Information Security: A Scientometric Study of the Profile, Structure, and Dynamics of an Emerging Scholarly Specialty

A Dissertation

Submitted to the Faculty

of

Long Island University

by

Nicholas Victor Olijnyk

In partial fulfillment of the requirements for the degree

of

Doctor of Philosophy

March 2014

Dedication

To my parents who have taught me that with true commitment, dedication, and passion anything is possible.

Acknowledgements

I was once told that the secret to my success would be to surround myself with people whom I aspire to be like. This is the advice that led me to select my esteemed Dissertation Committee members.

My primary acknowledgment is to my main dissertation advisor, Dr. Heting Chu, who has, since our first course together four years ago, shown me the embodiment of a true scholar and giving me an example for which to strive. Having Dr. Chu guide me along the dissertation process gave me all the confidence that I needed to be successful. Dr. Steven P. Bucci, my external dissertation advisor, has been with me from the beginning. Dr. Bucci's advice has been invaluable in grounding my academic endeavors to real-world needs, as well as supplying my research with an information security policy perspective. Dr. Michael Koenig presented a depth of knowledge and experience in the information science field that gave my study the essential perspectives it needed to become a suitable doctoral thesis. Dr. John Regazzi offered me important suggestions and new ways of thinking. Dr. Stephanie M. White provided me with a technical viewpoint for information security and unique critical insights.

Last, but certainly not least, I would like to acknowledge all my family and friends for emotionally supporting me along the way and always encouraging me to chase my dreams.

Abstract

Information Security: A Scientometric Study of the Profile, Structure, and Dynamics of an Emerging Scholarly Specialty

Nicholas Victor Olijnyk

Heting Chu, Dissertation Advisor

The central aim of the current research is to explore and describe the profile, dynamics, and structure of the information security specialty. This study's objectives are guided by four research questions:

1. What are the salient features of information security as a specialty?
2. How has the information security specialty emerged and evolved from the temporal perspective?
3. What scholarly domains contribute to information security in light of the sources used by researchers from the specialty?
4. What is the intellectual structure underlying the specialty of information security?

Scientometrics techniques, including co-citation, co-word, and network analyses, constitute the research methodology for this dissertation. Bibliometric data, extracted from 58,908 Scopus document records for the period 1972-2014, were examined and analyzed quantitatively and qualitatively to address the research questions of this study. Specifically, descriptive statistics were employed to establish the information security specialty's profile and changes over time. One hundred of the highest cited documents and most frequently occurring keywords were used as the basis for multivariate and network analyses to determine the information security specialty's intellectual structure.

This scientometric study presents a comprehensive view of the information security specialty from different perspectives. After a long and steady period of growth (i.e., 1972-2001), an exponential publication output occurred in the decade of 2001-2010 reflecting a societal shift from industrialization to informationalization. Among all the countries involved in the information security research, the United States and China contributed the greatest number of documents in the specialty. Chinese researchers, however, had little impact on the specialty in terms of citation counts while American researchers topped the citation chart. Information security, as a specialty, received its vast majority of publications from the technical fields of

computer science and engineering. Upon closer examination of its intellectual structure, the current researcher discovered that the specialty was primarily dichotomous between technical and social domains because social or process-oriented research topics such as information security management held notable positions in the specialty along with technical topics (e.g., cryptography).

This dissertation research provides science managers with what they need to engineer an information security specialty that is better positioned to deal with information security threats and vulnerabilities. Amid its implications for high-level information security science managing, this study reduces the complexity of the specialty to controllable terms, supplies objective data for science policy making, identifies the most productive academic institutions, and demonstrates historical movements locally as well as internationally. At the lower level of information security research, it serves as an information retrieval tool to identify key authors, source titles, and documents and makes explicit the intellectual links between researchers, works, and research topics. Finally, it adds to the accumulated wealth of knowledge on the science of scholarly domains by shedding light on the nature of specialty development.

Keywords: Bibliometric Research, Computer Security, Cyber Security, Information Assurance, Network Security, Specialty Development

Table of Contents

List of Tables

List of Figures

1. Introduction

According to Bell (1974) and Castells (1996), society has shifted to an information age; this shift is underscored by a change in the economy from industrial-centered capital to information-centered capital, the emergence of new types of social relationships, a networked cyber infrastructure spanning the globe, and an emphasis on the exchange of information facilitated by the network (Keenan 2010). Society's most vital institutions and functions (e.g., governments, militaries, public infrastructure, education, financial, health) are now reliant on the flow of information via networked computer systems (Lord and Sharp 2011). As the reliance on cyber infrastructure has grown, so has the understanding that information is vulnerable to a variety of threats. According to President Obama (2009), “it’s now clear this cyber threat is one of the most serious economic and national security threats we face as a nation". Congressman Rohrabacher’s (2013, 2) statement during a recent congressional hearing referred to U.S. economic losses from information espionage as constituting “the greatest transfer of wealth in history".

Lord and Sharp (2011, 7) argue that information-centric attacks can go beyond economic losses and cause “physical destruction, and even loss of human life". Information warfare has already been used by nation-states on a number of occasions (Carr 2010; Clarke and Knake 2010). Additionally, common computer based threats to information (e.g., hacking, malware, phishing, theft of intellectual property) are not the sole domain of major world powers and can be accomplished by individuals or small groups with little resources or technical expertise (Chabinsky 2010). Suffice it to say, the Information Age has led to a serious and prevalent problem, namely, information security despite the many benefits it brings to humanity. Cooper et al. (2010b, 50) suggests that the “desire to continue to gain benefits of complex electronics

systems with the recognition of their inherent vulnerabilities has made information assurance a global priority".

While at the same time the Information Age has seen the growth of threats towards information, investment in information security has also been steadily on the rise. For example, the Department of Defense's 2013 budget appropriated $4.65 billion for cybersecurity initiatives, up 18% from the previous year (Capaccio 2013, 1). Corrin (2013) reports that "in some cases, such as cybersecurity research, investment grew by as much as triple over fiscal year 2012, according to budget documents". Investment over the last decade in information security research has facilitated the development of innovative information security technology. For instance, a series of state of the art intrusion detection systems, called *Einstein I, Einstein II and Einstein III,* has been developed by federal agencies to combat technical threats aimed at breaching the information security of nonmilitary federal government networks (Oree 2013). Yet, according to the Office of Management and Budget (2013, 18), phishing[1], a socially enabled threat, accounted for "68.3% of the total incidents reported". This is in stark contrast to more technical modes of information security breaches such as malicious code (i.e., malware) which account for only 5.8% of all information security threats.

As the above situation indicates, advances in technology do not always lead to a reduction in security breaches. Meushaw (2012, 1) asks the question: "how are such widespread problems possible after decades of investment in computer security research and development?" Researchers have attributed this disparity to the lack of coordination among the different research specialties in information security. In referring to information security research, Siponen and Oinas-Kukkonen (2007, 60) observe that, "scholars belonging to a certain

[1] The National Institute for Standards and Technology defines phishing as "tricking individuals into disclosing sensitive personal information through deceptive computer means". (Kissel, 2013, 142).

discipline, such as computer science, cryptology, computer engineering or information systems, often seem to have a poor awareness of the contributions made by researchers in other disciplines". Siponen and Oinas-Kukkonen further suggested that “this leads to fragmentation in the field of information security" (2007, 60). Solms (2001, 1) cautions, “that if information security is not addressed in a holistic and comprehensive way, taking all its dimensions into account, real risks exist preventing a really secure environment". While, Vaughn, Dampier and Warkentin (2004, 41) argue that “to focus on one aspect of a system security solution (e.g., the operating system) and omitting another area (e.g., policy) still leaves vulnerability in the system and the security solution fails". In other words, even the most advanced encryption technology solution, making decryption of secure passwords impossible, is of little use if the human element (i.e., the way in which a user manages his/her password) is not dealt with in an equally advanced way. Research has labeled the frayed intellectual structure of the information security specialty problematic (Crowley 2003; Hammonds 1993; Perez et al. 2011; Vaughn, Dampier and Warkentin 2004).

The previous paragraph indicates that there are disjointed research efforts within the information security scientific research community leading to systematic problems of which the symptomatic issues presented earlier are a result. To use an expression: one arm of the information security specialty may not know what the other arm is doing, leading to redundancy and diminished effectiveness. Botha and Gaadingwe (2006) suggest that information security could only effectively move forward if its history and current state are examined and understood. This type of problem is not about information security (i.e., the protection of information) per se; rather, it is more about the structure and behavior of information security as a scientific domain. In other words, this is a metascience problem that requires turning science upon itself. From this

perspective, it is hypothesized that improving the information security specialty as a whole will exponentially reap more benefits for information security than merely solving a single technical or policy issue. This is not to diminish the necessity for micro scale research, for it is the building block on which the macro scale sits. Theoretical foundations for framing such a problem have been laid out in the sociology of science (Bernal 1939; Kuhn 1962; Merton 1973). The development and appropriateness of using the scientometric methodology to investigate similar issues has been articulated by seminal researchers such as Garfield (1955), Price (1963), and Small (1978) and successfully utilized in many studies since (Chen et al. 2002; Moravcsik 1977; Persson 2000).

Therefore, the present study approached information security from a sociology of science perspective. More precisely, the investigation used the scientometric methodology to explore and describe the information security research domain. The subsequent four research questions guided the study:

1. What are the salient features of information security as a specialty?
2. How has the information security specialty emerged and evolved from the temporal perspective?
3. What scholarly domains contribute to information security in light of the sources used by researchers from the specialty?
4. What is the intellectual structure underlying the specialty of information security?

A more detailed discussion of this study's objectives and research questions will be presented in Chapter 4. Results from the present study, according to Garfield (1979), gives scholars and policy makers a view of the information security research landscape by which to

form future strategic decisions in support of improving research collaboration among the disparate research silos in the domain.

The next chapter provides some background information about scientometrics and information security so that a common ground is developed for the reader to better comprehend the subsequent chapters.

2. Background

2.1 Scientometrics, Bibliometrics, and Citation Analysis

The following section is a brief discussion of scientometrics and its relationship to bibliometrics, which includes citation analysis. More in depth coverage of these topics from a methodological perspective is presented in the Methodology chapter.

2.1.1 Scientometrics

Science, according to Merton (1973) and Kuhn (1962), is a social system that embodies a collective effort. As argued in Chu (1991), formal and informal communications between scientists produce and sustain this collective effort. Furthermore, science, as a social system, is underscored by what Weaver (1948) called, organized complexity. Price (1965), a historian of science, explained that science's variables, and their interactions, are numerous and complex enough that generalizations about science as a whole, stemming from the analysis of its particular variables, are inappropriate. However, at an aggregated level, the structure and behavior of science's variables are coherent enough to be viewed as organized. In this sense, Price (1963) approached the study of science from a physical science perspective (i.e., searching for natural laws). As a metaphor, Price (1963) argued that scientists study the behavior of gas in thermodynamics by observing gas under different conditions (e.g., various pressures, temperatures). In these instances, scientists are not concerned with the motion of particular molecules of the gas. Rather, these scientists take a holistic view and observe the emergent behavior of the molecules as they combine in great numbers to form the gas. Likewise, science can be studied in the same respect. In particular, citations to scholarly publications, standing on their own, may not be valid indicators of the structure and behavior of science. However, the accumulation of large quantities of such citations can, as with gas, produce emergent behavior

that can be observed using quantitative analysis techniques. It can also shed light on the structure and behavior of science as a whole.

The inside of a complex system, such as science, is too difficult to grasp directly. Therefore, scientometric research focuses on the input and output indicators of science. An indicator, as opposed to data, is succinctly explained by van Raan (2004, 21) in relation to citations as,

> The result of a specific mathematical operation (often-simple arithmetic) with data. The mere number of citations of one publication in a certain time period is data. The measure in which such citation counts of all publications of a research group in a particular field are normalized to citation counts of all publications worldwide in the same field, is an indicator. An indicator is a measure that explicitly addresses some assumption.

