS coordinates can be placed into an

interactive data mining tools to search for tweets to and from that location. Essentially, a listening system is created to search for network traffic with that specific location. Figure 4.8 shows a location with four searches for 100 meter, 250 meter, 500 meter, and 1000 meter circular ranges.

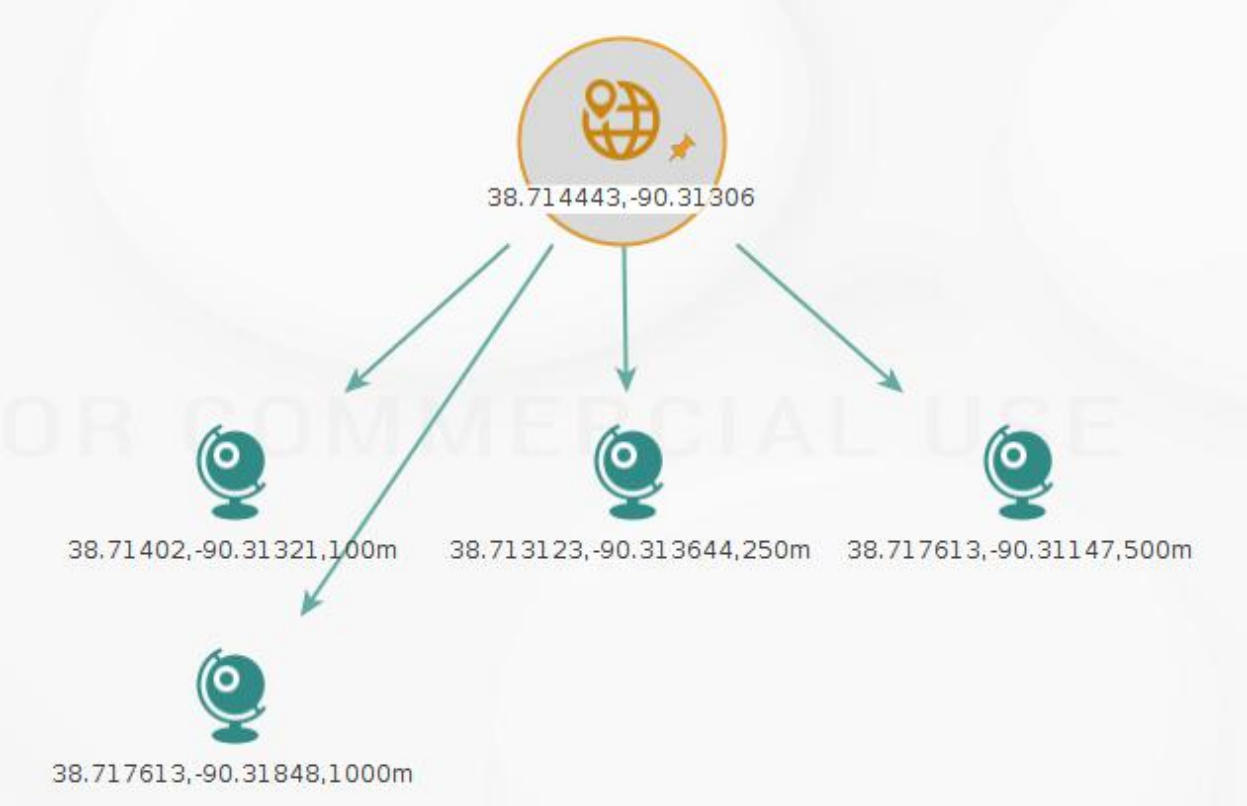


Figure 4.8: Geolocation From and To Tweet [Circular Area]

However, the mining of open source data can still provide valuable information that is captured in various state and federal databases. Thus, it is important that understanding how complex social engineering has become with the aid of technological tools for data mining, metadata extraction, and more.

4.21 Stenography

Tweets can contain photos that have compressed and encrypted embedded data. Data can be hidden in image and audio files, making it nearly impossible for institutions to look at files that could contain information that is geared towards radical, extremist, or terrorist ideologies. Researchers uncover the validity of tweets used by political organizations which can then be correlated to the use by nefarious organizations (Coddington, Molyneux, & Lawrence, 2014). This means that students, professors, or staff could be unknowingly retweeting images that can be used for communication propaganda or illicit instructions. Displayed in Figure 4.9 is an example of the extraction of a photo using Steghide where a simple text 123456 was embedded using the command steghide extract -sf pic.jpeg.

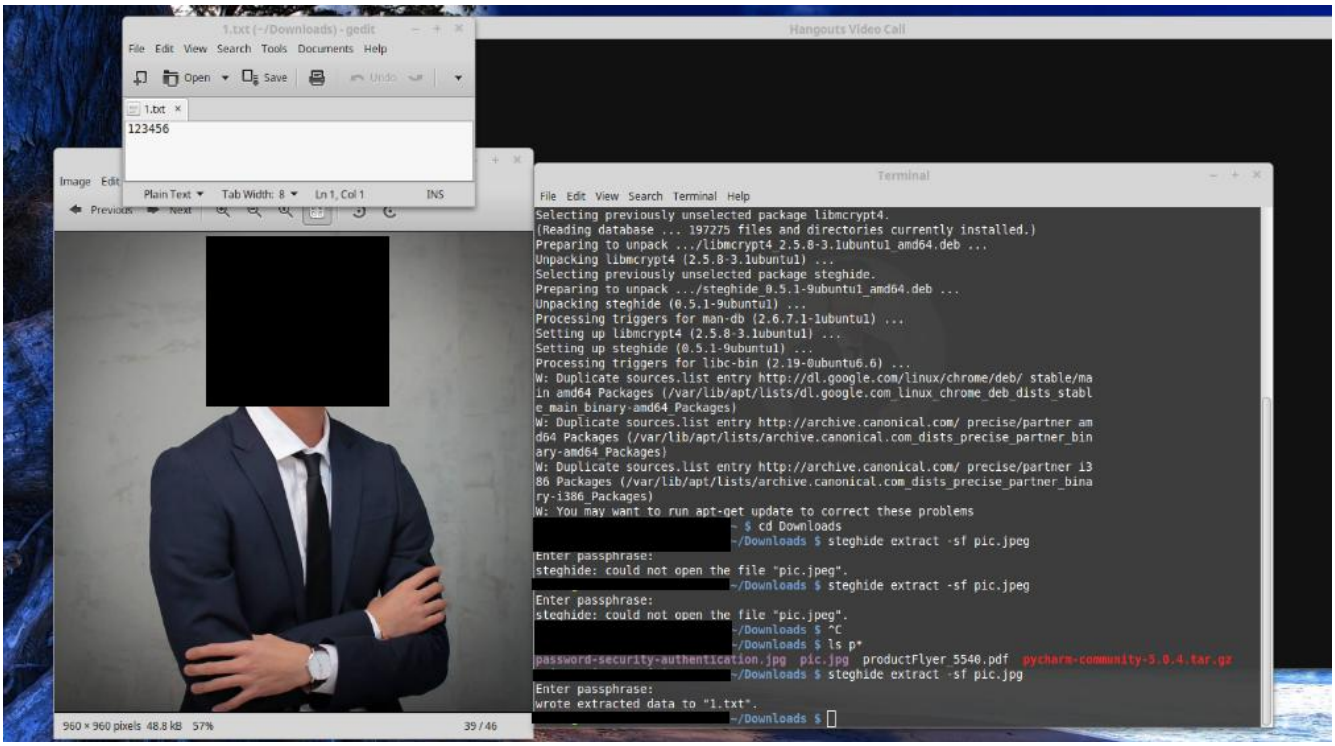


Figure 4.9: Steghide Stenography Example

4.22 Text Mining

The words contained in tweets provide another method of collecting intelligence through discovery of similar words, anomaly detection, and discussion tracking (Barry, 2004). Thus, conversations had with others in the forms of public replies can be further analyzed for patterns, keywords, and relationship discovery. Table 4.10: Open Source Mining Tools provides a list of software applications with their description and potential use.

Table 4.1: Open Source Mining Tools

Software Application	**Description and Potential Use**
R language	Language used for statistical computing and graphics.
Maltego	Program used to determine the relationships and real world links.
Rapid Miner	Program used for all steps of the data mining process including results visualization, validation, and optimization.
R Studio	IDE for R that allows for the use of R.
KNIME	Used for enterprise reporting, Business Intelligence (BI), data mining, data analysis, and text mining.
Python	High level, general purpose programming language.

4.23 Open Source Software Licensing

4.23a GNU GPL v3

After a review of the terms and conditions provided by this license, it appears to be more comprehensive in its requirements for use of the licensed software. It contains several more terms and appears to contain many more prohibitions that the previous version of the license terms contained. It contains the requirement to include appropriate notices for distribution of the code. It also contains specific prohibitions regarding restriction on the subsequent use of the code, including modified versions, by downstream users (Kumar, 2006).

4.23b GNU GPL v2

After review of the terms and conditions of this license, this version's license does not appear to have as many requirements and certainly is not as long as the newest version of this software's license appears to be. While considerably shorter than the subsequent version's license, this license does still maintain and include the requirement that appropriate notices accompany the distribution of the code (Kumar, 2006).

4.23c LGPLv3

After review of the terms and conditions of this license, this version's license does not appear to have as many requirements as either of the licenses under the GNUGPLv3 or v2, but it does maintain several requirements for compliance. Of note, this license includes an exception to the GNUGPL license, namely that the work produced under this license may be reproduced without compliance with Section 3 of the GNUGPL, which relates to Protecting Users' Legal Rights from Anti-Circumvention Law.

4.23d LGPL v2

After review of the terms and conditions of this license, this version's license appears to be somewhat longer than the terms and conditions of the subsequent version's license, but it appears to be closer to the GNUGPLv2's license terms than the LGPLv3's terms and conditions, and noticeably does not include the exception to the GNUGPL license as is contained in the subsequent version of this license.

4.23e LLGPL

After review of the Lisp Lesser General Public License (LLGPL), this version's license is like the LGPL but with a prequel. This prequel defines the effect in terms more typically used in Lisp programs. This license is grounded in the C programming language as the license specifically calls out functions not present in other languages that are not traditionally compiled (Greenbaum, 2013).

4.23f Creative Commons

After review of the terms and conditions of this license, it appears that this license is very similar to that of Modified BSD. It is interesting to note that the license begins by indicating that the company is not a law firm. Additionally, this license appears to include a waiver of copyrights and related rights, and a fallback in the event that the waiver is invalidated, which appears to be based upon the purpose of promoting the overall ideal of free culture. In addition, this license includes a limitation to make sure that neither patent nor trademark rights are being waived by this license.

4.23g Artistic License 2.0

After review of the terms and conditions of this license, this license appears to be very similar to that at issue in the Jacobsen case discussed above. Moreover, it appears that this license makes clear that the copyright holder intends to retain some creative control over the copyrighted work overall, while still trying to ensure that the copyrighted material remains as open and available to others as possible under the circumstances.

4.23h Modified BSD

After review of the terms and conditions of this license, these terms and conditions appear to be the shortest list of terms and conditions of all of the licenses reviewed in this paper. Additionally, this license appears to allow reproduction and modification of the copyrighted material provided certain conditions are met, which if subject to legal challenge, a court might construe as being subject to only protection as a contract, at best, and a bare license at worst. Moreover, based upon the legal authorities cited in this paper, it may be unclear whether this license will provide sufficient copyright protection.

4.23i Clear BSD License

After review of the terms and conditions of this license, this license appears to be very similar to the Modified BSD License, in that it is very short, and appears to allow reproduction only if certain conditions are met. This license does make clear that no patent rights are granted by this license.

4.24 Software Assurance

As malicious intent is an issue with OSS, it is important to deploy software security in the development lifecycle to ensure proper security posture (McGraw, 2004). To do this effectively while minimizing the effort for developing controls, organizations can adopt government cyber security controls from the NIST Special Publications (SP) 900 Series to include the DoD (Dawson Jr, Crespo, & Brewster, 2013). On April 26, 2010, the DoD released the third version of the Application Security and Development Security Technical Implementation Guide (STIG) provided by the Defense Information Systems Agency (DISA). This STIG can be used as a baseline for software configuration and development. DISA provides STIGs for other system components that can allow for full system hardening that will provide the OSS additional security through defense in depth. This process allows for AIC of the entire system.

In the event of a vulnerability being found within the OSS, the software code may require redesign and implementation. This iterative cycle is costly in time and resources. To truly understand security threats to a system, security must be addressed beginning with the initiation phase of the development process. For an organization, this means they must allow the IA controls and requirements to drive design and influence the software requirements. Therefore, any identified security threats found during the requirements and analysis phase will drive design requirements and implementation. Security defects discovered can then be addressed at a component level before implementation. The cost of discovery and mitigation can be absorbed within the review, analysis, and quality check performed during the design, and implementation of our SDLC. The resultant product is one with security built in rather than security retrofitted. Figure 4.10 displays the Secure-SDLC (S-SDLC) process in which OSS can be implemented into the development

process. For Agile or Scrum this process must be modified to be aligned with that specific design process.

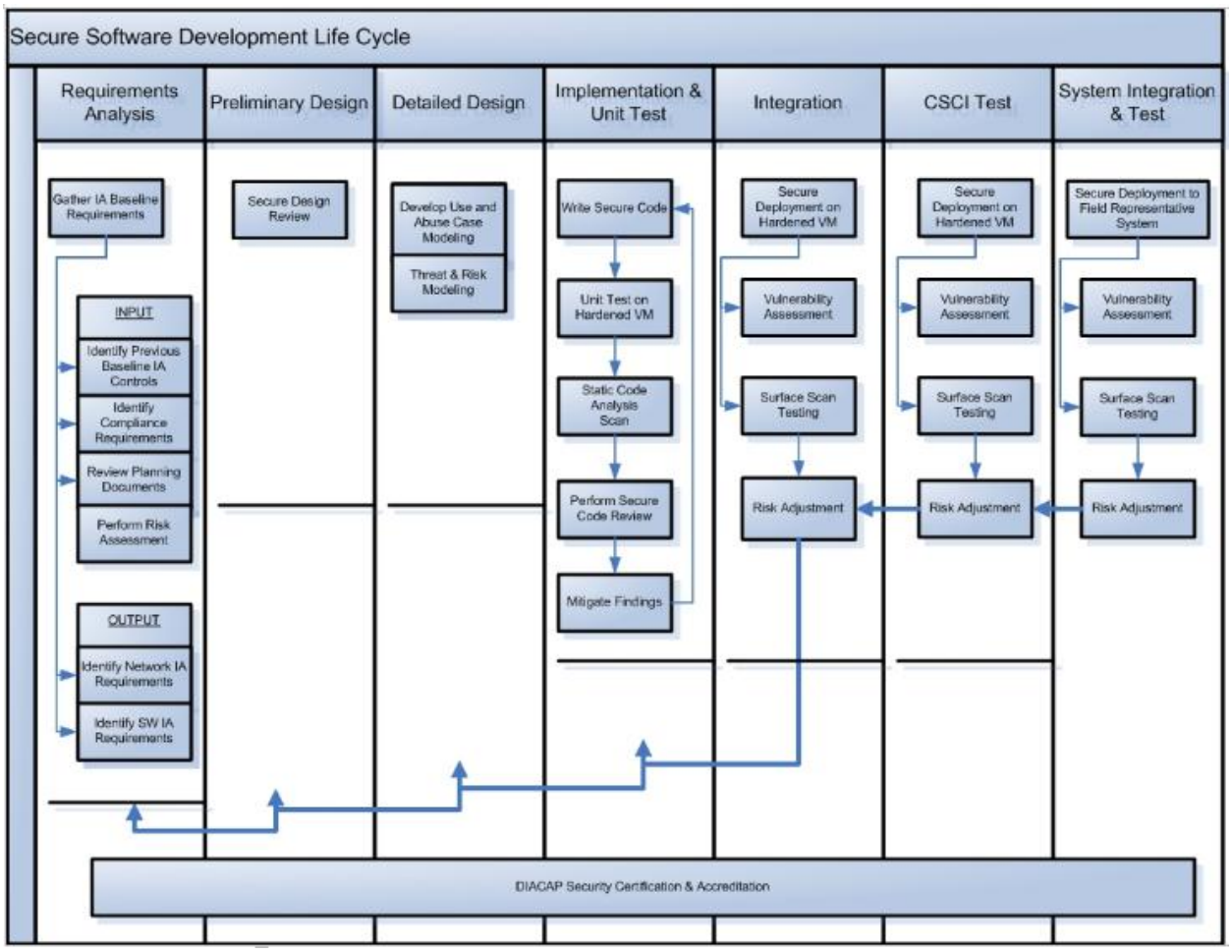


Figure 4.10: Industry Standard Secure Software Development Life Cycle Activities

4.25 Academic Contribution

Figure 4.11 below displays how connected devices need to follow policy and technology in order to ensure a hardened environment. This combines both technology and policy for the life-cycle of a product, use of a product, and creation of policies regarding technology usage.

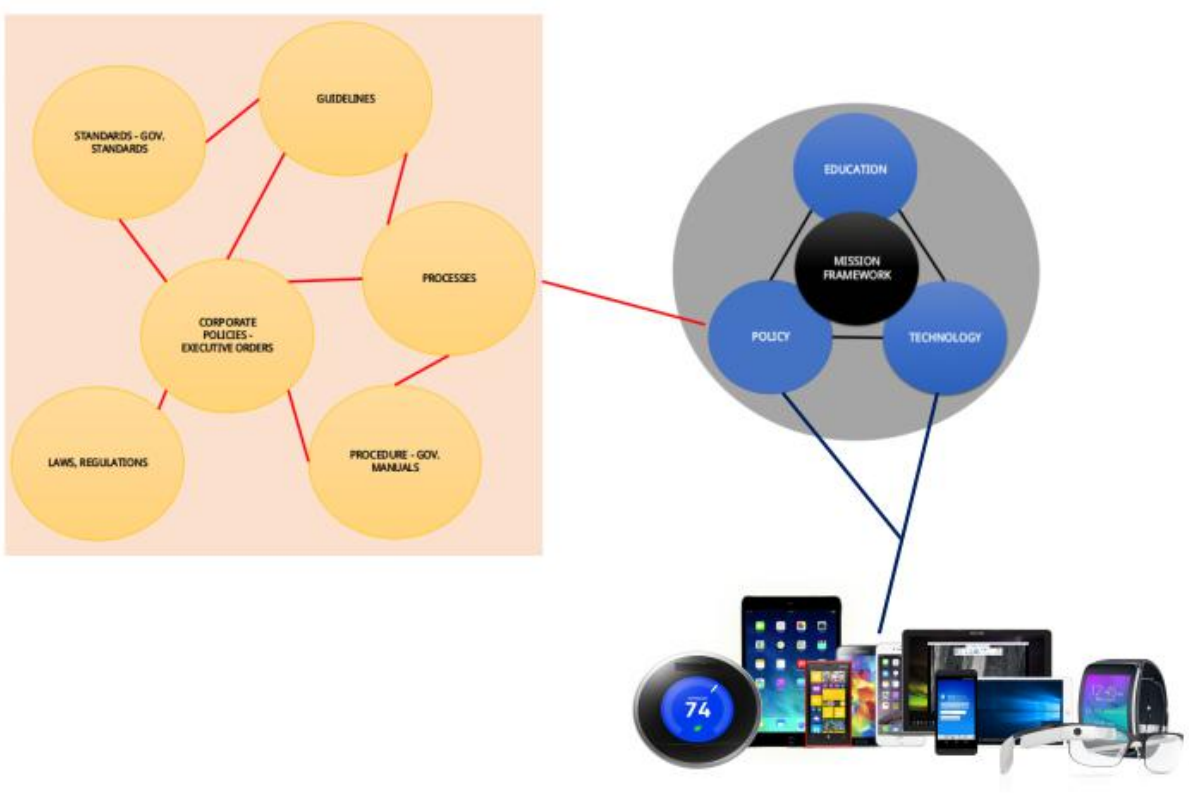


Figure 4.11: Mission Framework - Connected Devices

For a laptop, a script would be ran on the device that installs pre-approved applications, removes applications deemed a risk by the organization, and configures firewalls and anti-virus settings. This would include writing the results of the program to a .txt file that can read by the administrator later during an audit of the system.

Testing is integral to the software and systems lifecycle for development; however, there is guidance from NIST in the SP 800-15, but there is not truly something that addresses developing tests on commercial devices that provide an analysis that looks at risks. So, the need for the development of Built-In Test (BIT) like testing applications that allow users to set their level of

acceptable risk In Figure 4.12, shown is a testing process for multiple devices. In Steps 1a and 1b devices that decide to pair connect to the web in Steps 2a and 2b. During Step 3 is where a handshake is done. In Steps 4a and 4b the appropriate security measures are selected to allow the secure connection. In Step 4a an appropriate risk management framework is chosen with security controls being applied to the device. Step 4b looks at the CWE database, and uses the appropriate tests for the devices depending up applications discovered. Once tests have been satisfied Step 3 performs a handshake that allows devices to connect. Devices have the ability to perform checks as much as possible to remain securely attached. For this process to occur a software-based application will be on the devices that allows connectivity to the Internet. The risk management framework and CWE database get updated daily to ensure that the device owner understands the appropriate risk before deciding to connect or pair device ultimately.

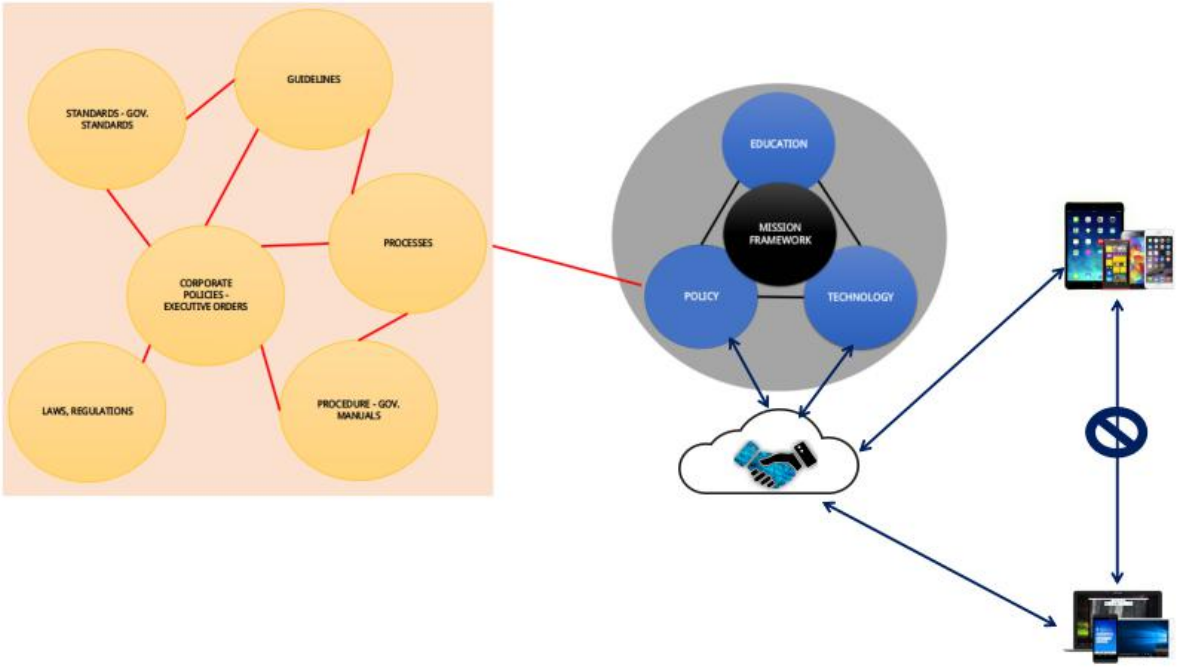


Figure 4.12: Mission Framework - Cyber Risk Management for Device Pairing

5.0 National and International Security Concerns in Africa

As the African continent has a significant number of emerging countries coupled with security issues, this is by far one of the best environments to test model and variants. As homeland security is becoming the cornerstone of multiple national security policies in many countries around the world as it is an interest to many stakeholders, including governments, utilities, regulators, energy markets, government entities, and even those that wish to exploit the critical infrastructure. The issues related to home security must first be addressed before providing the issues relating to cyber security. The African Union (AU) has released some press statements regarding matters dealing

with national security to the exploitation of natural resources (African Union Peace and Security, n.d.). Of these issues, the Somali originated group Al-Shabaab, and Nigerian originated group Boko Haram appear to be taking international headlines. The groups have continuously shaken the foundation for these countries. Also, these groups have expanded their reach to other neighboring states. Boko Haram has attacked not only Nigeria but Cameroon, Chad, Niger, and the Republic of Benin (Mantzikos, 2014). Their insurgency has cost more than 4,000 lives in the years of 2010 to 2014. Al-Shabaab is yet another result of a growing insurgency which is attracting global jihadists with shared ideology rather than ethnic or nationalist sentiments (Vidino, Pantucci, & Kohlmann, 2010).

The AU's African Peace and Security Architecture (APSA) has implemented the African Standby Force (ASF) to be divided into tasks with various regions. APSA provided the following recommendations: 1. clarify PSC relationship with panel, 2. enforce criteria for appointing PSC members, 3. improve synergy between PSC and other APSA components, 4. provide additional analysts for the CEWS and early warning, 5. provide joint training and skills development, 6. ensure connectivity between AUC and RECs, 7. increase and strengthen collaboration with other actors, and 8. increase flexibility and reliability of external support (Fisher, et al, 2010). Recommendations that cover the ASSF were the following: 1. adopt binding legal instrument with member states, 2. harmonize membership of standby arrangements, 3. improve staffing of PLANELMs at AU and RECs/RMs, 4. strengthen management of the ASF, 5. address logistics gap as priority, and 6. provide guidance and leadership for centers for excellence (Fisher, et al., &

2010).

5.1 Organisation for Economic Co-operation and Development

The Organisation for Economic Co-operation and Development (OECD) is an international economic organization that is comprised of 34 countries. OECD publishes reports, books, and other statistics that allow for further understanding of various markets. Key artifacts published are the OCED Economic Outlooks, Main Indicators, OECD Communications Outlook and the OECD Internet Economy Outlook (OECD, 2012). Significant amounts of reports are created for Kenya and Nigeria. These reports include economics, corruption indicators, and key events such as the Trans-Saharan gas pipeline which affects Nigeria significantly. This pipeline could pose a security issue as Nigeria is known for ongoing conflicts in the Niger Delta. The data contained within OECD can be mined, and literature analyzed to assist in making key strategic military decisions.

5.2 African Union

The AU, formally called Organization of African Unity (OAU), was founded in Cairo in the 29th Ordinary Session of the Assembly of Heads of State and Government of the organization that was held from the 28th to 30th of June 1993. The name of the union was changed from OAU to AU in May 2001. AU is a union of fifty-four countries in the African continent with its headquarters in Addis Ababa, Ethiopia. All the countries in Africa are members of the AU except Morocco due to the present status of the Western Sahara. The highest level decision-making body of the African Union is the AAU. The AAU is made up of all members of states and is currently headed by Robert Mugabe, the president of Zimbabwe.

The objectives of the AU include:

1. To defend the African territory and its member states.
2. Promote peace, security and unity among its member states.
3. To encourage and promote political and socio-economic cooperation among its member states.
4. To promote development in the African continent by encouraging research in all fields most especially in the areas of science and technology.
5. To eradicate and combat preventable disease and encourage the promotion of good health on the African continent.

5.3 Global Terrorism Database

University of Maryland's National Consortium of the Study of Terrorism and Responses to Terrorism retains an open source database on events from 1970 through 2014 (START, n.d.). START (n.d.) maintains the Global Terrorism Database (GTD) which includes more than 140,000 terrorist events. These events can be further examined to explore connections between people, places, and events. From the years 1975 to 2013, GTD reports 2482 incidents within Somalia with 446 incidents from 1973 to 2013 in Kenya. The Kenya events saw a huge increase starting in 2010 (START, n.d.). During those dates cities affected the most were Garissa, Ifo, Lami, Libooi, Likoni, Madio Gashi, and Mandera (START, n.d.). In the same time frame Nigeria has had 2251 incidents specifically during the years of 1991 to 2013. The spike in incidents occurs in the years of 2007 to 2013. Those responsible for the terrorist incidents in Nigeria are Boko Haram, Fulani Militants,

and other unknown identified groups. Some of the cities with fatalities of at least 15 are Kano, Gwoza, Bama, Jaji, Yelwa, Ife, Kautikiri, Fadama-Bona, Abulagu, Damboa Kampani, Maidurguri, Daku, Bantji, Shengev, Gajiram, Maikkadiri, Sangan Atakar, Kiyak, Musari, Ndongo, and Kuzen (START, n.d.). During the date of September 17, 2014, Konduga experienced 201 fatalities on a private citizen's property by armed assault. The armed attack included explosives, bombs, dynamite, and small arms (START, n.d.). Before that attack, there was another on September 12, 2014, and the results were 81 casualties due to a similar armed assault. In Ethiopia, Al-Shabaab is responsible for approximately 114 fatalities in the years of 2007-2014 (START, n.d.). The majority of the casualties caused in Ethiopia are due to violent political parties such as the Ethiopian People's Revolutionary Party, and the Tigray People's Liberation Front (TPLP). Together the groups have claimed more than 400 lives.

It is essential that you look at the number of casualties caused by terrorist groups to understand the deadliest organization. In reviewing the data from the Institute for Economics & Peace's Global Terrorism Database (GTD) another view is provided. Boko Haram has claimed a total of 6,644 lives while Isis claimed 6,073 [See Figure 5.1]. Looking at the Nigerian combined terrorist groups Boko Haram and Fulani Militants the total count is 7,873. The total casualty amount of three of the deadliest terror organizations on the continent of Africa is 8,894.

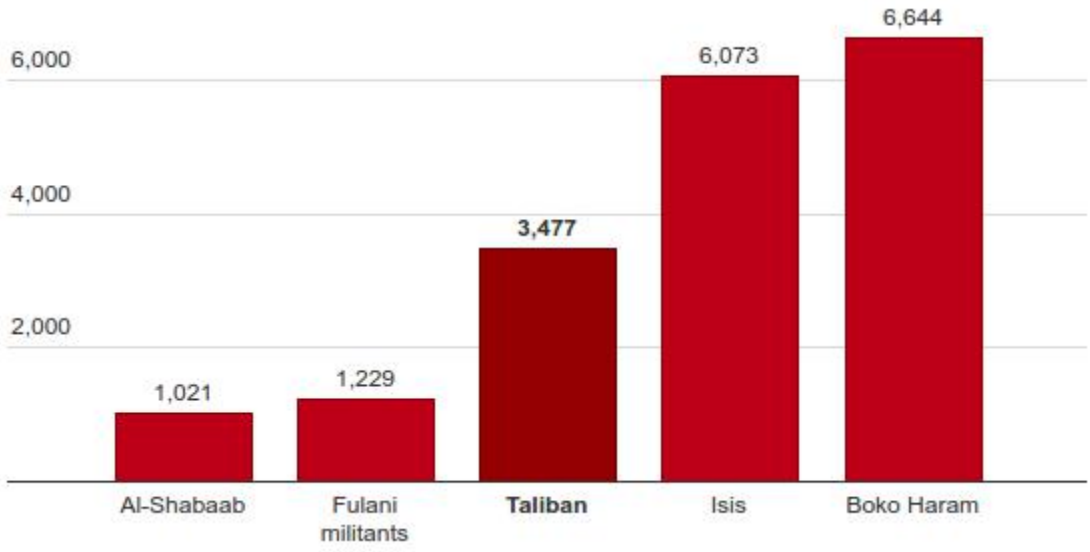


Figure 5.1: World's Deadliest Terror Organization (Source Institute for Economics & Peace, 2015)

In reviewing deaths that have occurred from 2013 - 2014, it is clear that Nigeria has the highest count at 5.662 with Iraq at 3,532, followed by Afghanistan at 1,391 [See Figure 5.2]. These deaths show how extreme the groups Boko Haram and Fulani Militants are in Nigeria and surrounding areas. The stability of this region is dependent upon neutralizing this threat which has claimed so many lives in a short period.

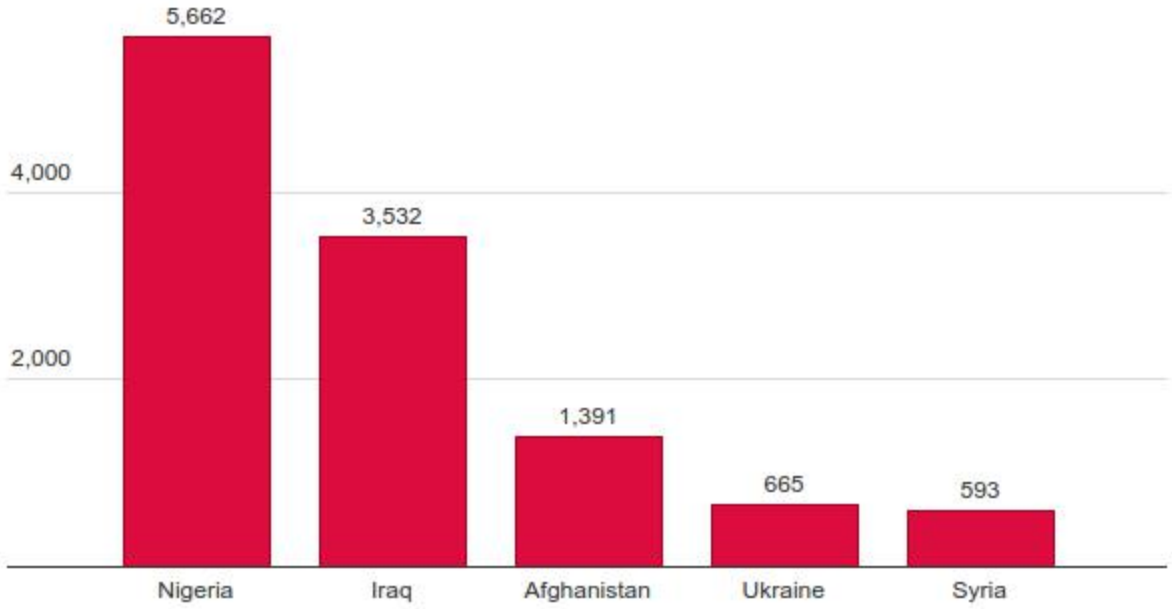


Figure 5.2: 2013-2014 Deaths (Source Institute for Economics & Peace, 2015)

The major themes discussed in this research can be applied to combat terrorism on the African continent. The use of OSINT and cyber intelligence applications can allow for data to be mined from terrorists. Provided in Figure 5.3 is a representation of a social media analysis through Maltego relative to the search term of "Al-Qaeda". The output of this function provided specific Twitter accounts that have some relation to Al-Qaeda based off each Twitter account's name and/or tweeting patterns. Further analysis was conducted on each of these Twitter accounts by performing a function that generated all the tweets for each Twitter account. In addition to this, sentiment analysis was performed on each of these tweets to determine whether or not the tweets for each of these Twitter users were positive, negative, or neutral. As shown, many of the tweets have different sentiment values, including positive, negative, and neutral.