Indicators, as described in Price (1978), include, but are not limited to, measures from the cognitive dimension of science such as in the development of scholarly content and communication, i.e., the amount of articles published, the amount of citations between the articles, and the amount of patents granted. Price's (1978) cognitive indicators differ from other forms of demographic and economic scientific indicators. The National Science Review Board (1973) proposed these other forms of scientific indicators, for example, the number of research grants awarded to institutions, the number of scientific degrees conferred, the amount of scientists working in a research area, the amount of money invested in a scientific area, and the monetary profit from scientific research. Scientometrics investigates science by focusing on its input and output indicators with the explicit aim to "analyze, quantify, and measure communication phenomena to build accurate formal representations of their behavior for explanatory, evaluative, and administrative purposes" (De Bellis 2009, 3). Statistical techniques play a central role in scientometrics, but scientometrics is not limited to quantitative methods.

The qualitative selection and interpretation of data is also a necessary part of scientometric analytical techniques.

2.1.2 Bibliometrics

As illustrated in Figure 2.1, bibliometrics is a research method that, at times, can be seen either overlapping or diverging from scientometrics.

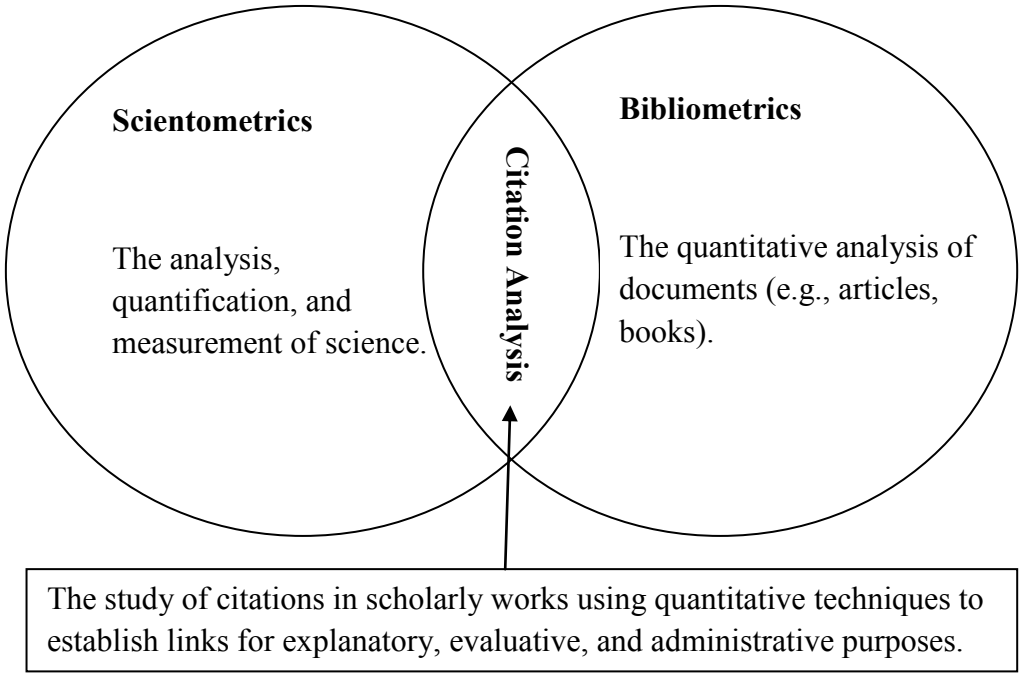


Figure 2.1 An Illustration of the Relationship Among Scientometrics, Bibliometrics and Citation Analysis

Biodato (1994, viii) defines bibliometrics as "the mathematical and statistical analysis of patterns that arise in the publications and use of documents". Scientometrics overlaps with bibliometrics when scientific communication, often through formal channels, (e.g., publications) and sometimes through informal channels (e.g., phone conversation and face-to-face chat), becomes the subject of analysis (Mikhailov, Chernyi, and Giliarevskii 1984). In this scenario,

scientometrics uses bibliometric and other data to investigate the structure and behavior of science. In contrast, bibliometrics need not focus on science as a research target. Likewise, scientometrics does not have to use bibliometric data in its methodology. Bibliometrics would study specific authors, institutions or ideas that may or may not involve science. Moreover, bibliometrics does not look to draw conclusions about science based on bibliometric data.

2.1.3 Citation Analysis

Scientometric research often involves the use of citation analysis, which is commonly regarded as one major part of bibliometrics. Invisible Colleges, as discussed in Crane (1972), create scientific specialties and informal networks of scholarly communication. Scientists build on and refine each other's work, gradually leading to the development of specialized areas of research within scientific disciplines. The term 'citation' usually refers to both reference and citation in the context of citation analysis. The use of citations, a synonym of references, is vital in this process. Citation analysis deals with the expressed connection between two documents, that is, either giving acknowledgment or receiving acknowledgment.

De Bellis (2009, 55) regarded the bibliographic citation as the "atom of recognition" and Garfield (1955, 108) referred to it as the "sub micro or molecular unit of thought". Price (1963) realized the utility of using citations as a reliable source of data in studying the social structure and behavior of science as it evolves. Price (1965) envisioned using citations to develop large topical maps of science that could be used for strategic and administrative purposes. These maps, according to Price (1965), could be refined to study the intellectual structure and behavior of science by looking at specific sources, authors, countries, documents, and specialties. This understanding has led to many scientometric studies seeking to understand scientific specialties

by researching their citation networks (e.g., Chen, McCain, White and Lin 2002; Moravcsik 1977; Persson 2000).

2.2 Understanding Research on Information Security

Although similar in many respects, the terms 'information security' and 'information assurance' are not synonymous. Both terms represent fields that desire, in one way or another, to protect information by creating information security systems using a combination of physical, technical, legal, and social instruments. However, information assurance is the broader of the two as it incorporates information security as a sub-domain. Both of these research areas, as discussed in Blyth and Kovacich (2006), Crowley (2003), and Maconachy al., (2001), can be placed in the broader domain of information operations— otherwise referred to as information warfare. Nevertheless, it should also be noted that in certain domains (e.g., business) information assurance can be found performing functions outside of the scope of information warfare. The following sections will clarify information security and information assurance and briefly discuss the historical development of research on these closely related scholarly domains.

2.2.1 Information Security and Information Assurance

The Department of Defense defines information security, or INFOSEC, as, "the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing or transit, and against denial of service to authorized users" (Department of Defense 2010, 175-76). Over two decades ago, McCumber (1991) laid out an argument and a model, illustrated in Figure 2.2, viewing INFOSEC as a complex phenomenon requiring the integration of multiple dimensions.

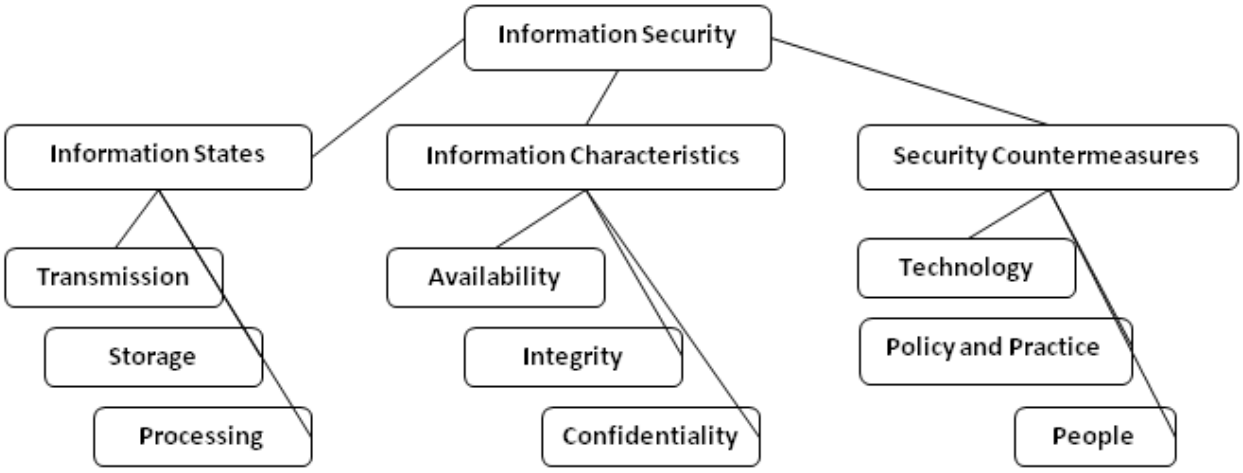


Figure 2.2 An Information Security Concept Map.[2]

In making his argument, McCumber (1991) stressed the importance of acknowledging that it is "information" at the center being secured. During the twentieth century, information and communication technology, mainly in the form of computers, increased in popularity. Consequently, there was a corresponding evolution of INFOSEC as it splintered, giving rise to other specialties, for example, computer and cyber security (Solms and Niekerk 2013). McCumber (1991) reacted to the focus on computer security by arguing that information must remain at the center of INFOSEC, regardless of the mode in which that information exists. He went on to warn, "in this sense, any paradigm which emphasizes the technology at the expense of information will be lacking" (McCumber 1991, 1).

Maconachy al., (2001, 1) suggested that originally, INFOSEC was "an attempt to integrate here-to-fore separate disciplines such as personal security, computer security, communication security and operational security, into a coherent identifiable profession". Following McCumber (1991), Maconachy al., (2001) argued that the field of INFOSEC, described by McCumber's (1991) model, had evolved into the broader field of information

[2] This figure is a concept map derived from McCumber's (1991) information security model that served to delineate the relationships and structure among information security dimensions.

assurance, or IA in brief. IA, according to the Department of Defense (2010, 175), can be defined as, “measures that protect information and information systems by ensuring the availability, integrity, authentication, confidentiality and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities”.

Although authoritative sources, such as the Department of Defense, have laid out definitions for IA and INFOSEC, Blyth and Kovacich (2006) suggest that there remains debate about the meanings and overlap of these concepts. On the one hand, IA and INFOSEC include the protection of information against accidental or intentional threats. Yet, IA also incorporates areas that are not covered by INFOSEC, for example, perception management, which deals with the intended cognitive interpretation of information. According to Blyth and Kovacich (2006, 4), IA operates at three levels, “physical, information infrastructure, and perceptual,” while INFOSEC is concerned with information in logical form (i.e., comprehensible pattern that conveys a message) and physical form (e.g., paper documents or computer hardware that are mediums for the message). Maconachy al., (2001) asserted that INFOSEC is a subset of IA. It is easy to see the potential for confusion with such overlapping concepts. Blyth and Kovacich (2006, vii) attributed the confusion to IA being a recent development, while INFOSEC dates back to “the birth of the computer”. As displayed in Figure 2.3, the present study carefully considers the overlap of INFOSEC and IA.

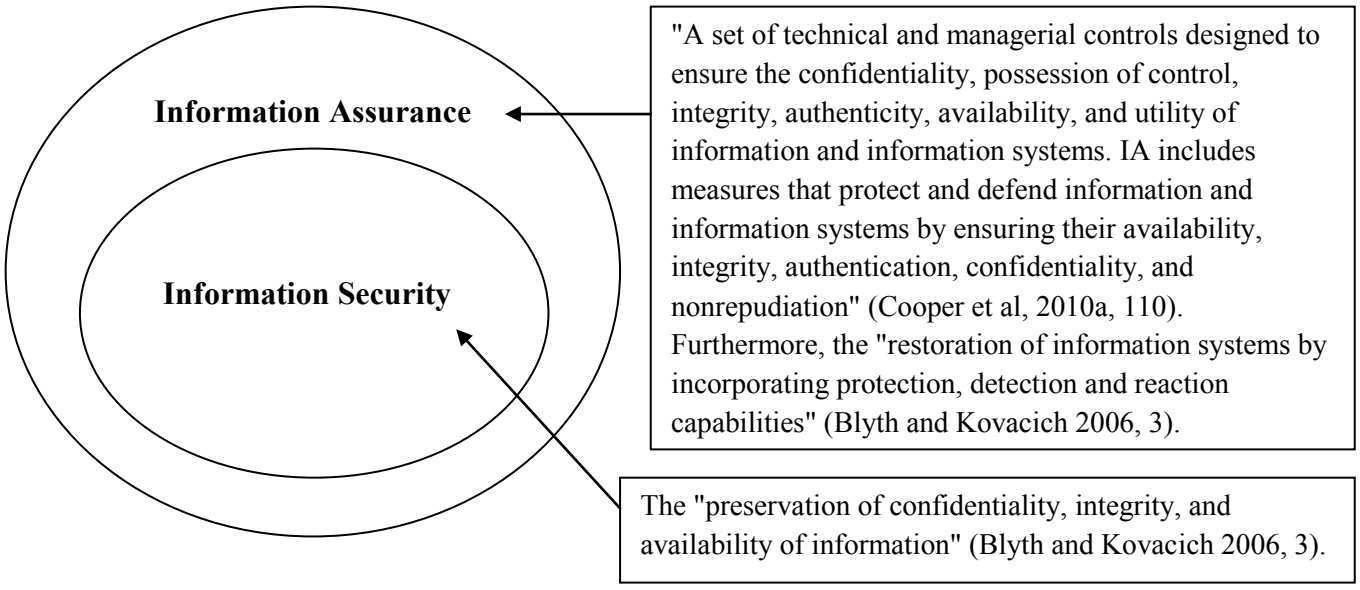


Figure 2.3 An Illustration of the Relationship Between Information Security and Information Assurance

Taking into account their overlap, the present study used the term INFOSEC (i.e., information security), but also, when appropriate, refer to IA as INFOSEC is the older of the two terms and more readily used when referring to security matters involving information. Having already discussed the terminology and concepts surrounding INFOSEC, the following sections will present a short historical review of research on INFOSEC, which will benefit readers by laying additional ground before the study moves further. Moreover, a more thorough historical description of research on information security is presented in Appendix A.