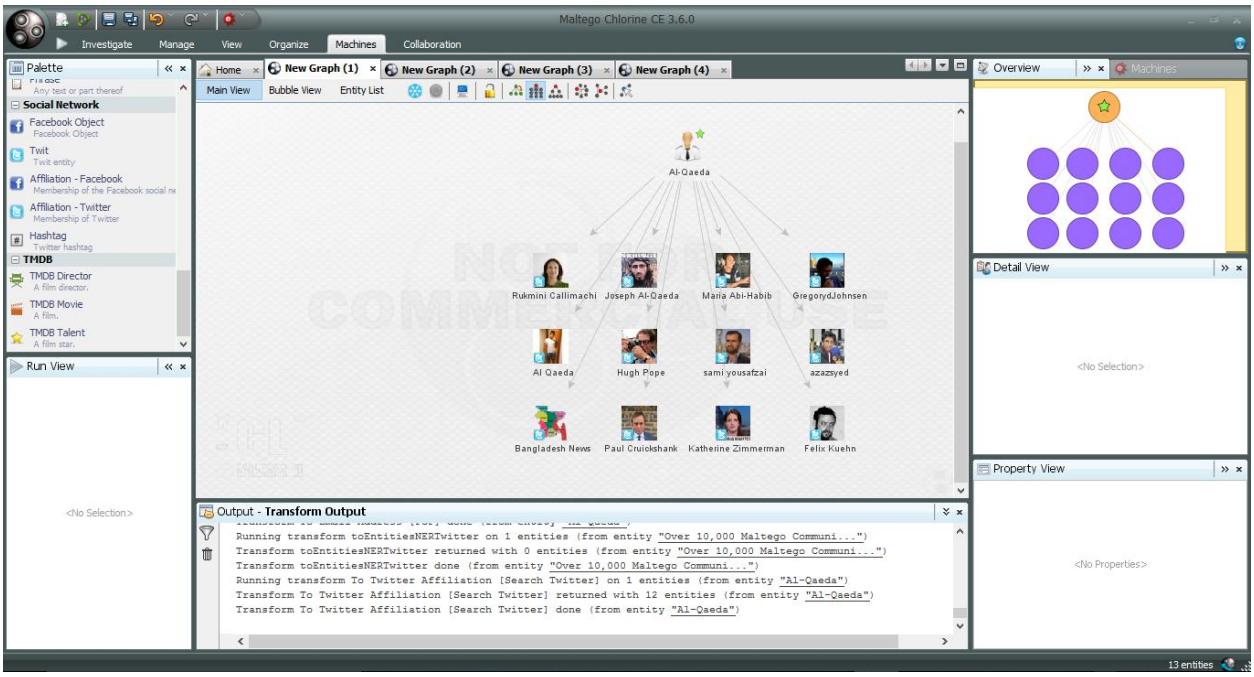


Figure 5.3: Al-Qaeda Maltego Social Media Analysis

Figure 5.4 shows the result of a search on the terrorist group "Boko Haram". This application allows a search on any entity that mentions Boko Haram, whether positive or negative, for further analysis. Additionally, transforms can continually be running to review the lowest level detail of a tweet that can be retweeted. This application serves as an ability to look at all links present.

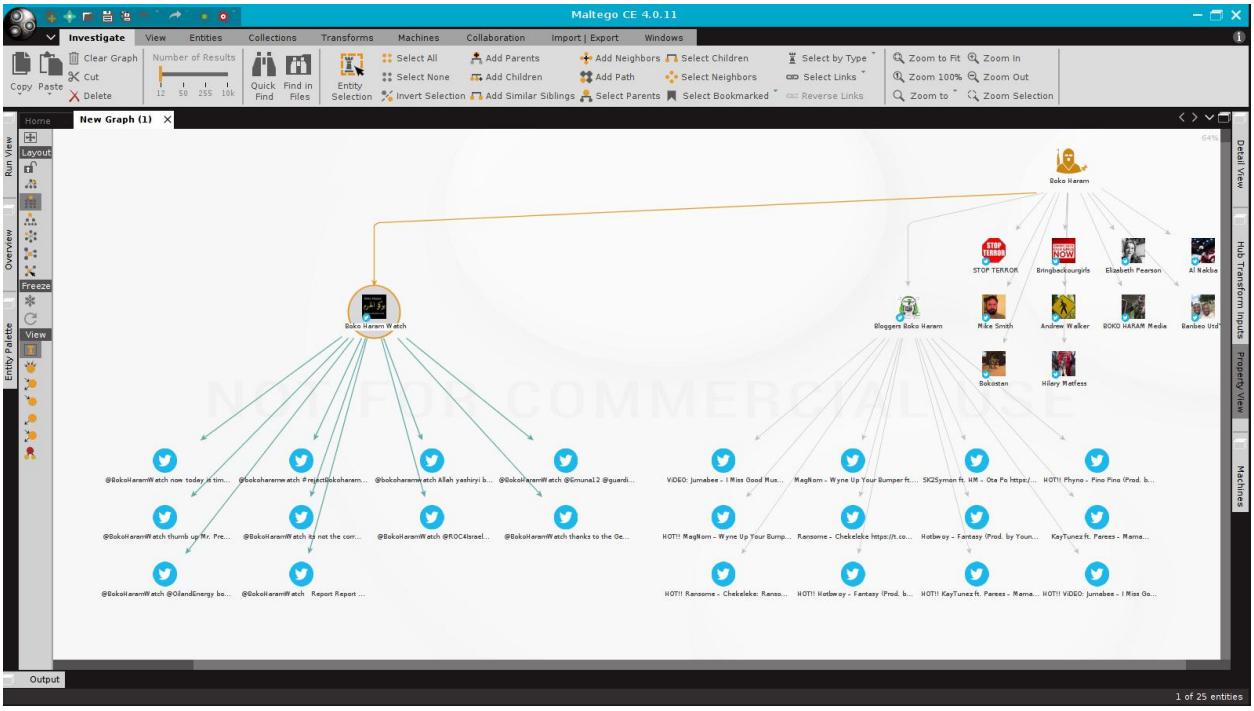


Figure 5.4: Boko Haram Maltego Social Media Analysis

This is important as terrorist groups are using the Internet to recruit and carry out other forms of propaganda to support their agenda. Also, running hash on files such as images will allow subjects the ability to see if there is embedded text in the file that is encrypted.

In the member nations of the AU there is no common cyber security curriculum or even country governance for cyber security education. Some of the countries that have the most advanced cyber security education programs are South Africa, Kenya, Nigeria, Egypt, and Ghana. However, none of these countries have a national cyber security or homeland security program to address the growing issues related to national security. Due to the constraints such as ability to devote resources for nationalized training, technology costs, attracting and retaining top talent can serve as a blueprint for cyber security and education initiatives. The literature detailed in the theme for education could allow countries to address this by using ubiquitous learning objects, virtual labs, virtual machines, and OSS applications.

With the AU focusing efforts now on homeland security, the policies that should govern cyber security are nonexistent. Countries such as Gambia recently published a Request For Proposal (RFP) to create a national CERT center. Kenya is struggling to pass laws on Internet governance, and Nigeria is slowly capturing those that commit the infamous 419 scams. And of those caught, only a small number are prosecuted. The policies created by NIST, DoD, and other organizations could be used as a baseline for policy development. For example, the RMF could serve as a method to manage cyber risks and set cyber security controls for organizations. These baselines provide a method for organizations to harden their systems, especially as the AU is looking at easing immigration within the continent.

5.4 Security Issues in AU

The AU is a relatively new organization in comparison to the European Union (EU). The AU came into existence in 2001 while the EU first signed treaty was in 1957 establishing the European Economic Community (EEC). The AU predecessor, OAU was founded in 1963 but the focus was eliminating colonialism and promoting solidarity between countries in Africa. This gap of years means there is lack of experience among physical security, economic collaboration, and more. The other issue is in the population size, number of members, and land size. The EU has a population over 500,000 while the AU has approximately 1.2 billion. Some organizations have estimated that population on the African continent could quadruple in the next 100 years. As Africa plans to remove borders, security has to be to addressed so that physical security includes national security. With home to three of the top five terrorist organizations, infamous Internet scams, and two well known narco states, the African continent has to address these challenges (Dawson, Lieble, & Adeboje, 2017; Dawson & Adeboje, 2016). With a failed attempt to deal with the Darfur issue, and aftermath of the Arab Spring.

The intelligence documents that were leaked provide information regarding an assassination attempt on an African Union Commission (AUC) chairperson (Al Jazeera, 2015). Other leaked secret documents show issues relating to South Africa's IT infrastructure for government, inability to control conflict regions, and more. Another big issue surrounds the actual physical security regarding Very Important People (VIP) such as high ranking members of government (USA Today, 2011). And with various AU regions looking to integrate further with technical infrastructure the laws governing the current technology are outdated.

5.5 Shadow Wars

Through unofficial released leaked documents various news agencies state that they reveal that the AFRICOM could be conducting up to a 100 missions per day with drone bases in several countries located throughout the continent. The French are located in a number of former colonized countries under the banner of providing security and humanitarian support (Gregory, 2000; Hansen, 2008). The development of a Chinese base on the continent, making it the first permanent base overseas, is yet another reason why a cyber war is eminent (Jacobs & Perlez, 2017). With the rush for resources coupled with the advances in technology there is a need stronger than ever to ensure that the cyber domain is protected as it may serve an Achilles heel in years to come.

6.0 Prior Output Mapping

The intention of the published works is to show the contribution of knowledge through the writings of the three themes and the effect on a national and international security. Table 6.1. Prior Output Relationship to Themes displays the works as they relate to specific themes.

Table 6.1: Prior Output Relationship to Themes

PUBLICATION	THEME [T] TECHNOLOGY [E] EDUCATION [P] POLICY	SYMNOPSIS/ABSTRACT
Dawson, M. (2016). Exploring Secure Computing for the Internet of Things, Internet of Everything, Web of Things, and Hyperconnectivity. In M. Dawson, M. Eltayeb, & M. Omar (Eds.) *Security Solutions or Hyperconnectivity and the Internet of Things* (pp. 1-12). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0741-3.ch001	[T]	Secure computing is essential as environments continue to become intertwined and hyperconnected. As the IoT, WoT, and the Internet of Everything (IoE) dominate the landscape of technological platforms, protecting these complicated networks is important. The everyday person who wishes to have more devices that allow for the ability to be connected needs to be aware of what threats they could be potentially exposing themselves to. Additionally, the unknowing consumer of everyday products needs to be aware of what it means to have sensors, RFID, Bluetooth, and WiFi enabled products. This submission explores how AIC can be applied to IoT, WoT, and IoE with consideration for the application of these architectures in the defense sector.
Davis, L., Dawson, M., &Omar, M. (2016). Systems Engineering Concepts with Aid of Virtual Worlds and Open Source Software: Using Technology to Develop Learning Objects and Simulation Environments. In F. Neto, R. de Souza, & A.Gomes (Eds.)Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning (pp. 483-509). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0125-1.ch020	[T][E]	Technology is changing the landscape of learning and teaching in America. The use of virtual worlds enable engineering and technology programs to implement software programs such as Second Life and Open Simulator to enhance what they may already have. Additionally, virtual worlds can add a more dynamic environment in the online classroom for multiple platforms such as the Personal Computer (PC), wearables, and mobile devices. The purpose of this chapter is to provide a review of these programs to include how to implement these items into an engineering course. Further detailed in this submission is how to incorporate IEEE documentation and other engineering guidelines into the projects. Included in this chapter is a detailed layout of a simulated environment as well as various approaches of structuring and organization for classroom activities.
Dawson, M., Omar, M., Abramson, J., Leonard, B., & Bessette, D. (2016). Battlefield Cyberspace: Exploitation of Hyperconnectivity and Internet o	[T][P]	The threat of cyber terrorism has become a reality with recent attacks such as Stuxtnet, Flame, Sony Pictures, and North Korea's websites. As the IoT continues to become more hyperconnected it will be imperative that cyber security

f Things. In M. Dawson, D. Kisku , P. Gupta, J. Sing, & W. Li (Eds.) *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 204-235). Hershey, PA: InformationScience Reference. doi:10.4018/978-1-5225-0703-1.ch010		experts develop new security architectures for multiple platforms such as mobile devices, laptops, embedded systems, and even wearable displays. The future of national and international security rely on complex countermeasures to ensure that a proper security posture is maintained during this state of hyperconnectivity. To protect these systems from exploitation of vulnerabilities, it is essential to understand current and future threats to include the laws that drive their need to be secured. The potential security related threats with the use of social media, mobile devices, virtual worlds, augmented reality, and mixed reality are examined within this chapter.
Dawson, M., & Adeboje, W. (2016). Islamic Extremists in Africa: Security Spotlight on Kenya and Nigeria. In M.Dawson, D. Kisku, P. Gupta, J. Sing, & W. Li (Eds.) *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 93-103). Hershey, PA : Information Science Reference. doi:10.4018/978-1-5225-0703-1.ch005	[P]	Security is a growing concern on the African continent as the Regional Economic Communities (REC) move toward economic integration. Furthermore, these regions collectively make up the AU which has an objective to promote peace, security, and stability on the African continent. In recent years, Africa has been plagued with political uprisings, civil wars, extremists, corrupt politicians, and the battle for natural resources. In particular, Kenya and Nigeria are facing Islamic extremists that threaten the foundation of multiple nations. Both countries are using military force to combat these threats. This chapter provides insight into these West and East African nations and their means to provide security assurances to their citizens.
Dawson, M. (2016). *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT).* doi:10.4018/IJHIoT	[T][E][P]	*The International Journal of Hyperconnectivity and the Internet of Things* (IJHIoT) promotes innovative, interesting and rigorously developed conceptual and empirical contributions and encourages theory based multi- or inter-disciplinary research. This journal covers topics relating to IoT and the current age of hyperconnectivity including security concerns, applications of IoT, development and management of the IoT, wearable computing, IoT for home automation, smart cities, and other environments.
Dawson, M., Eltayeb, M., & Omar, M. (2016). Security Solutions for Hyperconnectivity and the Internet of Things (pp. 1-347). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0741-3	[T][P]	The Internet of Things describes a world in which smart technologies enable objects with a network to communicate with each other and interface with humans effortlessly. This connected world of convenience and technology does not come without its drawbacks, as interconnectivity implies hackability. Security Solutions for Hyperconnectivity and the Internet of Things offers insights from cutting-edge research about the strategies and techniques that can be implemented to protect against cyber-attacks. This book calls for revolutionary protection strategies to reassess security, and is an essential resource for programmers, engineers, business professionals, researchers, and advanced students in relevant fields.
Dawson, M., Kisku, D. R.,Gupta, P., Sing, J. K., & Li, W. (2016). Developing Next-Generation Countermeasures for Homeland Security Threat Prevention (pp. 1-428). Her	[T][E][P]	In the modern world, natural disasters are becoming more commonplace, unmanned systems are becoming the norm, and terrorism and espionage are increasingly taking place online. All of these threats have made it necessary for governments and organizations to steel themselves against these threats in innovative ways. Developing Next-Generation Countermeasures for Homeland

shey, PA: IGI Global. doi:10.4018/978-1-5225-0703-1		Security Threat Prevention provides relevant theoretical frameworks and empirical research outlining potential threats while exploring their appropriate countermeasures. This relevant publication takes a broad perspective, from network security, surveillance, reconnaissance, and physical security; all topics are considered with equal weight. This book is ideal for policy makers, IT professionals, engineers, NGO operators, and graduate students; it provides an in-depth look into the threats facing modern society and the methods to avoid them.
Dawson, M., DeWalt, B., & Cleveland, S. (2016). The Case for UBUNTU Linux Operating System Performance and Usability for Use in Higher Education in a Virtualized Environment.	[T][E]	The use of Linux based OS in the classroom is increasing, but there is little research to address usability differences between Windows and Linux based OSs. Moreover, studies related to the ability for students to navigate effectively between Ubuntu 14.04 Long Term Support (LTS) and Windows 8 OSs are scant. This research aims to bridge the gap between modern Linux and Windows Oss, as the former represents a viable alternative to eliminate licensing costs for educational institutions. Preliminary findings, based on the analysis of the System Usability Scale results from a sample of 14 students, demonstrated that Ubuntu users did not require technical support to use the system; the majority found little inconsistency in the system and regarded it as well integrated.
Dawson, M., & Omar, M.(2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 1-368). Hershey, PA: IGI Global. doi: 10.4018/978-1-4666-8345-7	[T][E][P]	Technological advances, although beneficial and progressive, can lead to vulnerabilities in system networks and security. While researchers attempt to find solutions, negative uses of technology continue to create new security threats to users. New Threats and Countermeasures in Digital Crime and Cyber Terrorism bring together research-based chapters and case studies on security techniques and current methods being used to identify and overcome technological vulnerabilities with an emphasis on security issues in mobile computing and online activities. This book is an essential reference source for researchers, university academics, computing professionals, and upper-level students interested in the techniques, laws, and training initiatives currently being implemented and adapted for secure computing.
Dawson, M. (2015). A Brief Review of New Threats and Countermeasures in Digital Crime andCyber Terrorism. In M. Dawson, & M. Omar (Eds.)*New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 1-7). Hershey, PA: InformationScience Reference. doi:10.4018/978-1-4666-8345-7.ch001	[T][P]	Cyber security is becoming the cornerstone of national security policies in many countries around the world as it is an interest to many stakeholders, including utilities, regulators, energy markets, government entities, and even those who wish to exploit the cyber infrastructure. Cyber warfare is quickly becoming the method of warfare and the tool of military strategists. Additionally, it is has become a tool for governments to aid or exploit for their own personal benefits. For cyber terrorists, there has been an overwhelming abundance of new tools and technologies available that have allowed criminal acts to occur virtually anywhere in the world. This chapter discusses emerging laws, policies, processes, and tools that are changing the landscape of cyber security. This chapter provides an overview of the research to follow which will provide an in-depth review of mobile security, mobile networks, insider threats, and various special topics in cyber security.
Dawson, M., Wright, J., & Omar, M. (2015). Mobile Devices: Th	[T][P]	Mobile devices are becoming a method to provide an efficient and convenient way to access, find, and share information;