2.2.2 A Brief History of Information Security Research

Efforts to protect information, in one way or another, have likely been around as long as humans have recognized the value of information. Thanks to Khan's (1996) seminal work, historical records indicate that cryptology, an INFOSEC specialty, was being used around 3000 years ago. Cryptology is the study of cryptanalysis (i.e., the science of decrypting hidden

information) and cryptography (i.e., the science of encrypting information). The majority of people in many ancient societies were illiterate, thus there was no need to refine cryptological techniques. There is not much known about the role of cryptology in ancient societies, but records show that it was used in a very basic way in Ancient Egypt, China, Mesopotamia, Assyria, Babylon, Greece, and Rome (Kahn 1996).

In the ninth century, Arab scholars would be the first to approach cryptology in a scientific manner. Al-Kindi's (801-873 AD) *Treatise on Cryptanalysis* is considered by Mrayati, Alam, and at-Tayyan (2003) to be one of the first publications detailing the use of frequency analysis in cryptanalysis. Scientific coverage of cryptology would not surface again until the Italian Renaissance (14th-16th century). Like Al-Kindi, Alberti's (1466) *Treatise on Ciphers* dealt with the use of frequency analysis for cryptanalysis. Alberti is also credited with the invention of the cipher disk, an instrument for cryptography (Alberti, Buonafalce, Mendelsohn, and Kahn 1997).

Bauer (2007) suggested that technology permitted the development of mechanical devices for cryptology around the early 1900s. These devices, known as rotor machines, drastically increased the complexity of secured cryptographic messages. The invention and widespread use of wireless radio communication, in conjunction with the need for government secrecy during WWI, prompted the development of electromechanical rotors (most notably, the German ENIGMA machines.) Communication security, a subcomponent of INFOSEC, heavily reliant on cryptology, became a top priority for nations engaged in WWI.

Shortly after WWI, WWII began and once again, created a necessity for research and development on INFOSEC. Bauer (2007) pointed out that in 1938, an electromechanical cryptanalysis machine, called the Polish Cryptologic Bomb, was built by Marian Rejewski to

counter the advantage of ENIGMA. Increasingly more sophisticated cryptographic systems were being built by the Germans. This motivated the British, as discussed in Copeland (2007), to create the first fully electronic programmable digital computer system called Colossus. Research on communication security was also a priority for the Americans; it was especially important for those working at Bell Labs during WWII. In particular, Shannon (1945) produced, among his many seminal works, the classified article, *A Mathematical Theory of Cryptography*; this was later republished in a declassified version in 1949 as "Communication Theory of Secrecy Systems". Shannon (1949) investigated and found the mathematical requirements for constructing an unbreakable cryptographic system.

The development of the computer, particularly the U.S. military's Electronic Numerical Integrator and Computer (ENIAC), dramatically changed INFOSEC research. It is at this point, according to Whitman and Mattord (2009), research on INFOSEC largely shifted from communication security to computer security. The emergence of computer security as an INFOSEC research direction is underscored by a focus on securing computer infrastructure, as opposed to securing information. At this early phase, computer security was mainly accomplished by applying physical security measures that protected against sabotage and espionage. Moreover, physical threats, such as compromising emanations (i.e., the ability to eavesdrop on and decipher the electromechanical radiation emanating from computers) led the U.S. National Security Agency (NSA) to develop one of the first computer security standards, called TEMPEST (Yost 2007). TEMPEST required that computers be secured with radiation shields or placed in Secure Compartmented Information Facilities (SCIF).

In the 1950s, with the development of digital computer network technology, there was another significant shift in research on INFOSEC. The focus on physical security and computer

infrastructure turned towards network security. Networked computer system technology, as pointed out in DeNardis (2007), was dramatically on the rise: the Semi-Automatic Ground Environment (SAGE) system, a product of IBM and MIT created for the U.S. Department of Defense (DoD), MIT's Multiple Access Computer (MAC), which introduced computer time-sharing technology, and the Advanced Research Project Agency Network (ARPANET), a precursor to the Internet, developed by the DoD's lead researcher Larry Roberts. Large-scale computer networks, providing resiliency through redundancy, became a main line of homeland defense for U.S. military command and control during the Cold War. However, computer network technology development outpaced network security. Metcalfe (1973) published a paper, *Packet Communication*, pointing out fundamental security issues with ARPANET.

Following Metcalfe (1973), Bisbey and Hollingworth (1978) performed a comprehensive investigation, titled *Protection Analysis: Final Report,* into the security vulnerabilities and detection techniques of computer operating systems. One year later, Ware (1979) published, on behalf of the RAND Corporation and the DoD, a landmark study, titled *Security Control for Computer Systems: Report of Defense Science Board Task Force on Computer Security.* Researchers, namely Yost (2007), assert that Ware (1979) should be viewed as one of the most important and comprehensive studies to its date on INFOSEC. Ware (1979) investigated the shift from smaller closed computer network environments to large-scale open networks. This shift, as argued by Ware (1979), needed to coincide with a shift in research on INFOSEC from a focus on computer infrastructure, back to a focus on securing information in computer systems.

Cryptology, with its focus on securing the information in systems, steadily advanced to protect the information flowing over open computer networks. Feistel (1973) published, "Cryptography and Computer Privacy", a paper that would eventually lead to the Data

Encryption Standard (DES) adopted by the U.S. National Bureau of Standards. Diffie and Hellman (1976) produced an important work, entitled "New Directions in Cryptology," which presented a theoretical solution to secret key distribution, a problem for the one-time pad (i.e., a cryptographic technique). Rivest, Shamir, and Adleman (1978) put Diffie and Hellman's (1976) theoretical work to practical use with their development of a practical cryptographic algorithm, labeled RSA.

Over the last decade, computers have taken center stage in a variety of forms, whether for individual use (e.g., personal desktops, tablets, smart phones) or for use by society at large (e.g., industrial control systems: energy creation and distribution, water treatment facilities, transportation, telecommunications, military logistics). These systems have become networked to one another resulting in a massive and highly complex system that sustains contemporary living. Cyberspace, the term used to refer to this massive system, has been designation by the DoD (2011) as a new domain of war. Such a designation suggests that the U.S. government is galvanizing its resources to focus on INFOSEC as a main national strategic objective. President Obama (2009) has made it clear that the extent to which contemporary society, in particular the U.S., has become dependent on cyberspace has outpaced the level of INFOSEC needed to protect it. Shea (2003) outlined the vulnerabilities of U.S. society due to the level of integration between its most vital functions and cyberspace. As in the past, the major drivers (e.g., funding, agenda setting) for research on INFOSEC are coming from government.

The Executive Office of the President of the United States (2009; 2010) has investigated the nation's cybersecurity posture and set out national research objectives for INFOSEC. These objectives have been formulated into specific research goals and themes through the Cybersecurity Information Assurance Interagency Working Group (2010) and the National

Science and Technology Council (2011). Furthermore, as the lead agencies in charge of securing federal information systems, and to some extent, private information systems, the NSA and the Department of Homeland Security (DHS) have put forth a joint initiative called the National Center of Academic Excellence in Information Assurance Education and Research. The goal of their initiative is to promote higher education and research into INFOSEC by setting agendas and creating research partnerships between government, private industry and academia. There is no doubt, that over the last decade, the acknowledgement of the vulnerabilities and threats facing society from cyberspace and the consequent focus of national resources towards research on INFOSEC have had a marked impact on the field of INFOSEC. The only question is, 'how?'

3. Literature Review

The present chapter is a review of prior studies on scholarly specialties and other scholarly entities (e.g., fields, disciplines), including those that have specifically examined information security. Studies such as these have mainly, but not exclusively, used scientometrics/bibliometric methodologies. The proceeding sections are organized into four sections: emergence and research fronts, evolution, contributing domains, and scientometric/bibliometric studies on information security.

3.1 Research on the Emergence of a Specialty and Research Fronts

Emergence, as defined by Goldstein (1999, 49), "refers to the arising of novel and coherent structure, patterns, and properties during the process of self-organization in complex systems". Similarly, Templeton and Fleischmann (2013) described emergence as the systematic process by which a new upper-level entity comes into existence from the synergistic interactions of lower-level entities. The sociology of science views science as a social system (Merton 1973), often highlighted in terms of its underlying communication infrastructure. Thus, studying the systematic fluctuations of science is accomplished by focusing on units of analysis such as citations, authors, articles, and journals that stem from science's scholarly communications. Templeton and Fleischmann suggested taking a broader view of the emergent behavior observed by bibliometric/scientometric studies; one that considers the ways in which things outside of science (e.g., in nature) emerge. Research fronts are often viewed as new areas of interest that sprout within a field (Diodato 1994).

The culmination of research areas involving "metrics" (e.g., scientometrics, bibliometrics, and webometrics) has been investigated by Milojevic and Leydesdorff (2012). The researchers found three telltale signs that a new metric based scientific discipline was emerging:

firstly, metric literature had steadily increased over the last decade; secondly, a core of researchers was identified; and thirdly, shared problems, methods, and vocabulary were identified. In another study, Zhao and Strotmann (2008) found that information science research areas such as scholarly communication and the Web disappeared between 1996 and 2000, while others (e.g., Webometrics) sprouted into well-defined specialties. Ponzi (2002a), in his dissertation on the development of the knowledge management specialty, used bibliometrics to identify its emergence from organizational sciences literature. Using content analysis of bibliometric data, Ponzi also determined that computer science and business studies contributed to the early development of knowledge management as a specialty.

In relation to strategic management research, Ramos-Rodriguez and Ruiz-Navarro (2004) found that classic works were declining in citedness between 1980 and 2000. According to the researchers, this is an indication that the foundational knowledge contained in those works has been accepted as standard and strategic management is "coming of age" (Ramos-Rodriguez and Ruiz-Navarro 2004, 1001). In addition, one prolific author (i.e., Michael E. Porter) who laid down a number of highly used models was found to have played a central role in the establishment of strategic management as a specialty. In a similar study, Fernandez-Alles and Ramos-Rodriguez (2009) argued that since human resources management was dominated by published books instead of journal articles, its scientific research is not mature and needed to grow. Charvet, Cooper, and Gardner (2008), analyzing supply chain management, found that it had an immature intellectual structure and did not yet have convergence of thought. Moreover, the field's different streams of research did not share a common definition of supply chain management, a common understanding of the business processes involved, or functional area involvement. The different research streams, as reported by Charvet, Cooper, and Gardner, did

not have a similar base theory and were observed being held together, merely, by a parent discipline.