e Case for Cyber Security Hardened Systems. In M. Dawson, & M. Omar (Eds.) *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 8-29). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8345-7.ch002		however, the availability of this information has caused an increase in cyber attacks. Currently, cyber threats range from Trojans and viruses to botnets and toolkits. Presently, 96% of mobile devices do not have pre-installed security software while approximately 65% of the vulnerabilities are found within the application layer. This lack in security and policy driven systems is an opportunity for malicious cyber attackers to hack into the various popular devices. Traditional security software found in desktop computing platforms, such as firewalls, antivirus, and encryption, is widely used by the general public in mobile devices. Moreover, mobile devices are even more vulnerable than personal desktop computers because more people are using mobile devices to do personal tasks. This review attempts to display the importance of developing a national security policy created for mobile devices to protect sensitive and confidential data.
Leonard, B., & Dawson, M. (2015). Legal Issues: Security and Privacy with Mobile Devices. In M. Dawson, & M. Omar (Eds.) *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 95-104). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8345-7.ch006	[T][P]	Privacy and security are two items being woven into the fabric of American law concerning mobile devices. This chapter will review and analyze the associated laws and policies that are currently in place or have been proposed to ensure proper execution of security measures for mobile and other devices while still protecting individual privacy. This chapter addresses the fact that as the American society significantly uses mobile devices, it is imperative to understand the legal actions surrounding these technologies to include their associated uses. This chapter will also address the fact that with 9/11 in the not so distant past, cyber security has become a forefront subject in the battle against global terrorism. Furthermore, this chapter will examine how mobile devices are not like the devices of the past because the computing power is on par with that of some desktops and these devices have the ability to execute malicious applications. In addition, this chapter discusses the reality, significance, legal, and practical effects of the fact that suspicious programs are being executed offensively and security based attacks can be performed as well with the use of programs such as Kali Linux running on Android.
Dawson, M., Leonard, B., & Rahim, E. (2015). Advances in Technology Project Management: Review of Open Source Software Integration. In M. Wadhwa, & A. Harper (Eds.) *Technology, Innovation, and Enterprise Transformation* (pp. 313-324). Hershey, PA: Business Science Reference. doi:10.4018/978-1-4666-6473-9.ch016	[T][P]	As organizations must continually drive down costs of software-driven projects, they need to evaluate the Systems Development Life Cycle (SDLC) and other software-based design methodologies. These methodologies include looking at software-based alternatives that could save a significant amount of money by reducing the amount of proprietary software. This chapter explores the use and integration of OSS in software-driven projects to include enterprise organizations. Additionally, the legalities of the GNU General Public License (GPL), Lesser General Public License (LGPL), Berkeley Software Distribution (BSD), and Creative Commons are explored with the integration of these OSS solutions into organizations. Lastly, the chapter covers the software assurance and cyber security controls to associate with OSS to deploy a hardened product that meets the needs of today's dynamically evolving global business enterprise.
Dawson, M., Omar, M., & Abram	[T][E][P]	Cyber security has become a matter of national, international,

son, J. (2015). Understanding the Methods behind Cyber Terrorism . In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Scie nce and Technology, Third Editio n* (pp. 1539-1549). Hershey, PA: I nformation Science Reference. doi:10.4018/9 78-1-4666-5888-2.ch147		economic, and societal importance that affects multiple nations (Walker, 2012). Since the 1990s users have exploited vulnerabilities to gain access to networks for malicious purposes. In recent years, the number of attacks on U.S. networks has continued to grow at an exponential rate. This includes malicious embedded code, exploitation of backdoors, and more. These attacks can be initiated from anywhere in the world from behind a computer with a masked Internet Protocol (IP) address. This type of warfare, cyber warfare, changes the landscape of war itself (Beidleman, 2009). This type of warfare removes the need to have a physically capable military and requires the demand for a force that has a strong technical capacity, e.g. computer science skills. The U.S. and other countries have come to understand that this is an issue and have developed policies to handle this in an effort to mitigate the threats. In Estonia and Georgia there were direct attacks on government cyber infrastructure (Beildleman, 2009). The attacks in Estonia rendered the government's infrastructure useless. The government and other associated entities heavily relied upon this e-government infrastructure. These attacks helped lead to the development of cyber defense organizations within Europe.
Dawson, M., Omar, M., Abra mson, J., & Bessette, D. (2014). T he Future of National and International Security on the Inter net. In A. Kayem, & C. Meinel (E ds.) *Information Security in Di verse Computing Environment s* (pp. 149- 178). Hershey, PA: Informati on Science Reference. doi:10.4018/9 78-1-4666-6158-5.ch009	[T][E][P]	Hyperconnectivity is a growing trend that is driving cyber security experts to develop new security architectures for multiple platforms such as mobile devices, laptops, and even wearable displays. The future of national and international security rely on complex countermeasures to ensure that a proper security posture is maintained during this state of hyperconnectivity. To protect these systems from exploitation of vulnerabilities it is essential to understand current and future threats to include the laws that drive their need to be secured. The potential security-related threats with the use of social media, mobile devices, virtual worlds, augmented reality, and mixed reality are examined within this chapter. Further reviewed are some examples of the complex attacks that could interrupt human-robot interaction, children-computer interaction, mobile computing, social networks, and human-centered issues in security design.
Dawson, M., Al Saeed, I., Wright, J., & Onyegbula, F. (2014). Ope n Source Software to Enhance the STEM Learning Environme nt. In V. Wang(Ed.), *Handbook of* *Research on Education and Tech nology in a Changing Society* (pp. 569-580). Hershey, PA: Inf ormation Science Reference. d oi:10.4018/978-1-4666-6046-5.ch 042	[T][E]	This chapter examines the use of OSS technologies that can be used to improve the learning of STEM. The various methods that can be utilized to improve the percentage of STEM majors in the American educational system with resources such as: Open Source as Alternative (OSALT), virtualization, cloud computing, Linux distributions, open source programming, and open source hardware platforms are explored. Increasing the amount of students who pursue STEM majors is important because the projected job growth in the STEM field compared to non-STEM jobs is 33%. OSALT provides cost-effective alternatives to commercial products such as Microsoft Office Suite and Adobe Photoshop. Second, creating VMs is another avenue to teach complex concepts in computer science, engineering, and Information Technology (IT). Third, cloud

		computing is an inexpensive way for clients to access information from multiple locations and devices. Fourth, universities can use the OS Linux and its various distributions as replacements for commercial operating systems like Windows in order to reduce IT costs. Lastly, open source programming languages like Python and their associated Integrated Development Environments (IDEs) provide comprehensive facilities for software engineers for application development or testing.
Dawson Jr, M. E., Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secur e automated information systems. *International Journal of Business Continuity and Risk Management*, *4*(1), 1-22.	[T][P]	AIC is a key theme everywhere as cyber security has become more than an emerging topic. The DoD has implemented multiple processes such as the Department of Defense information assurance certification and accreditation process (DIACAP), common criteria (CC), and has created proven baselines to include IA controls to protect information system (IS) resources. The aim of this research study shall provide insight to the applicable processes, IA controls, and standards to include providing a method for selecting necessary government models and for system development.
Dawson, M. E., & Al Saeed, I. (2012). Use of Open Source Software and Virtualizati on in Academia to Enhance Higher Education Every-where. C*utting-edge Technologi es in Higher Education*, *6*, 283-31 3.	[T][E]	As costs for education continue to rise around the world, institutions must become innovative in the ways they teach and grow students. To do this effectively, professors and administrative staff should push toward the utilization of OSS and virtual tools to enhance or supplement currently available tools. In developing countries, OSS applications would allow students the ability to learn critical technological skills for success at a fraction of the cost. OSS also provides faculty members the ability to dissect source code and prepare students for low-level software development. It is critical that all institutions look at alternatives in providing training and delivering educational material regardless of limitations going forward as the world continues to be more global due to the increased use of technologies everywhere. Doing this could provide a means of shortening the education gap in many countries. Reviewing the available technology, possible implementations of these technologies, and the application of these items in graduate coursework could provide a starting point in integrating these tools into academia. When administrators or faculty debate the possibilities of OSS, gaming, and simulation tools, this applied research provides a guide for changing the ability to develop students that will be competitive on a global level.
Dawson, M., & Rahim, E(2011). Transitional leadership in the defense and aerospace industry: A critical analysis for recruiting and developing talent.*International Journal of Project Organisati on and Management*, *3*(2), 16 4-183.	[P]	This article proposes a framework to create effective transitional leadership in the defense and aerospace industries. The proposed framework identifies and maps traits and skills of military personnel in a manner that can be tested and validated in accordance with principles of human resource management. Applying this framework would assist hiring managers in their selection of program or project managers from the military in transition to a defense contractor support organization. Employing a research approach embracing a mix of both qualitative and quantitative strategies, the study examined more than 50 respondents to a 34-question survey, focusing on 14 respondents who submitted fully completed

		surveys. The conceptual framework for this study is derived from investigations conducted by project management practitioners and scholars who have built upon previous research, which studied project development models within various industries.
Dawson, M., Burrell, D. N., Rahim, E., & Brewster, S. (2010). Integrating Software Assurance into the Software Development Life Cycle (SDLC). *Journal of Information Systems Technology and Planning*, *3*(6), 49-53.	[T][P]	This article examines the integration of secure coding practices into the overall Software Development Life Cycle (SDLC). Also detailed is a proposed methodology for integrating software assurance into the DIACAP. This method for integrating software assurance helps in properly securing the application layer as that is where more than half of the vulnerabilities lie in a system.
Dawson, M., Burrell, D. N., Rahim, E., & Brewster, S. (2010). EXAMINING THE ROLE OF THE CHIEF INFORMATION SECURITY OFFICER (CISO) & SECURITY PLAN.*Journal of Information Systems Technology & Planning*,*3*(6).	[T][P]	The Chief Information Security Officer (CISO) is an emerging role in many organizations as cyber security continues to be on the minds of many executives. As the number of vulnerabilities and attacks on large enterprise systems continue to rise there must be an identified key leader with full responsibility: thus understanding the role and need of the CISO is essential to all organizations that have any technological footprint. One of the most important artifacts from a CISO is the security plan which provides an organization its direction in terms of providing availability, integrity, confidentiality, non-repudiation, and authentication.
Dawson, M., Lieble, M., & Adeboje, A. (2017). Open Source Intelligence: Performing Data Mining and Link Analysis to Track Terrorist Activities. In *Information Technology-New Generations* (pp. 159-163). Springer, Cham.	[T]	The increasing rates of terrorism in Africa is a growing concern globally, and the realization of such dreadful circumstances demonstrates the need to disclose who is behind such terrible acts. Terrorists and extremist organizations have been known to use social media, and other forms of Internet-enabled technologies to spread idealism. Analyzing this data could provide valuable information regarding terrorist activity with the use of OSINT tools. This study attempts to review the applications and methods that could be used to expose extremist Internet behavior.
Cardenas-Haro, J. A., & Dawson, M. (2016). Tails Linux Operating System: The Amnesiac Incognito System in Times of High Surveillance, Its Security Flaws, Limitations, and Strengths in the Fight for Democracy. In M. Dawson, M. Eltayeb, & M. Omar (Eds.), *Security Solutions for Hyperconnectivity and the Internet of Things* (pp. 260-271). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0741-3.ch010	[T][P]	After the information released by Edward Snowden, the world realized about the security risks of high surveillance from governments to citizens or among governments, and how it can affect the freedom, democracy and/or peace. Research has been carried out for the creation of the necessary tools for the countermeasures to all this surveillance. One of the more powerful tools is the Tails system as a complement of TOR. Even though there are limitations and flaws, the progress has been significant and we are moving in the right direction.
Dawson, M., & Cárdenas-Haro, J. A. (2017). Tails Linux Operating System: Remaining Anonymous	[T][P]	After the information released by Edward Snowden, the world realized about the security risks of high surveillance from

with the Assistance of an Incognito System in Times of High Surveillance. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, 1(1), 47-55. doi:10.4018/IJHIoT.2017010104		governments to citizens or among governments, and how it can affect the freedom, democracy, and peace. And organizations such as WikiLeaks has shown just how much data is collected to include the poor security controls in place to protect that information. Research has been carried out for the creation of the necessary tools for the countermeasures to all these surveillance. One of the most potent tools is the Tails system as a complement of TOR. Even though there are limitations and flaws, the progress has been significant, and we are moving in the right direction. As more individuals and organizations fall under a watchful eye on their Internet activities then maintaining anonymity it not only essential for getting out information but one's safety.
Dawson, Maurice, Sharon L. Burton, Dustin Bessette and Jorja Wright. "Massive Open Online Courses and Integrating Open Source Technology and Open Access Literature Into Technology-Based Degrees." *Encyclopedia of Information Science and Technology*, Fourth Edition. IGI Global, 2018. 7898-7911. Web. 8 Aug. 2017. doi:10.4018/978-1-5225-2255-3.ch687	[T][E][P]	Massive Open Online Courses (MOOCs) are a new phenomenon of course delivery for students, faculty, and administrators to use. As this technology continues to grow in the short term it is essential to develop a method in which OSS, open source technologies, and open access literature can be incorporated to strengthen the MOOC environment. Strengthening the MOOC environment can be used as a method to increase retention as well as increase enrollment in higher education. As STEM programs are going online it is imperative that the tools meet the demands of today's marketplace. This chapter provides insights on these open technology solutions so that current and future MOOCs can be enhanced with little to no cost added.
Dawson, M. (2017). Cyber Security Policies for Hyperconnectivity and Internet of Things: A Process for Managing Connectivity. In *Information Technology-New Generations* (pp. 911-914). Springer, Cham.	[T][P]	Hyperconnectivity and Internet of Things are changing the landscape of Information Technology (IT). Architectures are becoming more sophisticated while cyber security is slowing adapting to this shift of Internet-enabled technologies in automotive, industrial, consumer, and networking. This slow adoption of proper security controls, defenses, and aggressive measures is leaving individuals vulnerable. This submission explores how policies can be created that automate the process of device connectivity, and how current frameworks can be used to minimize system risks.

7.0 Conclusion

This research explored three key elements in hyperconnectivity in cyber security which are 1. education, 2. policy, and 3. technologies. The literature on these subjects and specifically on these three main themes showed a relation of these areas and how to shape cyber security. Described in this research was the interconnection of these three key elements and how they shape one another.

7.1 Summary of Thesis

The thesis has introduced an innovative way of looking at cyber security through a framework that ties education, policy, and technologies together. The education review provided insight on innovative ways to teach cyber security coursework to include discussing the accrediting bodies for programs related to IT, computing technologies, or computer science. Further reviewed were the policies, tools, and techniques that can be brought forward in cyber security education. Concepts such as simulation, U-Learning, virtualization, and engineering standards were explored. The policy section reviewed multiple directives, standards, mandates, laws, and best practices. These included policies form the DoD, NIST, United States military, and more. These provided the baseline for further guidance and direction for organizations setting policies. The technologies portion brought in data about emerging technologies such as those that include Internet enabled devices. Mobile phones, OSs, software, and other devices were reviewed as it relates to cyber security.

Design science, case study, and other research methods for understanding cyber security were explored through the public works. The application of these three elements can be used to drive

polices for the DoD and for the commercial sector that create a long-lasting effect in the battle against cyber-crime. This collective research argues that education, policies, and technologies are essential in the holistic view of cyber security. Previous viewpoints have researched these items in silos rather than capturing them as a whole; however, this research aimed to bring these themes together. The intention of the published works was to show the contribution of knowledge through the writings of the three themes and the effect it has on a broader audience. It is the sincere hope of the author that this thesis represents a valuable and useful addition to the existing body of work within security.

7.2 Future Work

Future work shall be implementing the mission framework for a developing nation so that they may establish a robust cyber security program. This initiative will be used to collect and analyze data from all participants including participating organizations. Once a framework is established for a particular country then a regional framework will be established that allows member countries in that region or economic partnership to participate. This section present two major projects..

Project 1: Cyber Security in Dominican Republic

The Dominican Republic National Police several years back created a unit focused on cyber crime; however, they are struggling with multiple challenges. These challenges range from the inability to acquire talent, and properly train the talent they have. Skills such as being able to run proprietary security software is readily available, but the ability to review malware isn't. Thus, the detailed cyber crimes involving complex skillsets are not present. This means that this country is

easily a target as they continue to move forward with initiatives such as solar panels, and other items relating to critical infrastructure. This project will require the participation of major universities in Santo Domingo, and Santiago. Once this has been completed and has resulted in a framework for this country then another country will adopt framework that is in this region.

Project 2: Development of Cyber Warfare Workforce

Cyber warfare is the war of today and the future; however, in countries such as the U.S., there is a significant shortage of talent. The developed framework will be adapted for addressing this matter and then capturing data over a long period on its success. This will be tested in a metropolitan region, and then provided to the body that specializes on cyber security accreditation in the U.S.

Additionally, the future work shall be focused on making an active engagement to the NSA CAE in shaping cyber security accreditation, and curriculum in U.S. The commitment will not be limited to the U.S. as others governments will receive information regarding using the model and replicating results. More dynamic development and enhancements to virtual learning environments that adapt based upon changes native to that country. When a new policy is created, the simulated environment will be modified based upon given guidance. The published outputs shall serve as a foundation for related research that affects one of the themes contained in this literature. The development of more inclusive models and detailed processes will allow for the growth of handling this changing world of hyperconnectivity.