Casillas and Acedo (2007), using co-citation analysis of family business research, found that, although having fragmented literature between 1988 and 2005 and having intense debates about fundamentals, family business appeared to have a large number of research approaches contributing to its aims. Thus, it was argued to be sprouting as a new research frontier. Coming from a different direction, Teixeira (2011) investigated entrepreneurship in terms of its invisible colleges i.e., informal scholarly groups that emerge and communicate about the formation of a specialty (Crane 1972; Price 1961). Teixera (2011) observed that while entrepreneurship's invisible college is steadily becoming more "autonomous, legitimate, and cohesive" (1), its move towards independence as a scientific specialty has been challenged by "fragmentation and specialization" (33). Core researchers, as reported by Teixeira, had been producing substantial core reference research allowing others to coalesce and laying the groundwork for independence from parent fields such as management and economics. Teixeira noted that the national research hegemony by English speaking researchers, particularly in the United States, marked a barrier for widespread international network growth. Durisin and Puzone (2009) illustrated a similar example of specialty emergence with a closely related research area. Corporate governance, according to Durisin and Puzone (2009, 284), had emerged as a viable specialty because, "there is a common body of knowledge influential across contributions from economics, management, finance, law, and accounting".

In reference to the emergence of the nanotechnology field, Leydesdorff and Zhou (2006) showed by using a journal delineation technique that from the year 2003 to 2004 the core set of journals had increased while merely relevant sets of journals had decreased. Furthermore, the

authors argued that this evidence indicated that nanotechnology was experiencing codification, as is also evidenced from its focused citation behavior. From a different perspective, Kajikawa and Takeda (2009) searched for emerging research domains within the organic light-emitting diodes field. The authors ran recursive co-citation analysis to cultivate cluster groups and found two-tight research groups in organics and polymers. West (2003), in his dissertation, studied instructional technology by comparing it to the field of information science via historical analysis and by performing a content analysis of university course catalogs. West's two methods produced conflicting results. The historical analysis revealed that the field was still immature and defining itself, while the content analysis of course catalogs showed that there was, indeed, a burgeoning set of core courses set out for instructional technology students. Jackson (2012), also as dissertation work, tracked the slow emergence of green energy research via a number of journals while Breitenstein (2003) traced the emergence of visual literacy by analyzing a decade of the specialty's conference proceedings in her dissertation research. Jackson concluded that journals play a central role in the diffusion of scientific ideas and sustaining the viability of an emerging specialty. Breitenstein concluded that setting the boundary of her analysis on a specialty's central scientific association and its conference proceedings revealed a clear picture of the specialty's emergence.

New research areas, sometimes discussed in terms of emerging research fronts, have also been seen emerging from within well-established fields. Natale, Fiore, and Hofherr (2012), for example, combined latent semantic analysis, topic modeling, and co-citation analysis techniques to study aquaculture research fronts. Co-citation analysis worked in a complementary fashion with other techniques, as reported by Natale, Fiore, and Hofherr, and was able to give a specific view of the emerging research fronts in relation to a global map of topics. Co-word analysis, as

argued in Jeong and Kim (2010), can overcome many of the limitations set forth by citation analysis when dealing with fields that have low citing activity. For example, Bhattacharya and Basu (1998) used the co-word analysis technique, which, according to the authors, was the most optimal technique to analyze micro level entities and uncover emerging research fronts in condensed matter physics. However, the authors also found that co-word analysis without adequate word filtering might create categories that did not represent specialty topics. Bhattacharya and Basu, from another angle, suggested using only high-ranking words to avoid the accumulation of useless word blocks.

In summary, information scientists have characterized the emergence of a research specialty as the "birth of a notion" (Morris 2005, 1252) and argued that it usually correlates with a high proportion of self-citations (Tabah 1999). Emergence was described by Goldstein (1999, 50) in a comprehensive manner and characterized with five indicators: "radical novelty" (unanticipated features of an emergent complex system come into existence that were not previously there), "coherence or correlation" (the emergent complex system begins to maintain some type of stable identity over time and correlates lower-level components into a higher-level organization, "global or macro level" (there is a distinct behavior of the emergent entity as a macro-level organization), "dynamical" (the emergent entity is highlighted by fluctuations stemming from the interactions of new attractors), and "ostensive" (emergent entities show themselves in some unique fashion). In regards to research fronts, Braam, Moed, and Raan (1991) observed that research fronts correlate to a high degree of density with publication and citation behavior; Moya-Anegon, Jimenez-Contreras, and Moneda-Corrochano (1998, 230) argued that this has two consequences: research fronts represent particular areas of focus within

disciplines and research fronts are identified by "the sum of contributions of the set of authors within a discipline", not by the decisions made by a single or a small group of researchers.

3.2 Research on the Evolution of a Specialty/Discipline

Kuhn's (1962) model of science purports that science evolves in a cyclical fashion. In the context of bibliometrics/scientometrics, Morris (2005, 1251) labeled the model "punctuated equilibria" and suggested it resembled "biological evolution". Morris' version of scientific development explains the evolutionary process in four stages: Stage one exhibits puzzle solving-activities, status quo, and "normal science"; stage two is illustrated by the introduction of new knowledge (derived empirically, logically, or methodologically) that causes intellectual conflict; stage three presents a paradigm shift induced by the new knowledge and replacing the old; stage four, a rebirth, reveals a new set of scientific problems to solve and methods to approach them. It has been argued, and largely substantiated (Garfield, Malin, and Small 1978; Garfield 1979), that this evolutionary cycle is isomorphic to that of the life cycle of scientific specialty literatures.

In regard to specialty evolution, Chen, Fang, and Borner (2011) investigated the field of scientometrics based on bibliographic data extracted from issues of the international journal, *Scientometrics,* between the years 2002 and 2008. Their research was particularly focused on mapping out contributions to scientometrics from the perspective of international geographical regions. In a similar study, Chen et al. (2002) centered on the relationships between countries, institutions, and authors via social network analysis. The *Web of Science* was used by Chen et al. to extract bibliometric data from articles published in *Scientometrics* between the years 1981 and 2001. The authors were particularly interested in exploring and validating the use of information visualization tools for scientometric research. Chen et al. (2002) approached bibliometric data using animation display techniques combined with co-word and co-citation analysis. The authors

found that this combination effectively reduced complexity and increased comprehension of the dynamics involved with the field's historic and evolutionary dimensions. Schubert and Maczelka (1993, 578) analyzed research article references in *Scientometrics* over two time intervals (1980 to 1981 and 1990 to 1991) resulting in a historical view illustrating that the field of scientometrics underwent a "crystallization process" in which it moved from soft to hard science over the two time periods.

Patra, Bhattacharya, and Verma (2006) analyzed the field of bibliometrics, focusing on its growth patterns, core journals, and prolific authors. The researchers found no definite pattern among growth literature, author productivity was not consistent with Lotka's law, and *Scientometrics* was seen as the premier journal in the field. In another study, Mulla (2012) analyzed the productivity of information science and scientometrics in India from 2005 to 2009. The authors found, via citation analysis, that this area of research had experienced dramatic change and exhibited multidisciplinary and interdisciplinary research behavior. White and McCain (1998), in their analysis of information science with a data set spanning 24-years, highlighted the changes in author positions in three 8-year intervals underscoring the fluctuations between the eminence and influence of information science's various specialties. Similarly, Zhao and Strotmann (2008) studied the evolution of information science from 1996 to 2005 in two 5-year intervals. They found that one research camp (i.e., literature study) was static while another research camp (i.e., information retrieval) underwent restructuring. In a longer historical view of the LIS field, covering a century, Lariviere, Sugimoto, and Cronin (2012) found that the field had diminished stature in the social sciences and humanities regardless of its increased research productivity. More recently, however, the field exhibited a high degree of collaborative authorship with other fields, consequently, increasing its influence.

Information retrieval was studied by Rorissa and Yuan (2011) in terms of its evolution from 2000 to 2009. The researchers found that co-authorship and collaboration patterns illustrated a linkage between highly productive authors and those who exerted greater intellectual influence. Furthermore, Rorissa and Yuan's results indicated that in the later years, information retrieval research areas were expanding into areas not previously covered towards the early 2000s. Rowlands (1999), using co-citation analysis on literature between 1972 and 1997, studied the evolving structure of information policy, another information science specialty. The author further validated his findings by sending out a customized postal questionnaire to experts in the information policy field. The two methods corroborated each other's results suggesting that the intellectual structure of information policy research is highly converging. Ponzi (2002a; 2002b) and Gu (2004) investigated the evolution of knowledge management. Ponzi found that it evolved through three distinct stages: origin and formation (1991 to 1995), an exponential growth period (1996 to 1999), and contraction and rebound (2000 to 2001). The data collected confirmed the bell shaped, three-stage evolution of knowledge management Ponzi reported. In another set of studies, Peritz (1980-81; 1981) performed a historical analysis of library science. The author found that there was an explosive increase in research output between 1960 and 1970. Peritz further concluded that library science predominantly used survey and experimental research methodologies.

The historical evolution of China's LIS field underwent author co-citation analysis from 1998 to 2007 (Ma 2012). The study found that some of the specialties within the field had emerged and increasingly developed, for example, Webometrics and competitive intelligence. While other specialty areas, such as bibliometrics and intellectual property, are in stasis and further specialties have steadily declined (e.g., cataloging). In another longitudinal study of the

field, Hu et al. (2011) used journal co-citation analysis concluding that although the 24 library science and information science journals under analysis exhibited homogeneity, the fields of library science and information science were not always intellectually overlapping and were still steadily moving towards each other. Moreover, the authors argued that their relationship is not balanced and library science holds the dominant position, potentially revealing a disparity between the fields in China compared to the west, where information science was found to be dominant (Astrom 2010; Moya-Anegon, Herrero-Solana, and Jimenez-Contreras 2006).

Zong et al. (2013) viewed the LIS field from the perspective of its dissertations via a co-word analysis covering 1994 to 2011. The authors analyzed the data using cluster analysis, strategic diagramming, and social network analysis. The results indicated that Chinese doctoral dissertations included an array of topics. Additionally, the authors also found that newly established research areas were still maturing and core research areas were few. From another ancillary direction, Zhao and Zhang (2011) and Liu, Hu, and Wang (2012) investigated digital library research using co-word analysis. Zhao and Zhang found that research in the area of Chinese digital libraries exhibited different characteristics in various periods. On the other hand, Liu, Hu, and Wang aggregated the longitudinal data but failed to address the dynamic development in digital library research. Liu, Hu, and Wang did, however, illustrate and concur with Zhao and Zhang in reporting that Chinese digital library research was without a research center.

Ramos-Rodriguez and Ruiz-Navarro (2004) and Nerur, Rasheed, and Natarajan (2008) studied strategic management research using bibliometrics and co-citation analysis. Looking at the field from the view of its publications, Ramos-Rodriguez and Ruiz-Navarro split the years between 1980 and 2000 into three intervals in order to see shifts in the literature. The researchers

found that works published in book form had the strongest influence in the earlier intervals, yet the usage of articles from journals appeared to be steadily increasing in later years. Moving towards a different unit of analysis (i.e., author), Nerur, Rasheed, and Natarajan found that there was a theoretical shift in strategic management from the dominant influence of organizational theory and industrial organizational economics to a fragmentation of the field. The fragmentation, as the authors suggested, resulted from the introduction of exogenous theoretical influences, leading to endogenous theoretical changes. The researchers further found that the field had clear research communities tied together via disciplinary origins and similar research problems, yet the communities were still separated by structural holes. Some authors, termed, "brokers", were found to navigate the different communities surpassing the holes and becoming pervasive throughout the field. (Nerur, Rasheed, and Natarajan 2008, 332).

Other management fields have also been the subject of longitudinal analysis. In line with Ramos-Rodriguez and Ruiz-Navarro (2004), Fernandez-Alles and Ramos-Rodriguez (2009) found that human resources management was also dominated early on by books, as opposed to articles, and its scholarly communication shifted from mostly using books between 1960 and 1990 to using journal articles between 1985 and 2000. Kumar and Mohad (2013) studied Malaysian business and management research as a network and found that author productivity was inconsistent with Lotka's law and co-authored papers were cited twice as much as single authored papers. Moreover, the mean number of authors per article had nearly doubled over the three decades under analysis. Durisin and Puzone (2009) investigated whether or not corporate governance research, represented by its literature from 1993 to 2007, had become an independent specialty. They found that the field increased in sophistication, depth, and rigor, as evidenced by its thematic consistency, emerging subfields, author relationships to one another, and publication

patterns. Business studies was approached by Wuehrer and Smejkal (2012) from the perspective of a longitudinal analysis of its conference proceedings. There was little uniformity over the years in each conference, shedding little light on the actual composition and change of the field but more light on the conference agenda.