8.0 References

African Union, Peace and Security (n.d.). Ending conflicts, sustaining peace - African Union - Peace and Security Department. Retrieved December 15, 2015, from http://www.peaceau.org/en/

Ahlemann, F., Teuteberg, F., & Vogelsang, K. (2009). Project management standards–Diffusion and application in Germany and Switzerland. *International Journal of Project Management*, *27*(3), 292-303.

Al Jazeera. (2015, February 25). Spy cables reveal African Union assassination threat. Retrieved August 07, 2017, from http://www.aljazeera.com/news/2015/02/spy-cables-reveal-african-union-assassination-threat-au-ssa-south-africa-150224142310003.html

Alvarez, P. (2004). Using extended file information (EXIF) file headers in digital evidence analysis. *International Journal of Digital Evidence*, 2(3), 1-5.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.

Barrera, D., & Van Oorschot, P. (2011). Secure software installation on smartphones. *IEEE Security and Privacy, 9*(3), 42-48. Retrieved June 26, 2012.

Becher, M., Freiling, F., & Leider, B. (2007). On the effort to create smartphone worms in Windows Mobile. Proceedings of the 2007 IEEE workshop on Information Assurance. United States Military Academy. West Point, NY. Retrieved March 22, 2013, from http://pil.informatik.uni-mannheim.de/filepool/publications/on-the-effort-to-create-smartphone-worms-in-windows-mobile.pdf.

Beidleman, S. W. (2009). Defining and deterring cyber war. Barracks, PA Army War College. Retrieved March I0, 2013, from http://www.hsdl.org/?abstract&doc=ll8653&coll=limited.

Berry, M. W. (2004). Survey of text mining. *Computing Reviews*, 45(9), 548.

Bellovin, S. M., & Housley, R. (2005, June). Guidelines for cryptographic key management. In *Symposium on Research in Security and Privacy*.

Bhattacharya, D. (2008). Leadership styles and information security in small businesses: An empirical investigation (Doctoral dissertation, University of Phoenix). Retrieved March 9, 2013, from www.phoenix.edu/apololibrary

Bullock, J., Haddow, G., Coppola, D., &Yeletaysi, S. (2009). Introduction to homeland security: Principles of all-hazards response (3rd ed.). Burlington, MA: Elsevier Inc.

Bose, A. (2008). Propagation, detection and containment of mobile malware. (Doctoral dissertation, University of Michigan). Retrieved March 11, 2013, from www.phoenix.edu/apololibrary.

Bradley, J., Barbier, J., & Handler, D. (2013). Embracing the Internet of everything to capture your share of $14.4 trillion. *White Paper, Cisco*.

Brock, J., Boltz, J., Doring, E., & Gilmore, M. (1999). Information security risk assessment practices of leading organizations. Director, USGAO [online] http://www. gao. gov/special. pubs/ai00033. pdf (accessed 20 March 2009)

Brown, B. (2009). Beyond Downadup: Security expert worries about smart phone, TinyURL threats: Malware writers just waiting for financial incentive to strike, F-Secure exec warns. Retrieved March 20,2013, from http://business.highbeam.com/409220/article-1G1-214585913/beyond-downadup-security expert-worries-smart-phone.

Boss, S., & Krauss, J. (2014). *Reinventing Project-Based Learning: Your Field Guide to Real-World Projects in the Digital Age*. Eugene, OR: International Society for Technology in Education.

Cardenas-Haro, J. A., & Dawson, M. (2017). Tails Linux Operating System: The Amnesiac Incognito System in Times of High Surveillance, Its Security Flaws, Limitations, and Strengths in the Fight for Democracy. In M. Dawson, M. Eltayeb, & M. Omar (Eds.), *Security Solutions for Hyperconnectivity and the Internet of Things* (pp. 260-271). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0741-3.ch010

Caddy, T. (2011). FIPS 140-2. In *Encyclopedia of Cryptography and Security* (pp. 468-471). Springer US.

Clarke, D. (2010). *Africa: Crude Continent: The Struggle for Africa's Oil Prize*. Profile books.

Cleveland, S., Jackson, B. C., & Dawson, M. (2016). Microblogging in higher education: Digital Natives, knowledge creation, social engineering, and intelligence analysis of educational tweets. E-Learning and Digital Media, 13(1-2), 62-80.

Cobb, S. (2006). Risks and response: Issues and attitudes. Retrieved June 1, 2012 from https://norwich.angellearning.com/AngelUploads/Content/MSIA_LOR/ _assoc/msia_s4/msia_ s4_w02_2_comm/msia_s4_w02_cobb_lecture.pdf .

Cobb, S. (2007). Risk analysis example. Retrieved March 20, 2009 from https://norwich.angellearning.com/ AngelUploads/Content/MSIA_LOR/_assoc/msia_s4/

msia_s4_w02_2_comm/msia_s4_w02_co bb_lecture.pdf.

Coddington, M., Molyneux, L., & Lawrence, R. G. (2014). Fact checking the campaign how political reporters use Twitter to set the record straight (or not). *The International Journal of Press/Politics*, *19*(4), 391-409.

Common Criteria Evaluation and Validation Scheme (CCEVS) (2008). Common criteria evaluation and validation scheme -- organization, management, and concept of operations (Version 2.0), National Security Agency, National Information Assurance Partnership website [online] http://www.niap-ccevs.org/policy/ccevs/scheme-pub-1.pdf (accessed 20 March 2012).

Dawson, M., & Adeboje, W. (2017). Islamic Extremists in Africa: Security Spotlight on Kenya and Nigeria. In M. Dawson, D. Kisku, P. Gupta, J. Sing, & W. Li (Eds.), *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 93-103). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0703-1.ch005

Dawson, M. E., & Al Saeed, I. (2012). Use of open source software and virtualization in academia to enhance higher education everywhere. *Cutting-edge Technologies in Higher Education*, *6*, 283-313.

Dawson, M., Al Saeed, I., Wright, J., & Onyegbula, F. (2015). Open source software to enhance the STEM learning environment. In *Open Source Technology: Concepts, Methodologies, Tools, and Applications* (pp. 1493-1503). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-7230-7.ch075

Dawson, M., & Cárdenas-Haro, J. A. (2017). Tails Linux Operating System: Remaining anonymous with the assistance of an incognito system in times of high surveillance. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, 1(1), 47-55. doi:10.4018/IJHIoT.2017010104

Dawson Jr, M. E., Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*(1), 1-22.

Dawson, M., Lieble, M., & Adeboje, A. (2017). Open Source Intelligence: Performing data mining and link analysis to track terrorist activities. In *Information Technology-New Generations* (pp. 159-163). Springer, Cham.

Dawson, M., & Omar, M. (2015). New threats and countermeasures in digital crime and cyber terrorism (pp. 1-368). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7

Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the methods behind cyber terrorism. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1539-1549). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-5888-2.ch147

Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). The future of national and international security on the internet. In A. Kayem, & C. Meinel (Eds.) *Information Security in Diverse Computing Environments* (pp. 149-178). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-6158-5.ch009

Dawson, M., Wright, J., & Omar, M. (2016). Mobile devices: The case for cyber security hardened systems. In *Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications* (pp. 1103-1123). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8751-6.ch047

Denning, D. E. (2012). Stuxnet: What has changed? *Future Internet*, 4(3), 672-687.

Department of Defense (DoD) (2007) Dod information assurance certification and accreditation process (DIACAP) (DoDI 8510.01), Assistant Secretary of Defense for Networks and Information Integration, Department of Defense Chief Information Officer [online] http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf (accessed 18 April 2012).

Department of Education. (2014, July 3). [Post-Secondary University Survey 2013]. Unpublished raw data. https://inventory.data.gov/dataset/032e19b4-5a90-41dc-83ff-6e4cd234f565/resource/3862c3d-5388-4c16-a30f-d105432553a4

Department of Energy (2002). Vulnerability assessment methodology. Retrieved June 1, 2012 from http://www.esisac.com/publicdocs/assessment_methods/VA.pdf .

Department of the Navy (2005). Department of the Navy information assurance program (SECNAV M-5239.1), The Department of Navy Chief Information Officer, Department of Navy Retrieved March 20, 2012 from http://doni.daps.dla.mil/secnav manuals1/5239.1.pdf .

Disaster Recovery Journal (2009) Glossary [online] http://www.drj.com/index.php?option=com_glossary&func=display&letter=All&Itemid=297&catid=35&page=1 (accessed 2 April 2009)

Dodson-Edgars, D. (2002). Due care in security management. Retrieved June 1, 2012, from http://www.bizforum.org/ whitepapers/dodson-edgars-2.htm .

Durán, E. B., Álvarez, M. M., & Únzaga, S. I. (2014, April). Ontological model-driven architecture for ubiquitous learning applications. In *Proceedings of the 7th Euro American Conference on Telematics and Information Systems* (p. 14). ACM.

Enck, W., Ongtang, M., & McDaniel, P. (2009). Understanding android security. IEEE security & privacy, 7(1), 50-57.

Evans, D. (2012). The internet of everything: How more relevant and valuable connections will change the world. *Cisco IBSG*, 1-9.

Fisher, L. M., Bah, A. S., Mniema, A., Okome, H. N., Tamba, M., Frederiksen, J., Abdelaziz, A. & Reeve, R. (2010). African peace and security architecture (apsa): 2010 assessment study. *Zanzibar (Tanzania)*.

Gartner. (2014, August 11). Gartner's 2014 Hype Cycle for Emerging Technologies maps the journey to digital business. Retrieved February 28, 2016, from http://www.gartner.com/newsroom/id/2819918

Gregory, S. (2000). The French military in Africa: Past and present. African Affairs, 99(396), 435-448.

Hansen, A. (2008). The French Military in Africa. *New York: Council on Foreign Relations*.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660.

Guinard, D. (2011). *A Web of Things application architecture-Integrating the real-world into the web* (Doctoral dissertation, ETH Zurich). Retrieved from?

Guinard, D., & Trifa, V. (2009, April). Towards the web of things: Web mashups for embedded devices. In *Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 2009), in proceedings of WWW (International World Wide Web Conferences), Madrid, Spain* (p. 15).

Glotzbach, R., Mordkovich, D., & Radwan, J. (2008). Syndicated RSS feeds for course information distribution. *Journal of Information Technology Education: Research*, 7(1), 163-183.

Harris, S., & Meyers, M. (2002). *CISSP*. McGraw-Hill/Osborne.

Hawker, J. S. (2009). A software process engineering course. In Proc. 2009 *American Society Engineering Education Annual Conference*. 25-31.

Jacobs, A., & Perlez, J. (2017, February 25). U.S. wary of its new neighbor in Djibouti: A Chinese Naval base. Retrieved August 08, 2017, from https://www.nytimes.com/2017/02/25/world/africa/us-djibouti-chinese-naval-base.html

Johnson, L., Levine, A., & Smith, R. (2009). The 2009 Horizon report. One year or less: Cloud computing.

IEEE Computer Society. Software Engineering Standards Committee, & IEEE-SA Standards Board. (1998). IEEE Recommended Practice for Software Requirements Specifications. Institute of Electrical and Electronics Engineers.

IEEE Standards Association. (1998). IEEE Std 1062–1998 IEEE Recommended Practice for Software Acquisition.

IEEE Standards Coordinating Committee. (1990). IEEE Standard Glossary of Software Engineering Terminology (IEEE Std 610.12-1990). Los Alamitos. *CA: IEEE Computer Society*.

Institute for Economics & Peace. (2015). Global terrorism index. Retrieved March 17, 2016, from http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf

International Telecommunication Union., Telecommunication Standardization Sector of ITU. (2012). ITU-T recommendation Y.2060: Series Y: Global information infrastructure, internet protocol aspects and next-generation networks: Frameworks and functional architecture models: Overview of the Internet of Things. Geneva: International Telecommunication Union.

International Telecommunication Union., Telecommunication Standardization Sector of ITU. (2012). ITU-T recommendation Y.2063: Series Y: Global information infrastructure, internet protocol aspects and next-generation networks: Frameworks and functional architecture models: Framework of the Web of Things. Geneva: International Telecommunication Union.

International Telecommunication Union., Telecommunication Standardization Sector of ITU. (2012). ITU-T recommendation Y.2069: Series Y: Global information infrastructure, internet protocol aspects and next-generation networks: Frameworks and functional architecture models: Terms and definitions for the Internet of Things. Geneva: International Telecommunication Union.

Jones, V., & Jo, J. H. (2004, December). Ubiquitous learning environment: An adaptive teaching system using ubiquitous technology. In *Beyond the comfort zone: Proceedings of the 21st ASCILITE Conference* (Vol. 468, p. 474).

Kirk, J. (2012). Pacemaker hack can deliver deadly 830-volt jolt. *Computerworld*, *17*.

Kortjan, N. (2013). A cyber security awareness and education framework for South Africa.

Kundra, V. (2010). State of Public Sector Cloud Computing. CIO Council. Retrieved from http://www.cio.gov/pages.cfm/page/State-of-Public-Sector-Cloud-Computing-HHS

Lee, J. W., Jung, S. H., Park, S. C., Lee, Y. J., & Jang, Y. C. (2005, August). System based SQA and implementation of SPI for successful projects. In *Information Reuse and Integration, Conference, 2005. IRI-2005 IEEE International Conference on.* (pp. 494-499). IEEE.

Lockefeer, L. (2010). *Encrypted SMS, an analysis of the theoretical necessities and implementation possibilities*. Retrieved from http://www.cs.ru.nl

LTSC. (2000a). *Learning technology standards committee website*. Available: http://ltsc.ieee.org/

LTSC. (2000b). IEEE standards board: Project authorization request (PAR) form [On-line]. Available: https://ieee-sa.centraldesktop.com/ltsc/

Mantzikos, I. (2014). Boko Haram Attacks in Nigeria and Neighboring Countries: A Chronology of Attacks. *Perspectives on Terrorism*, 8(6).

Marshall, G., & Ruohonen, M. (Eds.). (1998). *Capacity Building for IT in Education in Developing Countries: IFIP TC3 WG3. 1, 3.4 & 3.5*. Working Conference on Capacity Building for IT in Education in Developing Countries 19–25 August 1997, Harare, Zimbabwe. Springer Science & Business Media

Martinez-Maldonado, R., Dimitriadis, Y., Clayphan, A., Muñoz-Cristóbal, J. A., Prieto, L. P., Rodríguez-Triana, M. J., & Kay, J. (2013, November). Integrating orchestration of ubiquitous and pervasive learning environments. In*Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration* (pp. 189-192). ACM.

Martínez-Costa, M., Choi, T. Y., Martínez, J. A., & Martínez-Lorente, A. R. (2009). ISO 9000/1994, ISO 9001/2000 and TQM: the performance debate revisited. *Journal of Operations Management*, *27*(6), 495-511.

McGraw, G. (2004). Software security. *Security & Privacy, IEEE*, 2(2), 80-83.

McNulty, L. (2005, October). Preparing for implementation: Professional certification under DOD directive 8570.1. In *Military Communications Conference*, 2005. MILCOM 2005. IEEE (pp. 1485-1487). IEEE.

Mehlman, M., Lin, P., & Abney, K. (2013). Enhanced warfighters: Risk, ethics, and policy. *Case Legal Studies Research Paper*, (2013-2).

Möller, D. P., Haas, R., & Vakilzadian, H. (2013, July). Ubiquitous learning: Teaching modeling and simulation with technology. In *Proceedings of the 2013 Grand Challenges on Modeling and Simulation Conference* (p. 24). Society for Modeling & Simulation International.

Moore, J. W. (1998). *Software engineering standards*. John Wiley & Sons, Inc.

Morrison, A. (2010). How much security can you Manage?. *Computers and Law*, *21*(4), 39.

National Defense Authorization Act for Fiscal Year 2006, Pub. L. No. 109-163 § 119 Stat. 3136 (2006)

Neto, F. M., de Souza, R., & Gomes, A. S. (2016). Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning (pp. 1-673). Hershey, PA: IGI

Global. doi:10.4018/978-1-5225-0125-1

Nist, (2012). NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems and Organizations. CreateSpace, Paramount, CA.

Newman, D., & Pickholtz, R. (1986). Cryptography in the private sector. IEEE Communications Magazine, 24(8), 7-10.

Norton, Q. (2007). The next humans: Body hacking and human enhancement. O'Reilly Emerging Technology Conference.

Ogata, H. & ano, Y. (2012), Context-aware support for computer-supported ubiquitous learning. Retrieved from http://140.115.126.240/mediawiki/images/e/e9/Context_Awareness.pdf

Omar, M.,& Dawson, M. (2013, April). Research in progress- defending android smartphones from malware attacks. ln *2013 Third International Conference on Advanced Computing and Communication Technologies* (pp. 288-292) Rohtak, India: IEEE Proceedings.

Ontang, M., McLaughlin, S., Enck, W., & McDaniel, P. (2009). *Semantically rich application-centric security in Android*. Retrieved from Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC '09). Retrieved (date) fromhttp://dl.acm.org.

Phillips WM, Peterson GD, Aberle KB (2000) Quality assurance for engineering education in a changing world. Int J Eng Educ 16(2):97–103

Popper, S., Bankes, S., Callaway, R., & DeLaurentis, D. (2004). System-of-Systems Symposium: Report on a summer conversation. Arlington, VA: Potomac Institute for Policy Studies.

Ranadivé, V. (2013, February 19). Hyperconnectivity: The future is now. Retrieved March 21, 2016, from http://www.forbes.com/sites/vivekranadive/2013/02/19/hyperconnectivity-the-future-is-now/#401d45d26b9f

Richardson, C. critical infrastructure protection. *Alternative Energy CBRN Defense Critical Infrastructure Protection*, 13.