Viewing business-to-business marketing research, Backhaus, Lugger, and Koch (2011) revealed that its structure evolved along a highly dynamic path in the 1970s and 1980s. At first, this was underscored by intense exchanges of ideas as seen through high citations and then data indicated that there was a declining pace highlighted by diversification of subfields in the later years. Georgi, Darkow, and Kotzab (2010) researched the evolution of the business logistics field from 1978 to 2007 in three intervals. The researchers found that works on methodology and theory emanating from the marketing field heavily influenced business logistics, as indicated through citation patterns towards the last decade. Moreover, there were clear shifts in subject areas over each interval. Due to their overlapping research areas, Georgi, Darkow, and Kotzab's study can be compared to Charvet, Cooper, and Gardner's (2008) research on supply chain management. Although the two studies were found to be largely congruent when considering both sets of findings, cluster separation can be delineated between clusters containing logistics and supply chain management research aiming at managerial issues on the one hand, and operations issues on the other hand. Pilkington and Meredith (2009), focusing on operations management, found that significant changes occurred in each decade between 1980 and 2006. In specific, there was a notable shift from tactical topics towards a more strategic macro focus involving changing research methods and techniques. Moreover, 12 emerging research groups based on authors were plotted and tracked in time as they shifted their research aims. Shafique (2013) studied the knowledge base of innovation research between 1988 and 2008 and found that

it was splitting in two between the economics and management domains. Zhu and Guan (2013), using a social network approach on innovation research between 1992 and 2011, produced results inconsistent with that of Shafique's conclusions. Service innovation research, according to Zhu and Guan (2013, 1211), had many contributing research domains, namely, 'business and economics, engineering, public administration, operations research and management science, and computer science".

The field of computer science underwent investigation in two studies: one specific to Malaysian computer science research (Abrizah and Wee 2011) and the other to Indian computer science research (Gupta and Dhawan 2005). In the first study, Abrizah and Wee (2011) observed that computer science's overall publication output increased consistently from 23 in the year 2000 to 142 in 2010. Furthermore, Abrizah and Wee reported that author productivity deviated from Lotka's Law, and there were a total of 1662 authors that contributed to 903 studies over an eleven-year period. Only a few (14%) authors wrote more than 10 papers and most (74.4%) produced a single publication. Multi-author papers ranked first at 54.9% among the various authorship pattern categories (e.g., single-author, two-author, multi-author, and mega-author) rising dramatically in 2008 (Abrizah and Wee 2011). In the second study, Gupta and Dhawan (2005) investigated the evolution of computer science over a 7-year period aiming to uncover its publication output, areas of strengths and weaknesses, leading institutions, and prolific authors. The Researchers used data from the *Institute of Engineering and Technology*'s INSPEC database from 1994 to 2001. Gupta and Dhawan were expecting to see a sharp rise in research over the time period as a result of heavy R&D investment in the information technology sector. Nevertheless, this was not the case as the rise in publications was found to be marginal going from 2299 papers published in 1993-1997 to 2391 articles in 1998-2001 (Gupta and Dhawan

2005). Additionally, subject area publications such as computer hardware, computer software, computer applications, and general management topics were observed rising in 1993-1997 and in 1998-2001.

The evolving structure of similar ancillary computer science related specialties such as artificial intelligence (Besselaar and Leydesdorff 1996) and neural networks (Raan and Tijssen 1993) have undergone investigation. Besselaar and Leydesdorff (1996) used 5 divergent opinions from experts in the field of artificial intelligence (AI) as the basis by which to formulate hypotheses. In addition, Besselaar and Leydesdorff analyzed aggregated journal-to-journal citations and constructed maps depicting the shifting paradigmatic phases in AI research. The study's results illustrated that early on, just before 1986, AI was unstable and in a preparadigmatic phase; moreover, between 1986 and 1988, AI entered a new and increasingly stable phase, eventually becoming more pronounced and clearly distinct as a field towards 1988 (Besselaar and Leydesdorff 1996). In all the years under analysis, Besselaar and Leydesdorff observed that AI had a consistent set of core contributing scientific specialties, namely pattern analysis, computer science, and cognitive psychology. Raan and Tijssen (1993) investigated the next specialty, neural network research via co-word analysis covering two time periods, 1981-1984 and 1985-1988. The co-word technique was used to construct maps of neural network research illustrating, as reported by Raan and Tijssen, its highly interdisciplinary nature. The first map (1981-1984) was characterized by much less publications than the second map (1985-1988), underscoring the growth of the specialty. Additionally, Raan and Tijssen (1993, 179) suggested that there was a "remarkable distinction between neural network research and artificial intelligence research", irrespective of their intellectual overlap.

Nanoscience has been an area to undergo heavy analysis by scientometricians in terms of its evolution. Karpagam et al. (2011) focused on Indian nanoscience research productivity from 1990 to 2009 and found quantitative measures are not sufficient to draw real conclusions about the growth of the field. Mohammadi (2012) performed a similar longitudinal study aimed at nanoscience in Iran via text mining in 1974-2007 and found that Iranian nanoscience research had undergone dramatic growth in the last decade. Using mapping techniques, Chen and Guan (2011) plotted the exponential growth of nanopharmaceutical research from 1991 to 2008. Furthermore, the researchers showed that the United States and China were the leading contributors, respectively, and drug development was the main stream of research. Pouris (2007) approached South African nanoscience research from 2000 to 2005 revealing that nanoscience researchers largely publish independently, and nanoscience is in its early stages of development despite signs of high research output. Larsen (2007) focused on nanostructured solar cell research using co-authorship networks and social network analysis. Larsen reported that having had a central author or set of authors to promote international collaboration expedited and supported the evolution of nanostructured solar cell research, turning it into a burgeoning specialty. Bajwa, Yaldram, and Rafique (2013) analyzed research trends in nanoscience and nanotechnology from 2000 to 2011with a focus on specialty evolution. The authors used bibliometric techniques to reveal a sharp rise in publication from, merely, seven articles in the year 2000 to 542 in 2011, with the majority of publications coming from universities. Bajwa and colleagues also found that a high amount (67%) of the papers had three or more authors.

In another study, Davarpanah (2012) focused on the historical productivity of nuclear science and technology research from 1990 to 2010. The analysis uncovered that the nuclear science and technology specialty underwent exponential growth over the twenty-year period via

citation analysis. Davarpanah additionally reported that the main source for the publication growth was academic institutions, 93% of the articles were found to be co-authored, and internationally co-authored articles far exceeded Iranian domestic co-authorship. Within a similar timeline (1990 to 2006), Osareh and McCain (2007) observed that chemistry research had also undergone exponential growth via author co-citation analysis. Interestingly, Osareh and McCain concluded that geographic and institutional influences were seen as the foundation of research, perhaps, as the authors suggested, stemming from institutional affiliations and topic restrictions. While, Saghafi, Asadi, and Osareh (2013) studied engineering research and found, using a historiographical map covering research from 1939 to 2011, that scientific publication output was marked by fluctuations, despite an overall increase during the period.

Some longitudinal investigations of research specialties were performed with a particular focus on India (e.g., Walke and Dhawan) and other regions (e.g., Sagar et al. 2010). Such studies traced the productivity of research along geopolitical lines and produced large amounts of quantitative data to inform science policy making; however, these studies were noticeably lacking a much needed subjective dimension to validate and contextualize their conclusions. As argued in Garfield (1979), analyzing the historical evolution of the sciences is best served by validation through congruent findings with the use of highly quantitative data (e.g., citations), combined with highly qualitative data (e.g., first hand expert accounts). Since they are numerous and very similar, only a few examples of such studies will be discussed here. Walke and Dhawan (2007) investigated the evolution of materials science research from 1993 to 2001 via citation analysis. According to Walke and Dhawan, materials science grew approximately 7% annually with the majority of its thrust coming from research on composites and textiles, respectively. In another study, Diabetes research was analyzed from 1999 to 2008 using citation analysis (Gupta,

Kaur, and Bala 2011). The authors observed that publication output increased from 1534 articles in 1999-2003 to 3290 in 2004-2008 indicating a growth rate of 114.47% and an average annual growth rate of 13.71%. From another perspective, Bala and Gupta (2010) analyzed the evolution of collaboration in Indian research on biochemistry, genetics, and molecular biology from 1998 to 2007. Bala and Gupta found that international research collaboration grew from 16.81% between 1998 and 2000 to 18.38% between 2005 and 2007.

Dastidar and Ramachandran (2008) studied Antarctic science research over a 25-year period via network and citation analysis. Global research interest in Antarctic science had steadily increased between 1980 and 2004 as illustrated by the rising output of Antarctic science articles in journals and the tripling of subject specialty research (Dastidar and Ramachandran 2008). Li et al. (2009, 56), focusing on global stem cell research trends from 1991 to 2006, discovered that stem cell research grew annually from 1996 to 2004, and the central research focuses were “hematology, oncology, and cell biology fields”. In the last example, Tsay and Lin (2009) analyzed transport phenomenon research with regard to Bradford, Zipf, and Lotka’s Laws from 1900 to 2007, and observed that transport phenomenon research grew exponentially at a rate of approximately 8.67% annually. Tsay and Lin’s analysis further described transport phenomenon research as following the standard S-shape with regard to a Bradford-Zipf plot, and Lotka’s law was confirmed with 60% of authors found contributing only one paper. Superconductivity research in Israel underwent analysis in Arunachalam and Singh (1985). The authors showed that from 1971 to 1982 many of Israel's articles were published in high impact journals. According to Arunachalam and Singh, from 1972 to 1977 each article in their dataset had been cited at least six times. Furthermore, 67 studies published between 1968 and 1977 were observed up to 1982 being cited 480 times, averaging 7.1 citations per article. Park and

Leydesdorff (2008) studied the evolution of science and technology research output from South Korea from 1993 to 2006 using social network analysis with journal-to-journal citation data and found a clear linear upward trajectory in publication output. However, the researchers concluded that Korean journals were sparsely being used as a scientific communication channel with national and international scientists.

Moving away from smaller units, research on changes in science, as a whole, has also taken place. Porter and Rafols (2009) investigated the level of interdisciplinarity of science from 1975 to 2005, focusing specifically on six major research domains. The authors found that there has been marked fluctuations in the 30-year study period, most notably a rise in citations and references for disciplines per paper (50% increase) and co-authorship per paper (75% increase). Yet, interdisciplinarity, according to their index, only rose slightly (5%). Boyack, Klavans, and Borner (2005) performed a similar study, but they took a static view, not a longitudinal one. Boyack, Borner, and Klavans (2009) tracing the evolution of chemistry found that large trends can be viewed with journal level data, but journal data cannot provide information about interaction between disciplines. However, this limit was overcome by Neff and Corley (2009) in their analysis of ecology using co-word analysis on a large scale.

Hu et al. (2010) studied the evolution of the drinking water specialty from 1991 and 2007 combining historical review and bibliometrics. The historical review method called for the researchers to contextualize the bibliometric data by analyzing "the time(s), place(s), and context(s) in which events occur and develop" (Hu et al. 2010, 1739). With their use of citation analysis, they focused on a one-dimensional aspect of specialty structure illustrating that there was a spike in publication output during two specific periods of time (i.e., 1992-1997 and 2004-2007) and "Cadmium" stood out as the most frequently used keyword in the entire 17-year

period. On the other hand, Cobo et al. (2011) researched the thematic evolution of the fuzzy sets theory specialty via co-word analysis finding that intuitionistic-fuzzy-sets and fuzzy-rough-sets (i.e., two research themes) are the origin of the specialty's new research thematic areas.

In summary, the aforementioned scientometric/bibliometric researchers have studied the evolution of scientific specialties by viewing them as scholarly communication systems and plotting the dynamics of their citation behavior over time. It should be noted that other methodologies (e.g., historical) have also, at times, been adopted for examining the evolution of a scholarly specialty or field. Price (1969) found that growth patterns (i.e., output) of scientific publications correlated to the advancement and theoretical development of specialties. Normal scientific specialty evolution, as Tabah (1999) described, has been marked by consistent accumulation of scientific knowledge and a constant population of researchers contributing to a specialty. The temporal view of normal science would present itself along an equilibrium time path. Kuhn (1962), on the other hand, pointed to paradigm shifts, defined as drastic interruptions of normal science caused by new scientific discoveries that challenge the current way of thinking. Kuhn's revolution of scientific ideas is illustrated by rising activity and a dividing of the scientific community into different schools of thought on theory and explanations. The dynamic time paths of various specialties were illustrated in many ways (e.g., equilibrium, exponential growth, S-shaped growth).

3.3 Research on the Contributing Domains of a Specialty/Discipline

Research on the intellectual structure of specialties has aimed to observe and represent the network and relationship among authors that contribute to a specialty (Griffith, Small, Stonehill, and Dey 1974; Small and Griffith 1974). Scientific specialties are often impacted by what Morris (2005, 1252) termed, "loan knowledge". Loan knowledge is research information,

either in the form of books or articles that are created in one specialty and makes its way into another specialty. Specialties, according to Kuhn's (1962) model of scientific development, are often in prolonged periods of stasis and only rarely experience drastic shifts. Loan knowledge could precipitate such rare and drastic paradigm shifts by introducing knowledge from one research specialty, (either through empirical findings, logical leaps, or improved methods and techniques,) to a different specialty, possibly challenging and superseding the foundational knowledge of the receiving specialty. However, the process may be much more gradual and loan knowledge could simply be used to support existing conditions. In addition, new specialties can be formed by the sharing of knowledge between multiple domains as in, for example, biochemistry, where well established research domains (e.g., biology and chemistry) sprout branches that intersect the two domains giving birth to a new specialty. Boyack, Klavans, and Borner (2005) used journal-to-journal co-citation analysis to map science, as a whole, and found that biochemistry appeared to be the most interdisciplinary field in science.

It has been shown in some studies that interdisciplinarity is best investigated using journals to represent fields of study and tracking citations between them (Bjurstrom and Polk 2011; Leydesdorff and Goldstone 2012; Liu 2005; Liu and Wang 2005; McCain 2010). Nevertheless, other studies have been successful to gain a more detailed view by using other techniques such as author co-citation analysis (Zhao and Strotmann 2011), a combination of journal-to-journal analysis and expert interview (Schwechheimer and Winterhanger 2001), and classifying and analyzing publications using the Dewey Decimal Classification System (Hammarfelt 2011). In one such example, McCain (1995) used co-classification analysis to study biotechnology research and development. Co-classification, according to McCain, relies on the interpretation of subject analysts performing the indexing and can be negatively impacted by the

indexer effect (i.e., the subjective bias of the indexer). However, fields with widespread rigid vocabularies and developed concepts, such as pharmacy research (Spasser 1997), have shown the technique to produce reliable results.

Combining full text analysis and traditional bibliometric techniques, Glenission et al. (2005) found that the literature of bibliometrics, as reflected in the journal *Scientometrics* during the year 2003, had broad and heterogeneous coverage. In another example, Erfanmanesh, Rohani, and Abrizah (2012), using social network analysis and co-authorship techniques, illustrated that the field of scientometrics lacked a few central authors by which the field revolved around. Rather, a large number of popular authors were uncovered. Additionally, the United States was rated the highest on all measures, except for centrality, in scientometrics and information and library science was seen as the most active participating discipline.

Setting their sights on a field different from scientometrics, White and McCain (1998) performed a domain analysis on information science. They argued and showed evidence that information science was composed of two main specialties: bibliometrics and information retrieval. Other researchers, such as Harter (1992) and Wilson (1996), criticized the assertion White and McCain (1998) made. Consequently, White and McCain participated in the debate by using the largest dataset to date (i.e., from 1972 to 1995), and indicated that the two largest specialties in information science were experimental retrieval and citation analysis, followed by practical retrieval and bibliometrics, respectively. Related studies (Janssens, Glanzel, and Moor 2007; Persson 1994) have also revealed larger information science clusters forming into information retrieval and bibliometrics/scientometrics. In his study, Persson (1994) raised some issues with this line of research. For instance, the *Journal of the American Society for*

Information Science (JASIS) was found to have had multiple spelling variants of cited author initials and abbreviations of the same cited journal.

Shalini and Janaki (1985) used citation analysis to study the composition of the information science field in the early 1980s. The researchers found that the computer science domain was the greatest contributor, followed by information retrieval, and psychology. The authors were surprised by these findings that suggested that information science received much borrowed knowledge from ancillary domains and could be considered multidisciplinary in nature. According to Shalini and Janaki, this had an impact on the way in which information science should set up its educational programs. Focusing on a specialty within the information science field, Jamali (2013) used citation analysis to track theoretical contributions to human-information behavior (HIB). He found that the library and information science (LIS) dominated in contributing theories to the HIB specialty, In addition, Jamali also observed 29 other disciplines contributing to HIB to a lesser extent, for example, sociology, communications, psychology, and computer science, making HIB an interdisciplinary specialty. Information science and information systems appear to be highly overlapping fields, yet Ellis, Allen, and Wilson (1999) produced contrary results in their co-citation analysis. On the surface it seems that many aspects of information science are also present in information systems, for instance, overlap seems to occur in areas such as information retrieval. Yet, citation analysis showed that research recognition between the two fields does not overlap. Ellis, Allen, and Wilson found that the disparity was due to information science research (such as information retrieval) centering predominantly on information content and texts within systems, whereas information systems was aimed at formal modeling, data relationships, and organizational context.

In another study on information science, Zhao and Strotmann (2008) experimented with adjusting their author co-citation analysis threshold to include all authors, as opposed to only including authors with a minimum citation count of 5 or 10. They found that the intellectual structure of the field did not differ when reducing the threshold. Likewise, Persson (2010) used shared references and co-citations, combined with similarity measures for weighing the strength of direct citations in order to decompose publications by specialty in the LIS field. Persson reported that using direct citations produced a more precise view of specialties within LIS. Moreover, Persson suggested that using the strongest links in every paper would produce the greatest outcome.

Moving towards mapping and visualizing intellectual structures, Janssens et al. (2006) found that the best solution for clustering the LIS field was to use full text data and a combination of mapping techniques. Zhao (2009) tested the impact of field delineation via author co-citation analysis on the intellectual structure map of specialties and discovered that views of the general structure remained unchanged. However, at greater levels of granularity, differences appeared indicating that researchers seeking to address subtle research policy problems ought to pay particular attention to the way in which they delineate their specialties. Kim and Lee (2009) used another method, namely, profiling analysis to examine archiving research trends in LIS. The researchers concluded that the most prominent subject was digital libraries along with electronic media as the most prominent object.

Moya-Anegon, Jimenez-Contreras, and Moneda-Corrochano (1998) performed author co-citation analysis to map the intellectual structure of the LIS field in Spain between 1985 and 1994 with the help of cluster analysis, multidimensional scaling, and principal components analysis techniques. Some researchers (e.g., Kreuzman 2001) have argued that multidimensional

scaling is more appropriate for representing a global view, as opposed to a local one. Nevertheless, Moya-Anegon and colleagues were able to categorize particular research activities into three distinct types of research areas: informetrics, librarianship, and research approaches by university affiliation. Informetrics and librarianship derived from groups of authors connected through their participation in research revolving around these two research specialties. The third type of groupings were produced based on university affiliation, and they were composed of university researchers connected by their theoretical approaches to research and emphasis on professional training, or geographical area. Moya-Anegon, Jimenez-Contreras, and Moneda-Corrochano found a problem with a number of databases they used and recommended that when choosing a database to select author co-citation analysis data, try to use one that includes all authors of an article because some databases only use the first author and abbreviate the rest using '*et al'*. Additionally, other researchers (Bayer, Smart, and McLaughlin 1990; Tsay, Xu, and Wu 2003) using co-citation analysis have argued the necessity of using multiple complementary methods such as, consensus building techniques (e.g., the Delphi method) to offset the aforementioned limitations.

A number of studies investigated the intellectual structure of LIS in China. Ma et al. (2009) did a co-citation analysis of information science via the Chinese Google Scholar. The authors found that, although it is a powerful tool, the retrieved results were "mixed with much fuzzy data unavoidably". Using co-authorship network analysis, Yan, Ding, and Zhu (2010) concluded that Chinese library and information science's author collaboration network, represented by 18 core journals over a six-year period, was a small-world network; this means that shortcuts between authors were prevalent and far less ties were necessary for authors to collaborate. The small-world phenomena illustrates that social networks are not linear and in

some networks two distant points can be connected by transversing the network via a median count of five intermediaries (Milgram 1967). Yan, Ding, and Zhu (2010) argued that the small-world network facilitated faster and more precise information flow creating an environment more conducive for future collaboration. In a study by Hu et al. (2013), the researchers presented three substantial finds via co-word analysis in Chinese LIS: established research topics, emerging areas with good growth potential, and the variety of research topics.

Yerkey and Glogowski (1989, 90) analyzed the scatter of LIS literature and found that the most prominent subject categories outside the field came from "medicine/health sciences, business, education, and computer science". Levitt and Thelwall (2009, 57) uncovered that out of all the highly cited articles in LIS, the highest citation ratings came from those articles within LIS that included contributions from another field. Moya-Anegon, Herrero-Solana, and Jimenez-Contreras (2006) used author co-citation analysis and journal co-citation analysis, while Astrom (2010) used those methods as well, but he also experimented with a combination of self-organizing maps and multidimensional scaling. Both studies were able to confirm that each are distinct, yet closely related fields and LIS can be seen as a third distinct field that had sprouted from its two preceding cores. Holmes (2002), with his longitudinal citation analysis on contributing fields to information science, found that its principal contributors (e.g., library science, computer science, and economics) and secondary ones (e.g., engineering, sociology, and psychology) fluctuated over time.

Historical records, according to Lariviere, Sugimoto, and Cronin (2012), show that in the past, LIS had little influence on the social sciences and humanities. Using bibliometrics, Lariviere, Sugimoto, and Cronin found that LIS reemerged as a force in other fields through its use of authorship collaboration. The researchers found that 60% of the scientists who published

in the LIS field also published in other disciplines. This shift, according to Lariviere, Sugimoto, and Cronin, spurred an increase in other fields that contributed to LIS, most notably, the computer science field in the 1990s. Knowledge management, a specialty closely related to information science, was also found by Ponzi (2002a) to have high concentrations of contributing literature from "computer science (30.8%), business (23.7%), LIS (13.5%), and management science (13.1%)".

The close relationship between information systems and its related college of business disciplines also underwent a bibliometric analysis by Pratt, Hauser, and Sugimoto (2012). The researchers constructed the following list of disciplines to use in their analysis: accounting, entrepreneurship, finance, information systems, management, and marketing. A total of 148, 009 papers were analyzed between 1969 and 2008. Papers per discipline were found to differ to a great degree. The analysis indicated that there was an increase in the exportation of information systems literature to other college of business disciplines. In particular, the greatest increase was to marketing and entrepreneurship. The evidence showed, according to Pratt, Hauser, and Sugimoto, that information system is becoming a reference discipline. Visual analysis of the data set indicated the underlying relationships between groups of journals. Information systems, as a discipline, was seen to share a common group of journals with all other disciplines, except for finance, attesting to an overlap in research interests. In a similar manner, Park and Leydesdorff (2009) were able to use journal-to-journal citations in establishing that social and experimental psychology were the primary contributing disciplines for the communications field. Kim (2012) took a different view using author co-citation analysis and arrived at a more granular level of the field finding that the communication field was composed of numerous subfields (e.g., mass communications, organizational communications, and interpersonal communications). In another

study on communication, Lin and Kaid (2000) observed that the political communications specialty's diverse academic background resulted in a fractured structure leading to limited information exchange.