Sá, C., & Gaviria, P. (2011). How Do Professional Mutual Recognition Agreements Affect Higher Education? Examining Regional Policy in North America. *Higher Education Policy*, *24*(3), 307-330.

Sailer, R., Jaeger, T., Valdez, E., Caceres, R., Perez, R., Berger, S., ... & Van Doorn, L. (2005, December). Building a MAC-based security architecture for the Xen open-source hypervisor. In *Computer security applications conference, 21st Annual* (pp. 10-pp). IEEE.

Schneider, F., & Berenbach, B. (2013). A literature survey on international standards for systems requirements engineering. *Procedia Computer Science*, *16*, 796-805.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. (2010, March/April). Android: A comprehensive security assessment. *IEEE Security & Privacy, 8*(2), 35-44.

START. (n.d.). Information on more than 140,000 terrorist attacks. Retrieved March 16, 2016, from http://apps.start.umd.edu/gtd/.

Sung, J. S. (2009). U-learning model design based on ubiquitous environment. International Journal of Advanced Science and Technology, 13, 77-88.

Tešić, J. (2005). Metadata practices for consumer photos. MultiMedia, *IEEE*,12(3), 86-92.

Thierer, A. D. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation.

Tovar, E., & Castro, M. (2007). Building common spaces in engineering education: A review from icece05. *IEEE Transactions on Education*, *50*(1), 79-84.

Troy, G. (1999). Introduction to the Common Criteria for IT Security (ISO 15408).

Twitter. (2014, October 22). Geo guidelines. Retrieved February 16, 2016, from https://dev.twitter.com/overview/terms/geo-developer-guidelines

Twitter. (n.d.). GET geo/reverse_geocode. Retrieved February 16, 2016, from https://dev.twitter.com/rest/reference/get/geo/reverse_geocode

USA Today. (2011, July 20). Guinean president survives assassination attempt. Retrieved August 07, 2017, from https://usatoday30.usatoday.com/news/world/2011-07-19-guinea-president-assassination-attempt_n.htm

Vennon, T. (2010). *Android malware*. Retrieved from http://threatcenter.smobilesystems.com/

Vidino, L., Pantucci, R., & Kohlmann, E. (2010). Bringing global jihad to the horn of Africa: Al Shabaab, western fighters, and the sacralization of the Somali Conflict. *African Security*, 3(4), 216-238.

Vouk, M. A. (2008). Cloud computing–issues, research and implementations. CIT. *Journal of Computing and Information Technology*, 16(4), 235-246.

Vincenti, G. (Ed.). (2010). *Teaching through multi-user virtual environments: Applying dynamic elements to the modern classroom: Applying dynamic elements to the modern classroom*. IGI Global.

Westfall, L. (2008). *The certified software quality engineer handbook*. ASQ Quality Press.

Wiley, D. A. (2000). Connecting learning objects to instructional design theory: A definition, a metaphor, and a taxonomy. In D. A. Wiley (Ed.), *The Instructional Use of Learning Objects: Online Version*. Retrieved October 3, 2015, from http://reusability.org/read/chapters/wiley.doc .

Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). Designing system-level defenses against cellphone malware. Retrieved March 21, 2013, from www.cse.psu.edu .

Appendix A: List of Acronyms

2-D - 2 Dimensional
3-D - 3 Dimensional
AAU - Assembly of the African Union
ABET - Accreditation Board for Engineering and Technology
AFRICOM - African Command
AI - Artificial Intelligence
AIC - Availability, Integrity, and Confidentiality
ANSI - American National Standards Institute
API - Application Programming Interface
APSA - African Peace and Security Architecture
ASF - African Standby Force
ASSE - American Society for Engineering Education
AU - African Union
AUC - African Union Commission
BYOB - Bring Your Own Device
CA - Certification Authority
C&A - Certification & Accreditation
CAE - Centers for Academic Excellence
CC - Common Criteria
CCIG - Computer Crime Investigation Group
CCM - Configuration Control and Management
CD - Cyber Defense
CERT - Community Emergency Response Team
CESG - Communications Electronics Security Group
CEWS - Continental Early Warning System
CIO - Chief Information Office
CNO- Chief of Naval Operations
ConOps - Concept of Operations
CPU - Central Processing Unit
DAA - Designated Approving Authority
DC3 - Department of Defense Cyber Crime Center
DCIO - Defense Criminal Investigative Organizations
DHS - Department of Homeland Security
DIACAP - Department of Defense Information Assurance Certification & Accreditation Process
DIP - DIACAP Implementation Plan
DITSCAP - Department of Defense Information Technology Security Certification & Accreditation Process

DNI - Director of National Intelligence
DoD - Department of Defense
DoDI - Department of Defense Instructions
DoN - Department of Navy
DRP - Disaster Recovery Plan
DSL - Damn Small Linux
EAL - Evaluated Assurance Level
EEC - European Economic Community
EO - Executive Order
EXIF - Exchange Image File Format
FIPS - Federal Information Processing Systems
FISMA - Federal Information Security Management Act
GHz - Gigahertz
GNU - GNU Not Unix
GPL - General Public License
GPS - Global Positioning System
GTD - Global Terrorism Database
HDD - Hard Disk Drive
HIDS - Host Intrusion Detection System
HTML - Hyper Text Markup Language
IA - Information Assurance
IAM - Information Assurance Manager
IAO - Information Assurance Officer
IC - Intelligence Community
ICEE - International Conference on Engineering Education
ICT - Information Communication Technologies
ID - Identification
IDS - Intrusion Detection System
IEEE - Institute of Electrical and Electronic Engineers
IFIP - International Federation for Information Processing
INCOSE - International Council of Systems Engineering
IoE - Internet of Everything
IoT - Internet of Things
IP3 - International Professional Practice Partnership
IS - Information Systems
ISO - International Organization for Standardization
ISP - International Studies and Programs
ISR - Intelligence, Surveillance, Reconnaissance
IT - Information Technology
JPEG - Joint Photographic Experts Group

KDE - K Desktop Environment
LLGPL - Lisp Lesser General Public License
LTSC - Learning Technology Standards Committee
M2M - Machine to Machine
MMS - Multimedia Messaging Service
NICE - National Initiative on Cyber Security Education
MRA - Mutual Recognition Agreements
NCIS - Naval Criminal Investigative Service
NIOC - Network Information Operations Command
NIST - National Institute of Standards and Technology
NSA - National Security Agency
NSPE - National Society of Professional Engineers
OA - Open Access
OAU - Organization of African Unity
OECD - Organisation for Economic Co-operation and Development
OPSEC - Operations Security
OSINT - Open Source Intelligence
OSS - Open Source Software
OS - Operating System
P2M - People to Machine
P2P - People to People
PGCS - Portable Ground Control System
PII - Personal Identifiable Information
PLANELM -
PLC - Programmable Logic Controller
PM - Program Manager
POA&M - Plan of Actions & Milestones
PSC - Peace and Security Council
PP - Protection Profile
RFID - Radio Frequency IDentification
RHEL - Red Hat Enterprise Linux
RMF - Risk Management Framework
RPM - Red Hat Package Manager
REC - Regional Economic Communities
RFP - Request For Proposal
RM - Regional Mechanisms
SCADA - Supervisory Control and Data Acquisition
SCP - System Contingency Plans
SIP - Systems Identification Plan
SMS - Short Message Service

SP - Special Publication
SPAWAR - Space and Naval Warfare Systems Center
ST - Security Target
Std - Standard
STEM - Science, Technology, Engineering, and Mathematics
STIG - Security Technical Implementation Guides
TOE - Target of Evaluation
TOR - The Onion Router
TPLP - Tigray People's Liberation Front
UAV - Unmanned Air Vehicles
UGV - Unmanned Ground Vehicles
U.K. - United Kingdom
U-Learning - Ubiquitous Learning
U.N. - United Nations
U.S. - United States
USGAO - United States Government Accountability Office
USN - United States Navy
VDI - Virtual Desktop Infrastructure
VHD - Virtual Hard Disk
VIP - Very Important People
VM - Virtual Machines
VMDSK - Virtual Machine Disk
WiFi - Wireless Fidelity
WoT - Web of Things
WWW - World Wide Web
ZitMo - Zeus-in-the-Mobile

Appendix B: Outputs Submitted for Award

The following outputs by the research have been included in the submission for the award of Ph.D. by Prior Output:

1. Dawson, M., Burton, S. L., Bessette, D., & Wright, J. (2018). Massive Open Online Courses and Integrating Open Source Technology and Open Access Literature Into Technology-Based Degrees. In M. Khosrow-Pour, D.B.A. (Ed.), *Encyclopedia of Information Science and Technology,* Fourth Edition (pp. 7898-7911). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2255-3.ch687
2. Dawson, M., & Cárdenas-Haro, J. A. (2017). Tails Linux Operating System: Remaining Anonymous with the Assistance of an Incognito System in Times of High Surveillance. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, 1(1), 47-55.
3. Dawson, M. (2017). Cyber Security Policies for Hyperconnectivity and Internet of Things: A Process for Managing Connectivity. In *Information Technology-New Generations* (pp. 911-914). Springer, Cham.
4. Dawson, M., Lieble, M., & Adeboje, A. (2017). Open Source Intelligence: Performing Data Mining and Link Analysis to Track Terrorist Activities. In *Information Technology-New Generations* (pp. 159-163). Springer, Cham.
5. Dawson, M. (2016). Exploring Secure Computing for the Internet of Things, Internet of Everything, Web of Things, and Hyperconnectivity. In M. Dawson, M. Eltayeb, & M. Omar (Eds.) *Security Solutions for Hyperconnectivity and the Internet of Things* (pp. 1-12). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0741-3.ch001

6. Davis, L., Dawson, M., & Omar, M. (2016). Systems Engineering Concepts with Aid of Virtual Worlds and Open Source Software: Using Technology to Develop Learning Objects and Simulation Environments. In F. Neto, R. de Souza, & A. Gomes (Eds.)*Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning* (pp. 483-509). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0125-1.ch020

7. Dawson, M., Omar, M., Abramson, J., Leonard, B., & Bessette, D. (2016). Battlefield Cyberspace: Exploitation of Hyperconnectivity and Internet of Things. In M. Dawson, D. Kisku, P. Gupta, J. Sing, & W. Li (Eds.) *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 204-235). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0703-1.ch010

8. Dawson, M., & Adeboje, W. (2016). Islamic Extremists in Africa: Security Spotlight on Kenya and Nigeria. In M. Dawson, D. Kisku, P. Gupta, J. Sing, & W. Li (Eds.) *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 93-103). Hershey, PA: Information Science Reference. doi:10.4018/978-1-5225-0703-1.ch005

9. Dawson, M., Eltayeb, M., & Omar, M. (2016). Security Solutions for Hyperconnectivity and the Internet of Things (pp. 1-347). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0741-3

10. Dawson, M., DeWalt, B., & Cleveland, S. (2016). The Case for UBUNTU Linux Operating System Performance and Usability for Use in Higher Education in a Virtualized Environment.

11. Dawson, M., & Omar, M. (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 1-368). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7

12. Dawson, M. (2015). A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism. In M. Dawson, & M. Omar (Eds.) *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 1-7). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8345-7.ch001

13. Dawson, M., Wright, J., & Omar, M. (2015). Mobile Devices: The Case for Cyber Security Hardened Systems. In M. Dawson, & M. Omar (Eds.) *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 8-29). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8345-7.ch002

14. Leonard, B., & Dawson, M. (2015). Legal Issues: Security and Privacy with Mobile Devices. In M. Dawson, & M. Omar (Eds.) *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 95-104). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8345-7.ch006

15. Dawson, M., Leonard, B., & Rahim, E. (2015). Advances in Technology Project Management: Review of Open Source Software Integration. In M. Wadhwa, & A. Harper (Eds.) *Technology, Innovation, and Enterprise Transformation* (pp. 313-324). Hershey, PA: Business Science Reference. doi:10.4018/978-1-4666-6473-9.ch016

16. Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the Methods behind Cyber Terrorism. In M. Khosrow-Pour (Ed.)*, Encyclopedia of Information Science and Technology, Third Edition* (pp. 1539-1549). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-5888-2.ch147

17. Dawson, M., Omar, M., Abramson, J., & Bessette, D. (2014). The Future of National and International Security on the Internet. In A. Kayem, & C. Meinel (Eds.) *Information*

Security in Diverse Computing Environments (pp. 149-178). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-6158-5.ch009

18. Dawson, M., Al Saeed, I., Wright, J., & Onyegbula, F. (2014). Open Source Software to Enhance the STEM Learning Environment. In V. Wang (Ed.), *Handbook of Research on Education and Technology in a Changing Society* (pp. 569-580). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-6046-5.ch042
19. Dawson Jr, M. E., Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*(1), 1-22.
20. Dawson, M. E., & Al Saeed, I. (2012). Use of Open Source Software and Virtualization in Academia to Enhance Higher Education Everywhere.*Cutting-edge Technologies in Higher Education*, *6*, 283-313.
21. Dawson, M., & Rahim, E. (2011). Transitional leadership in the defence and aerospace industry: a critical analysis for recruiting and developing talent.*International Journal of Project Organisation and Management*, *3*(2), 164-183.
22. Dawson, M., Burrell, D. N., Rahim, E., & Brewster, S. (2010). Integrating Software Assurance into the Software Development Life Cycle (SDLC).*Journal of Information Systems Technology and Planning*, *3*(6), 49-53.
23. Dawson, M., Burrell, D. N., Rahim, E., & Brewster, S. (2010). Examining the role of the chief information security officer (ciso) & security plan. *Journal of Information Systems Technology & Planning*, 3(6), 1-5.
24. Cardenas-Haro, J. A., & Dawson, M. (2017). Tails Linux Operating System: The Amnesiac Incognito System in Times of High Surveillance, Its Security Flaws, Limitations,

and Strengths in the Fight for Democracy. In M. Dawson, M. Eltayeb, & M. Omar (Eds.), *Security Solutions for Hyperconnectivity and the Internet of Things* (pp. 260-271). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0741-3.ch010

25. Eltayeb, M., & Dawson, M. (2016). Understanding user's acceptance of personal cloud computing: Using the Technology Acceptance Model. *Information technology: New generations*, 448, 3-12.

26. Omar, M., & Dawson, M. (2013, April). Research in Progress-Defending Android Smartphones from Malware Attacks. In *Advanced Computing and Communication Technologies (ACCT), 2013 Third International Conference on* (pp. 288-292). IEEE.

Appendix C: All Published Outputs

In accordance with the guidance notes for submission, the following list includes all scholarly outputs produced by the researcher, including those that have not been included as a part of the submission:

A. Abramson, J., Dawson, M., & Stevens, J. (2015). An Examination of the Prior Use of E-Learning Within an Extended Technology Acceptance Model and the Factors That Influence the Behavioral Intention of Users to Use M-Learning. *SAGE Open*, *5*(4), 2158244015621114.

B. Burrell, Darrell, Andrea Todd, Aikyna Finch, and Maurice Dawson. "Developing the Next Generation of Women and Minority Scientists for the Nuclear Energy Industry." *The International Journal of Science in Society* 3, no. 2 (2012).

C. Cleveland, S., Jackson, B. C., & Dawson, M. (2016). Microblogging in higher education: Digital Natives, knowledge creation, social engineering, and intelligence analysis of educational tweets. *E-Learning and Digital Media*, 13(1-2), 62-80.

D. Dawson, M., Al Saeed, I., Wright, J., & Omar, M. (2013). Technology Enhanced Learning with Open Source Software for Scientists and Engineers.*INTED2013 Proceedings*, 5583-5589.

E. Dawson Jr, M. E., Wright, J., & Abramson, J. (2013). Transforming Information Systems and Information Systems and Computer Science Education with Virtualization. *ICERI2013 Proceedings*, 2679-2682.

F. Dawson Jr, M. E., Wright, J., & Abramson, J. (2013). Open Source Software to Teach Technology Entrepreneurship Concepts and Practices. *ICERI2013 Proceedings*, 2637-2639.

G. MacPherson, J., & Dawson, M. (2016). Common protocol to support disparate communication types within industrial Ethernet environments. *International Journal of Network Science*, *1*(2), 134-154.

H. Wright, J., & Dawson Jr, M. E. (2013). Importance of Integrating Information Technology Related Curriculum in American Inner City Schools. *INTED2013 Proceedings*.

Appendix D: Research Background

To date, publications have been in three major areas which are education, policy, and technologies that have been aligned to the field of cyber security. The publication outlets have been Springer, IEEE, IGI Global, Emerald, Sage, Inderscience, Intellectbase, Southern Association of Information Systems (SAIS), DeGruyter, Alabama Academy of Science, Florida Academy of Science, and the Missouri Academy of Science.