In another scientometric study on information systems, Cabanac (2012) shifted the focus towards the demographics of information systems journal editorial boards. The researcher intended to represent the landscape of research in information systems and uncover the characteristics underlying its leading journals. The researcher specifically placed an emphasis on the overlap between information systems and computer science since, as Cabanac (2012, 978) notes, "few scientometrics studies have addressed computer science". In a similar study, Eom (1996) used author co-citation analysis to investigate decision support systems research. One dilemma Eom came across in his methodology was that no systematic and objective ways could be found to establish a list of candidate authors for co-citation analysis mainly because Eom had a particularly large number of potential authors. Otherwise, the author co-citation analysis procedure is well established. Even with large numbers of authors, the researcher can always raise the threshold for including particular authors for co-citation computation. Eom decided to use the number of co-citations of an author with him/herself as the selecting factor. Using factor analysis, Eom (1996, 319) uncovered a number of external influences for the field: "multicriteria decision making, cognitive science, organizational science, artificial intelligence, and systems science". The field's internal construction, represented by its literature, was found to be composed of "group decision support systems, foundations, model management, interface systems, multicriteria decision support systems, and implementation" (Eom 1996, 319).

Acedo and Casillas (2005) mapped the intellectual structure of international management and then claimed that this specialty is heterogeneous and with multidisciplinary research

approaches. Furthermore, Acedo and Casillas (2005, 632) argued that this structure of international management might be a "weakness" as it could cause fragmentation and potentially challenge its future development. As the authors suggested, this stems from a lack of a central body or collection of research works that could serve as the backbone of the field. On the other hand, some researchers state that fragmentation in the development of an interdisciplinary field "indicates the field's growth and is a common phenomenon" (Lin and Kaid 2000, 159). The international management field, according to Acedo and Casillas (2005, 632), shares research approaches with such fields as "economics, strategic management, and organizational theories".

From management research perspectives, Kumar and Mohad (2013) that collaboration was positively correlated with research performance in the field of business and management in Malaysia, and geographical proximity was a major factor with intra-national collaborations. Interestingly, Malaysian institutions tend to collaborate internationally with foreign partners more often than with institutions within its own borders; the same was echoed by Abrizah and Wee (2011) with regard to Malaysian computer science research. Supply chain management, as reported by Charvet, Cooper, and Gardner (2008), is composed of many different avenues of research (e.g., operations research, logistics, interorganizational relationship, and strategic alliance) that appear fairly independent of each other. Furthermore, Charvet, Cooper, and Gardner indicated that there was a high degree of interest by other disciplines and journals ancillary to the field, ranging from business and economics to operations research. Chen and Lien (2011) studied the intellectual structure of e-learning from a perspective of management information systems, finding that behavior and cognitive psychology played a dominant role in this specialty. In addition, Chen and Lien showed that Taiwanese researchers focused on information technology in e-learning. Using social network analysis techniques, Khan, Moon,

and Park (2011) developed a novel approach to mapping and visualizing the core of science domains, particularly management information systems (MIS). Khan, Moon, and Park (2011, 763) identified e-government and information technology outsourcing as core science domains in MIS, illustrating the utility of their methodological approach.

In early research on macroeconomics, White (1983) found that co-citation analysis could identify a wide variety of associations (e.g., institutional, geographical, language) beyond merely scientific schools of thought. White (1983, 285) was also able to validate the use of co-citation authors as "concept symbols"; that is, as standing for more than simply their substantive contributions but for what the authors have come to represent. Dolfsma and Leydesdorff (2010) reported on the interdisciplinarity of evolutionary economics by tracing contributions to the field from the core journals of other disciplines. Locke and Perera (2001), in their co-citation analysis on the intellectual structure of the accounting field, uncovered evidence indicating that the field is fragmented. More research, as the authors argued, is necessary to integrate accounting's diverse four research topics. Consistent with the findings of Ramos-Rodriguez and Ruiz-Navarro (2004) and Fernandez-Alles and Ramos-Rodriguez (2009), Locke and Perera found that books were the dominant form of publication in accounting, a phenomenon that appears to be part of the broader business and management disciplines.

Hoffman and Holbrook (1993) developed a novel approach to analyze the intellectual structure of consumer research over a 15-year period. In particular, they used a two-stage procedure incorporating the from-vs.-to (i.e., citing-cited) matrix producing a scale of from-vs.-to asymmetry and a subsequent citation-similarity space to uncover citation patterns and atypicality. The intellectual structure of consumer research, as Hoffman and Holbrook (1993, 514) reported, had been seen developing along two primary dimensions. The first dimension

correlated to the selection of focus for research, i.e., “more macro or social to the more micro or individual level of analysis”. The second dimension represented a splitting between researchers who preferred laboratory studies and experimental designs versus those who focused on model production, measurement, and mapping. Hoffman and Holbrook chose to only use the *Journal of Consumer Research* for analysis over a 15-year period. Considering the study covered such a long period, perhaps an analysis of the changes occurred during that time span would have been beneficial.

Some studies focused on the intellectual structure of Korean research. For example, Yoo, Lee, and Choi (2012) analyzed Presbyterian theology over an eight-year period and found that the field was composed of such major clusters as Reformed theology, general theology, and Evangelicalism. In addition, the authors identified nine key research areas among the clusters. Park and Leydesdorff (2008) investigated Korean science and technology research from a social network perspective using the *Science Citation Index*. The authors found that Korean journals did not act like research channels or data sources for Korean scientists, but more like publication outlets. The journals were found to link Korean scientists to international scientists, yet not link Korean scientists together.

Beyhan and Cetindamar (2011) used bibliometrics and social network analysis to investigate whether the intellectual base of technology management literature from developing countries differed from that of developed countries. The analyses produced three particular findings. First, the literature of technology management created by developing countries is heavily influenced by publications of developed countries. Second, scholars from developing countries are often prolific and develop prominent works. However, these authors were left out of previous bibliometric studies on technology management. Finally, researchers from

developing countries tend to focus on issues pertinent to their own context rather than to the context of the entire field. Likewise, Dastidar (2004) observed that socio-economics and political stability of a country had a marked impact on its research production enterprise in studying ocean science and technology research across countries.

McCain et al. 2005, in another similar study, researched the intellectual structure of software engineering using a combination of methods: author co-citation analysis and knowledge elicitation. The use of the two research methods, according to McCain et al. 2005, provided cross validation. The results indicated that software engineering's central figures were Boehm, Basili, Booch, and Hoare. Furthermore, the study uncovered the following specialties emanating from within software engineering: object oriented programming, analysis and design, formal methods, software process management, and software metrics.

Nanoscience has proved to be a good scientometric/bibliometric case study being found in some studies to have a high degree of contributing research domains. In one such study, Leydesdorff and Rafols (2009) extracted domain contributions to establish factors for analysis using ISI subject categories, which are developed in its citation indexes, to delineate domain journals. The authors found that the ISI's subject categories work well for classification. However, they do not function well with high granulation views using aggregated journal-to-journal citations. Aggregating journal-to-journal citations, as Leydesdorff and Rafols reported, poses difficulties when mapping higher levels entities (e.g., specialties). Chen and Guan (2011) argued that nanotechnology, biotechnology, and pharmaceuticals all contributed to establishing the runoff specialty, nanopharmaceuticals. Larsen (2007) studied nanostructured solar cell research combining a qualitative case study approach, bibliometrics, and social network analysis. The study revealed that there were contributions to the specialty from several disciplines

including “chemistry, physics, electrochemistry, nanotechnology, and material science” (Larsen 2007, 133).

Likewise, Bajwa, Yaldram, and Rafique (2013) observed that in Pakistan, nanoscience was receiving input from materials science (35%), chemistry (20%), and physics (10%), to name a few. In a contrasting view, Schummer (2004) found that nanoscience research, according to co-author analysis results, exhibited no discernible pattern of interdisciplinarity. Moreover, Schummer indicated that nanoscience’s multidisciplinarity (e.g., nanophysics, nanochemistry, nanoelectrical engineering) is composed of various mono-disciplinary fields that are not related to one another but for their focus on the “nano” scale. Differing from what Schummer reported, Bassecoulard, Lelu, and Zitt (2007) showed that moderate multidisciplinarity existed at the aggregate level; however, this was seen to somewhat come from an interdisciplinary nature when viewing the data from the article level. While, Milojevic (2009) had uncovered that nanoscience exhibited properties of a transdisciplinary field.

Using author co-citation analysis combined with a variety of information visualization techniques, Reid and Chen (2007, 43) were able to shed light on the terrorism research domain which, according to the authors, “is not a topic that is easily researchable because of the clandestine nature of terrorist groups”. Several subfields were found emanating from the domain. Each subfield seemed to represent the diverse influences of contributing social science disciplines such as political science, international studies, and history. Reid and Chen were able to uncover quantitatively that research behavior prior to the terrorist attacks on September 11 showed a marked lack of interest in the specialty.

In summary, Morris and Martens (2008) suggested that the intellectual structure of specialties exhibit important characteristics that are often the focus of investigation. Studies on

the intellectual structure of specialties have sought to reveal the size of specialties, overlap and scatter that serves to differentiate specialties from one another, homogeneity within specialties, and areas or components within a specialty. Moreover, scientific specialties have been shown to be highly composite open scholarly communication systems that fluctuate with scientists and knowledge often being exchanged via citation behavior. Studying the contributions from one scientific entity (i.e., specialty, discipline, and field) to another is a salient topic for researchers, since, as Chubin (1976, 465) notes, "the redistribution of scientists through migration has been shown to alter the course of disciplines", and he goes on to suggest that "the transition of scientists from one specialty to another harbors massive potential for intellectual change".

3.4 Scientometric/Bibliometric Studies on Information Security

Some studies investigated the intellectual structure of either INFOSEC or closely related specialties (e.g., cryptography, role-based access control) using bibliometric data. However, few of those studies used traditional scientometric/ bibliometric techniques (e.g., co-citation analysis) but instead employed content analysis to determine the subject composition of literary artifacts (e.g., journals, articles).

Dlamini, Eloff, and Eloff (2009) examined the past, present, and future research themes of the INFOSEC field by distributing surveys to experts in the field, in conjunction with using content analysis on INFOSEC research publications. Dlamini, Eloff, and Eloff (2009, 9) concluded, "as we entered the twenty-first century, the scope of information security has widened, and its focus is fast shifting towards a strategic governance one". For example, their journal analysis results indicated that there were three dominating INFOSEC research themes that focused of strategic governance: legal and regulatory compliance, risk management, and information security management (Dlamini, Eloff, and Eloff 2009). The authors argued that

INFOSEC research is undergoing a significant change from dealing with threats via “reactive technical measures” to now trying a more “proactive strategic approach” (Dlamini, Eloff, and Eloff 2009, 7).

Similarly, Botha and Gaadingwe (2006) used content analysis to investigate significant research trends in a set of 20 conference proceedings of the International Information Security Conference (SEC) between 1983 and 2005. Botha and Gaadingwe observed that INFOSEC research mainly centered on the following topics: business continuity, management related, network related, crypto-like topics, and auditing. These research topics overlap with those found by Dlamini, Eloff, and Eloff on strategic governance research. Moreover, Botha and Gaadingwe showed that there was a significant trend between 1998 and 2005 in which technical outputs accounted for 70% of the papers, while both formal and informal accounted for only 30%. The authors concluded that there was a real lack of research aiming at informal and formal topics; they specifically point out a need for research on user awareness, auditing, and business continuity.

Siponen and Oinas-Kukkonen (2007), in another study that used content analysis, argued that there was a lack of research on contributions made to INFOSEC research by other research domains. The authors used a wide-ranging review of INFOSEC literature to investigate “how and to what extent information security issues have been covered by previous research and what research approaches and reference disciplines have been used by prior research" (Siponen and Oinas-Kukkonen 2007, 61). The authors used a highly qualitative approach as there was no formal content analysis procedures included. Rather, an analytical framework was developed, based on prior research, which allowed them to review and interpret INFOSEC issues, approaches, and reference disciplines (Siponen and Oinas-Kukkonen 2007). It was unclear as to

the date range that the authors used in obtaining their INFOSEC literature, but it was stated that they examined INFOSEC journals leading up to the beginning of the year 2000. Siponen and Oinas-Kukkonen did not include any explanation of how the INFOSEC journals and articles were selected, and there was no details relating to the factors and procedures involved in extracting data from the articles. The study's highly qualitative nature limited its reliability; however, its results and conclusions may be useful in comparison with other studies. In line with Botha and Gaadingwe (2006), Siponen and Oinas-Kukkonen reported that most INFOSEC research has focused on technical issues, issues of access to information systems, and secure communications. Additionally, it was observed that the main research approach used in dealing with INFOSEC issues was applied mathematics, and the dominating reference discipline was mathematics and philosophical logic (Siponen and Oinas-Kukkonen 2007).