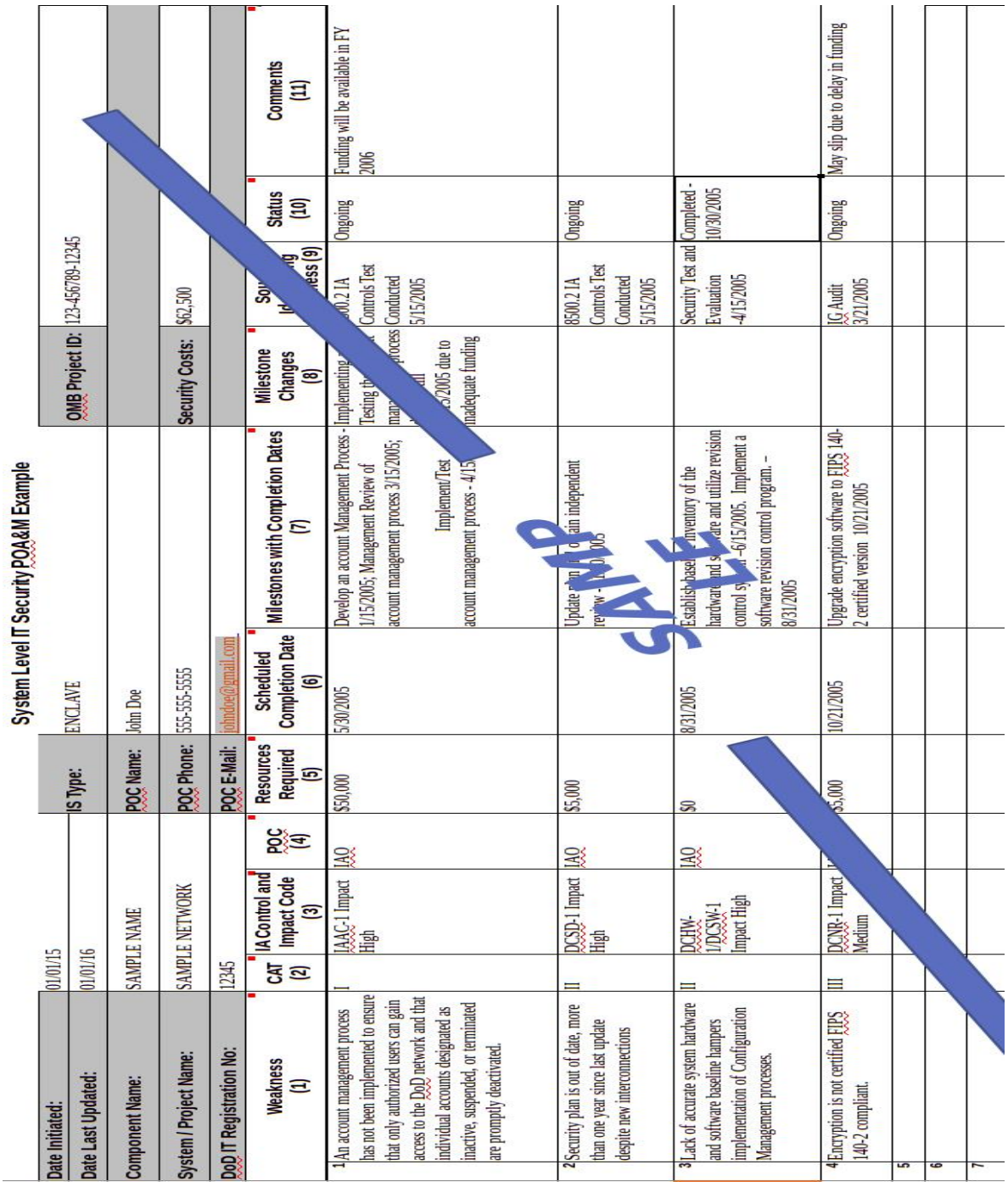
Maurice Dawson is an Assistant Professor of Information Systems (Cyber Security) at the College of Business Administration at University of Missouri- St. Louis with affiliation to the Cybersecurity and Information Technology Innovation Lab (CITIL). He is Visiting Professor at the Polytechnic University of Puerto Rico, Visiting Professor at the University of Nairobi, and a Senior Research Fellow at the American Leadership & Policy Foundation (ALPF). Additionally, he was a Visiting Assistant Professor (Honorary) at the University of Tennessee in the College of Engineering within the Department of Industrial and Systems Engineering. Dawson has received two Fulbright Specialist Grants, first to Russia in 2014 [Project #5824/South Ural State University] and then to Saudi Arabia for 2017-2018 [Project #65824/Prince Sultan University]]. Dawson served as Visiting Scholar with the University of the Gambia through the International Studies and Programs (ISP) Fellowship awarded from UMSL in 2014. Dawson received an appointment as an International Business (IB) Research Associate in the UMSL International Business Institute (IBI) which is nationally ranked. Dawson was a Visiting Professor at the University of Nairobi in Nairobi, Kenya in 2016 in the field of cyber security. In December 2013 he was mentioned in Lloyds of London for cyber security attacks on critical infrastructure.

Dawson holds a Doctor of Computer Science from Colorado Technical University. Additionally, the institution is classified as a Doc/STEM: Doctoral, STEM Dominant; DRU: Doctoral/Research Universities by the Carnegie Foundation and has ABET accreditation. He is currently a PhD student at London Metropolitan University in the Intelligent Systems Research Centre (ISRC). He holds multiple professional certifications such as (ISC) 2's Certified Security Software Lifecycle Professional (CSSLP), ISACA's Certification in the Governance of Enterprise IT (CGEIT), and EC-Council's Certified Chief Information Security Officer (C|CISO). He is a member of the International Association for Engineers (IAENG), Institute of Electrical and Electronic Engineers (IEEE), IAENG Society of Information Systems Engineering, IAENG Society of Computer Science, IAENG Society of Data Mining, and IAENG Society of Wireless Networks.

Dawson is a member of the International Advisory Board for the International Journal of Productivity Management and Assessment Technologies, founding editor-in-chief of the *International Journal of Hyperconnectivity* and the Internet of Things (IJHIoT). This journal has been indexed in ACM Digital Library, and Cabell's Directories. Formerly, served as the associate editor-in-chief of the *Journal of Information Systems Technology and Planning*. Recent edited books include *New Threats and Countermeasures in Digital Crime* and *Cyber Terrorism*. Other scholarly works include "Understanding the Methods Behind Cyber Terrorism", "The Future of National and International Security on the Internet", "DoD Cyber Technology Policies to Secure Automated Information Systems", and Research in Progress-"Defending Android Smartphones from Malware Attacks". At the moment, Dawson has 12+ peer reviewed book chapters, 20+ referred papers, and over 65 conference proceedings.

Aside from educational accomplishments Dawson has 14+ years in industry and more than five + years' experience as a Profit & Loss (P&L) leader over $4 Million with responsibility up to $25 Million. The five year portfolio responsibility was approximately $250 Million. He has proudly served in the Army Reserves as a System Analyst and as a Crypto Technician in the Reserve Intelligence Area (RIA) in the Navy Reserves. Dawson has worked with the Program Executive Office (PEO) for Army Aviation, PEO Unmanned Air Systems (UAS), US Army 160th Special Operations Aircraft (SOA), United States Special Operations Command (USSOCOM), Defense Intelligence Agency (DIA), and NSA. Dawson is recognized by the DoD as an Information Assurance Architect & Systems Engineer.

Appendix E: Plan of Actions & Milestones (POA&M)



System Level IT Security POA&M Example

Date Initiated:	01/01/15							OMB Project ID:	123-456789-12345		
Date Last Updated:	01/01/16	IS Type:	ENCLAVE								
Component Name:	SAMPLE NAME	POC Name:	John Doe								
System / Project Name:	SAMPLE NETWORK	POC Phone:	555-555-5555					Security Costs:	$62,500		
DoD IT Registration No:	12345	POC E-Mail:	johndoe@gmail.com								
Weakness (1)	CAT (2)	IA Control and Impact Code (3)	POC (4)	Resources Required (5)	Scheduled Completion Date (6)	Milestones with Completion Dates (7)	Milestone Changes (8)	Sou... Iden...ess (9)	Status (10)	Comments (11)
1 An account management process has not been implemented to ensure that only authorized users can gain access to the DoD network and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.	I	IAAC-1 Impact High	IAO	$50,000	5/30/2005	Develop an account Management Process - 1/15/2005; Management Review of account management process 3/15/2005; Implement/Test account management process - 4/15	Implementing ... Testing th... mana... proces... Aud... 9/2005 due to inadequate funding	8500.2 IA Controls Test Conducted 5/15/2005	Ongoing	Funding will be available in FY 2006
2 Security plan is out of date, more than one year since last update despite new interconnections	II	DCSD-1 Impact High	IAO	$5,000		Update plan ... ain independent review - 4/1/2005		8500.2 IA Controls Test Conducted 5/15/2005	Ongoing	
3 Lack of accurate system hardware and software baseline hampers implementation of Configuration Management processes.	II	DCHW-1/DCSW-1 Impact High	IAO	$0	8/31/2005	Establish base... inventory of the hardware and s... are and utilize revision control s... -6/15/2005. Implement a software revision control program. – 8/31/2005		Security Test and Evaluation -4/15/2005	Completed - 10/30/2005	
4 Encryption is not certified FIPS 140-2 compliant.	III	DCNR-1 Impact ... Medium	...	5,000	10/21/2005	Upgrade encryption software to FIPS 140-2 certified version 10/21/2005		IG Audit 3/21/2005	Ongoing	May slip due to delay in funding
5										
6										
7										

Appendix F: DIACAP Scorecard Example

FOR OFFICIAL USE ONLY

DIACAP SCORECARD

System Name	System Owner			IS Type
Designated Accrediting Authority (DAA)	Accred. Status	Period Covered		Last Update
		Accreditation Date	ATD	
Certifying Authority (CA)	Cert. Date	MAC	CL	Overall System Risk
		III	Sensitive	

IA Control Subject Area	IA Control Number	IA Control Name	Inherited	Compliance C/NC/NA	Impact Code	Last Update
Continuity	COAS-1	Alternate Site Designation			Medium	
Continuity	COBR-1	Protection of Backup and Restoration Assets			High	
Continuity	CODB-1	Data Backup Procedures			Low	
Continuity	CODP-1	Disaster and Recovery Planning			Low	
Continuity	COEB-1	Enclave Boundary Defense			Medium	
Continuity	COED-1	Scheduled Exercises and Drills			Low	
Continuity	COEF-1	Identification of Essential Functions			Low	
Continuity	COMS-1	Maintenance Support			Low	
Continuity	COPS-1	Power Supply			Low	
Continuity	COSP-1	Spares and Parts			Low	
Continuity	COSW-1	Backup Copies of Critical SW			High	
Continuity	COTR-1	Trusted Recovery			High	
Security Design and Configuration	DCAR-1	Procedural Review			Medium	
Security Design and Configuration	DCAS-1	Acquisition Standards			High	
Security Design and Configuration	DCBP-1	Best Security Practices			Medium	
Security Design and Configuration	DCCB-1	Control Board			Low	
Security Design and Configuration	DCCS-1	Configuration Specifications			High	
Security Design and Configuration	DCCT-1	Compliance Testing			Medium	
Security Design and Configuration	DCDS-1	Dedicated IA Services			Medium	
Security Design and Configuration	DCFA-1	Functional Architecture for AIS Applications			Medium	
Security Design and Configuration	DCHW-	HW Baseline			High	
Security Design and Configuration	DCID-1	Interconnection Documentation			High	
Security Design and Configuration	DCII-1	IA Impact Assessment			Medium	
Security Design and Configuration	DCIT-1	IA for IT Services			High	
Security Design and Configuration	DCMC-1	Mobile Code			Medium	
Security Design and Configuration	DCNR-1	Non-repudiation			Medium	
Security Design and Configuration	DCPD-1	Public Domain Software Controls			Medium	
Security Design and Configuration	DCPP-1	Ports, Protocols, and Services			Medium	
Security Design and Configuration	DCPR-1	CM Process			High	
Security Design and Configuration	DCSD-1	IA Documentation			High	
Security Design and Configuration	DCSL-1	System Library Management Controls			Medium	
Security Design and Configuration	DCSQ-1	Software Quality			Medium	
Security Design and Configuration	DCSR-2	Specified Robustness - Medium			High	
Security Design and Configuration	DCSS-1	System State Changes			High	
Security Design and Configuration	DCSW-1	SW Baseline			High	
Enclave Boundary Defense	EBBD-2	Boundary Defense			Medium	
Enclave Boundary Defense	EBCR-1	Connection Rules			Medium	
Enclave Boundary Defense	EBPW-1	Public WAN Connection			High	
Enclave Boundary Defense	EBRP-1	Remote Access for Privileged Functions			High	
Enclave Boundary Defense	EBRU-1	Remote Access for User Functions			High	
Enclave Boundary Defense	EBVC-1	VPN Controls			Medium	
Enclave Computing Environment	ECAD-1	Affiliation Display			Medium	
Enclave Computing Environment	ECAN-1	Access for Need-to-Know			High	
Enclave Computing Environment	ECAR-2	Audit Record Content – Sensitive Systems			Medium	
Enclave Computing Environment	ECAT-1	Audit Trail, Monitoring, Analysis and			Low	

Appendix G: System Identification Plan (SIP) Example

FOR OFFICIAL USE ONLY

Implementation Plan

System Name:	MAC:	CL:
	III	Sensitive

Control Number	Implementation Status				Responsible Entity	Resources	Estimated Completion Date	Comments
	NA	Inherited	Implemented	Planned				
COAS-1								
COBR-1								
CODB-1								
CODP-1								
COEB-1								
COED-1								
COEF-1								
COMS-1								
COPS-1								
COSP-1								
COSW-1								
COTR-1								
DCAR-1								
DCAS-1								
DCBP-1								
DCCB-1								
DCCS-1								
DCCT-1								
DCDS-1								
DCFA-1								
DCHW-1								
DCID-1								
DCII-1								
DCIT-1								
DCMC-1								
DCNR-1								
DCPD-1								

Appendix H: DIACAP Implementation Plan (DIP) Example

FOR OFFICIAL USE ONLY

Implementation Plan

System Name:	MAC:	CL:
	III	Sensitive

Control Number	Implementation Status				Responsible Entity	Resources	Estimated Completion Date	Comments
	NA	Inherited	Implemented	Planned				
COAS-1								
COBR-1								
CODB-1								
CODP-1								
COEB-1								
COED-1								
COEF-1								
COMS-1								
COPS-1								
COSP-1								
COSW-1								
COTR-1								
DCAR-1								
DCAS-1								
DCBP-1								
DCCB-1								
DCCS-1								
DCCT-1								
DCDS-1								
DCFA-1								
DCHW-1								
DCID-1								
DCII-1								
DCIT-1								
DCMC-1								
DCNR-1								
DCPD-1								

Appendix I: Doctoral Diploma

Colorado Technical University

Institute for Advanced Studies

Greeting to all to whom these Letters shall come:
The Colorado Technical University Board of Directors
by virtue of the authority vested in it by law and
on recommendation of the University Faculty does hereby confer on

Maurice Eugene Dawson Jr.

who has satisfactorily completed the Studies prescribed therefore
the Degree of

Doctor of Computer Science

with a concentration in Enterprise Information Systems
with all the rights, Privileges and Honors appertaining thereto.
In Witness Whereof the Seal of the University is hereto affixed.
Granted at Colorado Springs, Colorado, this month of September,
two thousand nine.

Appendix J: NSA & DHS CAE Designation Award

National Centers of Academic Excellence in Cyber Defense Education
9800 Savage Road
Ft. Meade, MD 20755-6804

University of Missouri-St. Louis
Dr. Maurice Dawson
228 Express Scripts Hall
One University Blvd
St. Louis, MO 63121-4400

Dr. Dawson:

I am pleased to inform you that the National Security Agency and the Department of Homeland Security have designated the University of Missouri – St. Louis as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) through academic year 2021.

Your ability to meet the increasing demands of the program criteria will serve the nation well in contributing to the protection of the National Information Infrastructure. The Presidents' National Strategy to Secure Cyberspace, 14 February 2003 and the International Strategy for Cyberspace, May 2011, addresses the critical shortage of professionals with these skills and highlights the importance of higher education as a solution to defending America's cyberspace. "Like all nations, the United States has a compelling interest in defending its vital national assets, as well as our core principles and values, and we are committed to defending against those who would attempt to impede our ability to do so." Education is the key to promoting these ideals.

Certificates will be presented during an evening reception at the National Cyber Security Summit in Huntsville, Alabama on June 8, 2016. Details on the Summit, to include a CAE Community Meeting on June 7th, are attached. For those unable to attend the Summit, certificates will also be presented at the November 1-2, 2016 NICE Conference & Expo in Kansas City Missouri. Information on the Expo can be found at: https://www.fbcinc.com/e/nice/default.aspx . We appreciate your participation in this program and look forward to seeing you in June.

Sincerely,

\s\

Karen Leuschner
National CAE Program Manager, NSA

Appendix K: NSA & DHS CAE Focus Area Award

National Centers of Academic Excellence in Cyber Defense Education
9800 Savage Road
Ft. Meade, MD 20755-6804

University of Missouri – St. Louis
Dr. Maurice Dawson
228 Express Scripts Hall
One University Blvd.
St. Louis, MO 63121-4400

11 May 2017

Dr. Dawson:

I am pleased to inform you that the National Security Agency and the Department of Homeland Security have designated the University of Missouri – St. Louis with a Focus Area specialization in Security Policy Development and Compliance through academic year 2021.

Your ability to meet the increasing demands of the program criteria will serve the nation well in contributing to the protection of the National Information Infrastructure. The Presidents' National Strategy to Secure Cyberspace, 14 February 2003 and the International Strategy for Cyberspace, May 2011, addresses the critical shortage of professionals with these skills and highlights the importance of higher education as a solution to defending America's cyberspace. "Like all nations, the United States has a compelling interest in defending its vital national assets, as well as our core principles and values, and we are committed to defending against those who would attempt to impede our ability to do so." Education is the key to promoting these ideals.

Certificates will be presented during an evening reception at the National Cyber Security Summit in Huntsville, Alabama. The NCS is scheduled for 6 – 8 June 2017. Details on the Summit, to include a CAE Principals Meeting will be finalized soon. We appreciate your participation in this program and look forward to seeing you in June.

Sincerely,

\s\

Karen Leuschner
National CAE Program Manager, NSA

Appendix L: Fulbright Specialist Award for Bangladesh

INSTITUTE OF INTERNATIONAL EDUCATION | CIES Council for International Exchange of Scholars

August 3, 2015

Dr. Maurice Dawson
University of Missouri-St. Louis
College of Business and Public Affairs
1 University Blvd.
St. Louis, MO 63121-4400

Dear Dr. Dawson,

On behalf of the J. William Fulbright Foreign Scholarship Board (FFSB), the Bureau of Education and Cultural Affairs of the Department of State (the Department), and the Council for International Exchange of Scholars (CIES), it gives me great pleasure to inform you that you have been selected for a Fulbright Specialist grant in Information Technology at University of Rajshahi, Bangladesh.

As a Fulbrighter, you will be joining the ranks of distinguished scholars and professionals worldwide who are leaders in the educational, political, economic, social, and cultural lives of their countries. It is our expectation that, as a representative of the United States, you will also demonstrate the qualities of excellence and leadership that have been the hallmarks of this respected international academic exchange program founded in 1946 by the U.S. Government.

Following you will find the **Terms and Conditions of Award** along with the **Program Overview** for your Fulbright Specialist project. To complete the administration of your grant, proceed to the password-protected Specialist Grantee webpage at www.cies.org/G_specialists. This page outlines the next steps that will get you quickly through the grant administration process and to your host institution abroad. To log in, you will need to enter the password: ***CIES_special!***

After carefully reviewing all of the materials concerning your grant, please follow the steps outlined on the "Preparing to Go" document. Once your budget has been approved you will need to let us know your decision by signing and returning to CIES the countersigned **Grant Authorization**.

If you have questions or need further information about this grant, please e-mail program staff at fspgrants@iie.org or call Carmel Geraghty, Program Officer, at 202-686-8641.

The FFSB, the Department, and CIES join in congratulating you and wishing you a successful experience abroad. We hope that your Fulbright experience will be highly rewarding and that you will share the knowledge you gain as a Fulbrighter for years to come.

Sincerely,

María de los Ángeles Crummett
Executive Director of CIES

Appendix M: Fulbright Specialist Award for Russia

INSTITUTE OF INTERNATIONAL EDUCATION | CIES Council for International Exchange of Scholars

May 5, 2014

Dr. Maurice Dawson
Assistant Professor of Information Systems
University of Missouri- St. Louis
Department of Information Systems
College of Business Administration 487 SSB
One University Blvd
St. Louis, MO 63121-4400

Dear Dr. Dawson,

On behalf of the J. William Fulbright Foreign Scholarship Board (FFSB), the Bureau of Education and Cultural Affairs of the Department of State (the Department), and the Council for International Exchange of Scholars (CIES), it gives me great pleasure to inform you that you have been selected for a Fulbright Specialist grant in Information Technology at South Ural State University, Russia.

As a Fulbrighter, you will be joining the ranks of distinguished scholars and professionals worldwide who are leaders in the educational, political, economic, social, and cultural lives of their countries. It is our expectation that, as a representative of the United States, you will also demonstrate the qualities of excellence and leadership that have been the hallmarks of this respected international academic exchange program founded in 1946 by the U.S. Government.

Following you will find the **Terms and Conditions of Award** along with the **Program Overview** for your Fulbright Specialist project. To complete the administration of your grant, proceed to the password-protected Specialist Grantee webpage at www.cies.org/G_specialists. This page outlines the next steps that will get you quickly through the grant administration process and to your host institution abroad. To log in, you will need to enter the

After carefully reviewing all of the materials concerning your grant, please follow the steps outlined on the "Preparing to Go" document. Once your budget has been approved you will need to let us know your decision by signing and returning to CIES the countersigned **Grant Authorization**.

If you have questions or need further information about this grant, please e-mail program staff at fspgrants@iie.org or call Carmel Geraghty, Program Officer, at 202-686-8641.

The FFSB, the Department, and CIES join in congratulating you and wishing you a successful experience abroad. We hope that your Fulbright experience will be highly rewarding and that you will share the knowledge you gain as a Fulbrighter for years to come.

Sincerely,

Jamie Bellis
Deputy Executive Director of CIES

Appendix N: Polytechnic University of Puerto Rico Letter of Invitation

Escuela de Ingeniería,
Agrimensura y Ciencias
Geoespaciales

377 Ponce de León Ave.
Hato Rey, PR 00918
(787) 622-8000
www.pupr.edu

January 12, 2016

Attention Dr. Maurice Dawson

Letter of Invitation,

Let the present letter be our official invitation to Dr. Maurice Dawson to visit our Department of Electrical & Computer Engineering and Computer Science. We understand his availability for such visit will be the during the Summer of 2016 for a period of 2-3 weeks.

The immediate objectives are to provide a seminar and be a guest researcher within our Center of Academic Excellence in Cyber Security.

We are interesting in further expanding this initial visit with collaborations between our university and the University of Missouri System and to seek and obtain research funding.

Polytechnic University of Puerto Rico has had a MOU with University of Missouri-Columbia Campus in the past. At least five (5) of our faculty members have completed their PhD's at University of Missouri-Columbia campus in areas such as Nuclear Engineering, Civil Engineering, Electrical Engineering, and Computer Engineering. We look-forward to expand our research collaboration with the St. Louis Campus as well.

Please let us know a more detailed schedule of your availability during this period so we can complete the required coordination on our part.

Best Regards,

Othoniel Rodríguez-Jiménez, PhD.
Director
Electrical & Computer Engineering
and Computer Science Department
Polytechnic University of Puerto Rico
Tel.: (787) 622-8000 ext. 370
E-mail: orodrigu@pupr.edu

Appendix O: University of Nairobi Letter of Invitation

UNIVERSITY OF NAIROBI
Office of the Vice-Chancellor

Prof. Peter M. F. Mbithi, IOM, EBS, MKVC (Surgery), MKIM, BVM, MSc., (Nbi), MVSc. (Sask), PhD, (Nbi)

Fax: +254-20-2212604/2216030
Email: vc@uonbi.ac.ke
Website: www.uonbi.ac.ke

Tel: +254-20-3318262, +254 732 020 207
P.O. Box 30197 - 00100 - GPO
Nairobi, Kenya

August 18, 2015

Prof. Maurice Eugene Dawson
University of Missouri, St. Louis
Department of Information Systems
College of Business Administration
228 Express Scripts Hall
One University BLVD
ST. LOUIS, MO 63121-4400 USA

Dear Prof, Dawson,

CYBER SECURITY PROFESSOR AND FULBRIGHT SCHOLAR

It is with great pleasure that I take this opportunity to invite you to the University of Nairobi between March 24 and April 2, 2016.

Your area of specialization, Cyber Security, is quite relevant and strategic to the institution given the global emerging issues in the Information and Technology arena.

The intended engagement and interaction with faculty and students of the School of Computing and informatics will be of great interest, not only to the school, but also the entire university community.

I look forward to your visit and most welcome.

PETER M.F. MBITHI, PhD, EBS
VICE-CHANCELLOR
AND
PROFESSOR OF VETERINARY SURGERY

MWM/emk

Appendix P: International Studies & Programs Award Letter - 2016

UMSL | International Studies & Programs

Office of the Director
International Studies and Programs
University of Missouri–St. Louis
366 Social Sciences & Business Bldg.
1 University Boulevard
St. Louis, MO 63121-4400
314-516-5753

September 27, 2016

Maurice Dawson, Jr., Assistant Professor-Information Systems
2nd floor ESH

Dear Mo,

Based on the recommendations by a panel of senior faculty who reviewed the Fellow applications, I am pleased to notify you of your appointment as a Fellow in International Studies and Programs (ISP) for the 2016-2017 academic year. You will receive the following support for your research:

- $2000 – Airfare and lodging to Dominican Republic for strengthening cyber security research ties in Latin America/Caribbean

We are expecting you to expend these funds by June 30, 2017. You must obtain written permission to spend funds after that date or unexpended funds will be retained by ISP.

I am glad that the Office of International Studies and Programs is able to provide support for your work and to formally recognize the importance of your research.

Please remember that part of accepting ISP funds is a commitment to be an active participant in ISP conferences, seminars and other activities. I look forward to working with you on ISP activities and programs.

Also, please remember to acknowledge ISP support for your research in any papers or publications that are developed as part of your project.

If you have any questions about this, please let me know.

Sincerely,

Joel Glassman
Associate Provost, Academic Affairs
Director, International Studies and Programs

Cc: Dinesh Mirchandani, Department Chair
Charles Hoffman, Dean COBA
Melody Freeman, ISP Business Fiscal Manager
Bob Baumann, ISP Assistant Director

Appendix Q: International Studies & Programs Award Letter - 2014

UMSL | International Studies & Programs

Office of the Director
International Studies and Programs
University of Missouri–St. Louis
366 Social Sciences & Business Bldg.
1 University Boulevard
St. Louis, MO 63121-4400
314-516-5753

September 29, 2014

Maurice Dawson, Assistant Professor of Information Systems
College of Business Administration
2nd floor Express Scripts Hall

Dear Maurice,

Based on the recommendations by a panel of senior faculty who reviewed the Fellow applications, I am pleased to notify you of your appointment as a Fellow in International Studies and Programs (ISP) for the 2014-2015 academic year. You will receive the following support for your research:

- $1676 airfare for symposium in Gambia
- $324 meals, local travel, and other costs for same symposium

We are expecting you to expend these funds by June 30, 2015. You must obtain written permission to spend funds after that date or unexpended funds will be retained by ISP.

I am glad that the Office of International Studies and Programs is able to provide support for your work and to formally recognize the importance of your research.

Please remember that part of accepting ISP funds is a commitment to be an active participant in ISP conferences, seminars and other activities. As funds become ever scarcer, it is only possible to provide support for faculty who most actively support the overall international education program of ISP. I look forward to working with you on ISP activities and programs.

Also, please remember to acknowledge ISP support for your research in any papers or publications that are developed as part of your project.

If you have any questions about this, please let me know.

Sincerely,

Joel Glassman
Associate Provost, Academic Affairs
Director, International Studies and Programs

Cc: Robert Nauss, Department Chairperson
Charles Hoffman, COBA Dean
Renae Smith, ISP Business Fiscal Manager
Bob Baumann, ISP Assistant Director

an equal opportunity institution

Appendix R: The University of the Gambia Letter of Invitation

THE UNIVERSITY OF THE GAMBIA
(School of ICT)

Chancery Building
Brikama
18th March, 2015.

University of Missouri-S t. Louis
United States of America

Dear Dr. Dawson,

An Invitation

The University of the Gambia (UTG) presents its compliments to you and has the honor to invite you for a visit to the University of The Gambia to host the **West African Symposium on Technology, Science, Sustainability, and Computing** in March, 2015.

Given your expertise, experience and knowledge in cyber security and computer science, your visit to the University of The Gambia is invaluable and highly welcome, especially to our young School of Information, Technology & Communication. The visit will further pave way for establishing collaboration and cooperation between your current University and the University of the Gambia.

The University of The Gambia is pleased to provide you with an accommodation and transportation from your resident to our campuses during your visit.

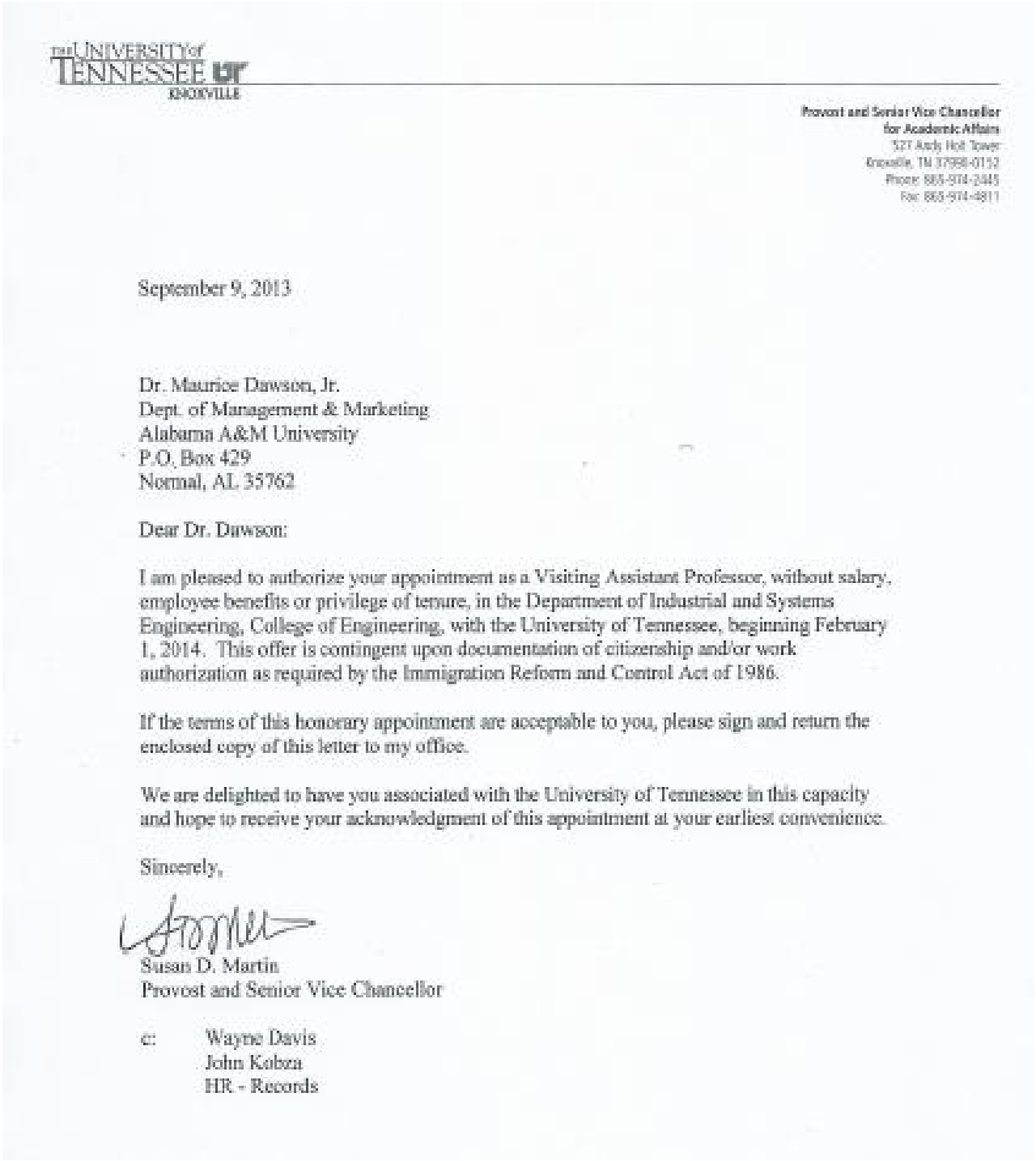
While looking forward to your enjoyable and fruitful visit, please accept our very best wishes.

Yours faithfully,

Mr. Yorro Njie
For: Ag Dean School of ICT
Cc: Vice Chancellor
Deputy Vice Chancellor
University Relations Office

P.O. Box 3530, Serrekunda Tel: +220 3650009 /3650084 email: yorro.njie@utg.edu.gm

Appendix S: The University of Tennessee, Knoxville Visiting Appointment



THE UNIVERSITY of TENNESSEE KNOXVILLE

Provost and Senior Vice Chancellor
for Academic Affairs
527 Andy Holt Tower
Knoxville, TN 37996-0152
Phone: 865-974-2445
Fax: 865-974-4811

September 9, 2013

Dr. Maurice Dawson, Jr.
Dept. of Management & Marketing
Alabama A&M University
P.O. Box 429
Normal, AL 35762

Dear Dr. Dawson:

I am pleased to authorize your appointment as a Visiting Assistant Professor, without salary, employee benefits or privilege of tenure, in the Department of Industrial and Systems Engineering, College of Engineering, with the University of Tennessee, beginning February 1, 2014. This offer is contingent upon documentation of citizenship and/or work authorization as required by the Immigration Reform and Control Act of 1986.

If the terms of this honorary appointment are acceptable to you, please sign and return the enclosed copy of this letter to my office.

We are delighted to have you associated with the University of Tennessee in this capacity and hope to receive your acknowledgment of this appointment at your earliest convenience.

Sincerely,

Susan D. Martin
Provost and Senior Vice Chancellor

c: Wayne Davis
John Kobza
HR - Records

Appendix T: The University of the Gambia Letter of Invitation

THE UNIVERSITY OF THE GAMBIA
(Office of University Relations)

Chancery Building
Brikama
9th December, 2013.

Alabama A&M University
Department of Management and Marketing
P.O. Box 429
Normal, Alabama 35762
United States of America

Dear Dr. Dawson,

An Invitation

The University of the Gambia (UTG) presents its compliments to Alabama A&M University, the President and the entire management for the recent signing of Memorandum of Understanding (MoU) by our two institutions. In the spirit of the MoU, UTG has the honor to invite you for a visit to the University of The Gambia in March, 2014.

Given your expertise, experience and knowledge in cyber security and computer science, your visit to the University of The Gambia is invaluable and highly welcome, especially to our young School of Information, Technology & Communication. The visit will further strengthen the existing collaboration and cooperation between the two Universities.

The University of The Gambia is pleased to provide you with an accommodation and transportation from your resident to our campuses during your visit.

While looking forward to your enjoyable and fruitful visit, please accept our very best wishes.

Yours faithfully,

UNIVERSITY OF THE GAMBIA
DATE 15/12/13
SIGN
OFFICE OF UNIVERSITY RELATION

Mr. Abdoulie Sillah
University Relations Office
Ag. Academic Coordinator SMCM Peace Program
Cc: Vice Chancellor
Deputy Vice Chancellor

P.O. Box 3530, Serrekunda Tel: +220 3650050 /3650029 email: asillah@utg.edu.gm