Fushs, Pernul, and Sandhu (2011) studied role-based access control publications, a topic closely associated with INFOSEC, using survey, classification, and statistical analysis techniques. The Digital Bibliography and Library Project (DBLP) was chosen as the primary source for data based on three reasons: it was not found to be limited to particular publishers, delineating criteria was included when it returned many identified publications, and the DBLP contained most of the information technology journals and proceedings. In addition, Fushs, Pernul, and Sandhu used IEEE and ACM Digital Libraries in a second data retrieval stage in order to offset any publications missing from the DBLP. The authors identified 1361 publications on role-based access control from 1996 to 2010 and a few publications were also retrieved and included from 1992 to 1995. According to the researchers, artificial intelligence, social psychology, organizational management, and human-computer interaction contributed to role-based access control research. Fushs, Pernul, and Sandhu analyzed, via descriptive statistics,

the frequency of role-based access control articles in journals and the growth of its various subtopics. The authors observed a number of results: literature on role-based access control steadily rose, yet at times could also be seen slightly plateauing; approximately half of the publications addressed theoretical problems, while the other half dealt with applied problems; the majority of applied research was seen dealing with the adoption of roles in different security technologies, and the theoretical research was found being dominated by the framework of role models and the design of role based systems; and theoretical and applied research seemed to have risen in tandem (Fushs, Pernul, and Sandhu 2011).

Cryptography is another major topic that overlaps with INFOSEC. Baskaran (2013) investigated year-wise cryptography research outputs, relative growth rate, doubling time of publications, international publication distributions, and subject-wise distribution of research output for studies published from 2000 to 2011. Baskaran extracted data from the Science Citation Index (SCI) using the term, "Cryptography" and focusing on titles, abstracts, and keywords. Overall cryptography research productivity (number of papers, pages per article, cited references, numbers of authors per paper, and average number of article per journal), as Baskaran reported, were all found to have increased. In particular, Baskaran found that the mean relative growth rate for the first six years was 0.178 and for the following six years it was 0.103, while the doubling time was 11.658 (first six years) and 20.746 (last six years). Contributions to cryptography research from other disciplines, as Baskaran (2013, 418) observed, are as follows: 3468 (52.48%) computer science, physics 2361 (35.71%), engineering 1421 (21.49%), and optics 904 (13.67%).

Lee (2008), via co-word analysis, examined new and emerging technology research trends in INFOSEC research using a scientometric/bibliometric methodology. The author argued

that research trends could be used to ascertain potential future technology developments. Lee was able to confirm that information security literature has a moderate amount of established research themes and is dynamic enough to quickly adapt to new themes. However, Lee presented no indication that the information security literature foreshadowed technology development. The data for Lee's study was collected from the Science Citation Index-CD version between 1994 and 2003. Furthermore, Lee applied network analysis, clustering, and multidimensional scaling to keywords extracted from titles, abstracts and, in some cases, entire documents. The analysis produced thirteen clusters: Security Assessment, Detection, Monitoring, Systems, optical security, Encryption, Verification, Cryptography, Computation, Cryptosystem, model, Authentication, and Privacy. INFOSEC research areas, as Lee (2008, 524) uncovered, were categorized into "security assessment, computation, and cryptosystems", and cryptosystems, as Lee suggested, had a high possibility of becoming the most popular subject in the near future.

It seems thoroughly evident that there are few studies that use bibliometric data to map the intellectual structure of the INFOSEC specialty. With the exception of Lee (2008), who mainly focused on emerging future INFOSEC technology trends, studies using a scientometric/bibliometric approach to map out the intellectual structure of INFOSEC seem to be even fewer.

3.5 Concluding Remarks

A review of the literature shows the different perspectives by which specialties have been investigated by researchers. Most of the reviewed studies can generally be seen falling into one of four categories: analytical, structural, holistic, or dynamic. The analytical studies (e.g., Sagar et al. 2010) had a one-dimensional view focusing on the information exuded by individual units (e.g., authors, articles, and journals). These studies put forth an analytical view of a specialty by

investigating output, productivity, and composition via citation and word analysis techniques combined with descriptive statistical measures. The analytical perspective was a prerequisite for studies on the emergence, intellectual structure, contributing domains, and evolution of specialties, since they all required an aggregated view of the aforementioned individual units of analysis. On its own, analytical views have been used to evaluate many such individual units (e.g., researchers and the h-index) (Egghe 2010). Secondly, other studies (e.g., White and Griffith 1981) took their primary aim at the intellectual structure of a given specialty. Studies of this type were centrally concerned about the relationships among the individual units from a multidimensional view. The main techniques most often used in structurally focused studies were co-occurrence (i.e., co-citation, co-word, co-authorship) and network analysis. Thirdly, more comprehensive studies (e.g., Besselaar and Leydesdorff 1996) took a holistic view of the specialty; taking it as a single collective unit and plotting its relation to contributing domains. Specialty research from the holistic perspective usually involved intra-journal citation analysis or a combination of co-occurrence approaches. Fourthly, dynamics was seen as a variable common in those reviewed studies (e.g., Pilkington and Meredith 2009); they mainly analyzed the evolution of specialties. Furthermore, such studies traced specialty behavior along temporal lines to discern history, development, and trajectory for future directions.

In addition, the above review also indicated that few studies combined multiple techniques and units of analysis in studying specialties. However, combining such complementary views is not just valuable but necessary in establishing valid conclusions. Traditional bibliometric measures are highly quantitative and have a distinct set of benefits and drawbacks. Likewise, other methods (e.g., content analysis) present their own set of unique advantages and disadvantages. The information security specialty was found to be mostly absent

from scientometric and bibliometric studies. Yet, with the growth of information technology over the last decade, information security research is an area of vital concern. Therefore, the present study fills this knowledge gap by investigating the information security specialty using a combination of methodologies to uncover the analytical, structural, holistic, and dynamic dimensions of the information security specialty.

4. Objectives and Scope

4.1 Objectives and Research Questions

The primary aim of this study was to explore and describe information security as a research specialization. This aim was met with the objective to utilize bibliometric data extracted from a database (i.e., Scopus) in order to create an intellectual profile and underlying structure of the information security specialty. A specialty profile and visualization of information security was used to shed light on the following research questions:

1. What are the salient features of information security as a specialty?
2. How has the information security specialty emerged and evolved from the temporal perspective?
3. What scholarly domains contribute to information security in light of the sources used by researchers from the specialty?
4. What is the intellectual structure underlying the specialty of information security?

The scholarly domain responsible for research, according to Chubin (1976, 448), is the specialty, and it could be found "nestled within and between disciplines". As Small and Griffith (1973, 17) explained, science is not a social or intellectual uniformed whole; it is a "mosaic of specialties". Morris and Martens (2008) posit that the specialty, considering its homogeneity, is the most appropriate level of analysis when studying science as a system that will produce a valid and coherent local view. Specialties tend to develop considering "growth in authorship and literature, cognitive development, and the development of organizational infrastructures" (Tabah 1999, 274). Research Question 1 (RQ1) addressed the research problem outlined in this study in a number of ways. In general, providing a profile of a specialty, as Chen et al. (2002) and Porter

et al. (1991) have argued, can be used to advise government policy makers and business leaders in their management of research agendas and strategies.

Specifically, for instance, a view of the most prolific authors can assist scientists in their search for expert collaborators. Information retrieval can be made more efficient for researchers and educators by presenting information security's core articles and journals in a user-friendly interface (De Bellis 2009; Garfield 1955; Lunin and White 1990; Small 1973). An understanding of the most productive institutions can provide data for the management of government and private research funding programs (Ismail et al. 2009), and also be used by universities to attract high performing faculty (Abrizah and Wee 2011). Moreover, knowledge of research output at the international level can inform national security R&D perspectives (Leydesdorff 2004).

Research Question 2 (RQ2) brought another scientometric perspective commonly used by information scientists (e.g., Georgi, Darkow, and Kotzab 2010; Neff and Corely 2009; Saghafi, Asadi, and Osareh 2013) to bear on the research problem presented in this study, expressly evolution of a specialty. Statements by the following researchers explain the way in which investigating the emergence and evolution of information security as a specialty over time directly deals with the research problem underpinning the present study. Botha and Gaadingwe (2006, 2) suggested, "The future of information security can be realized only if its past and current positions are well understood". Likewise, Siponen and Oinas-Kukkonen (2007, 61) posit that such research endeavors are "needed in order to see the 'big picture', to make sense of the field, to see what previous research work has emphasized and identify those areas where the need for future work is greatest". A longitudinal view of the information security specialty allows researchers to backtrack from current research to its origin and consider, as Leydesdorff (2004) recommends, its lineage as only one of many possible paths that could have been taken. RQ2

established a temporal view of the information security specialty, aggregating the entire data set and analyzing the emergence and evolution of its patterns along temporal lines with a longitudinal perspective.

Research Question 3 (RQ3) brings to light the other scholarly domains that lent the information security specialty their theories, methods, experimental findings, and validation standards. An understanding of the domains and the amount that they contributed to the information security specialty approached this study's research problem by helping to explain the orientation of the specialty in regards to its emphasis on technical (e.g., computer science, engineering), social (e.g., psychology, criminology), or policy (e.g., business, management, government studies) research. A list of the full range of scholarly domains participating in information security research provided a clear view of possible opportunities for scientific cross fertilization. Moreover, RQ3 brings information security research articles hidden in journals outside the information security mainstream back in view (Yerkey and Glogowski 1989). Knowledge of the intersections of information security research and other domains gives science managers an outlook of areas ripe to exploit for collaboration, thus, avoiding one of the major reported (e.g., Siponen and Oinas-Kukkonen 2007) problems in the specialty (i.e., scholarly isolation of information security research).

Visualizing the intellectual landscape of information security, as was accomplished with Research Question 4 (RQ4), addressed this study's research problem in many ways. Visualizations provide a description of information security's intellectual structure with limited human bias and relevance criteria, aiding managers in tracking and evaluating the relative position and strength of research fronts, individual scientists, research groups, and countries (Garfield 1979b). Researchers (e.g., Borner, Chen, and Boyack 2003; Kessler 1963a; 1963b;

Lunin and White 1990) have also suggested that a map can serve as an information retrieval aid for researchers and librarians when searching through a large collection of data in information security via user-friendly interfaces that maximize the human ability to visualize and understand the spatial organization of objects and concepts. In addition, Reid and Chen (2007) pointed out that domain mapping could provide a clear view of the challenges facing researchers. Mapping the information security specialty can inform the greater field of scientometrics/bibliometrics as it will contribute another piece of the science puzzle by establishing an empirical foundation for gauging the importance of established scholarly abstract concepts such as specialty, discipline, and paradigm (Price 1963; 1965).

4.2 Concepts, Variables, and Operational Definitions

This section provides explanations and operationally defines, where needed, concepts and variables involved in the present study. Morris and Martens (2008, 214-215) defined research specialty with particular reference to its social manifestation:

> A research specialty is a self-organized network of researchers who tend to study the same research topics, attend the same conferences, read and cite each other's research papers and publish in the same research journals. A research specialty produces, over time, a culminating corpus of knowledge, embodied in educational thesis, books, conference papers, and a permanent journal literature. Members of a research specialty also tend to share and use, to some degree, a framework of base knowledge, which includes knowledge of theories, experimental data, techniques, validation standards, exemplars, worrisome contradictions, and controversies.

A discipline, on the other hand, is the much larger scholarly domain responsible for the training and education of new scientists, and disciplines are commonly associated with academic departments (Chubin 1976). Another domain of science, the field, is also associated with academic departments, but it represents the microenvironment in which scholarly investigations take place (De May 1982). In the present study, information security is considered a specialty and not a discipline or field. Academic degrees are not conferred in information security. Rather,

a scholar may belong to a scholarly discipline (e.g., computer science, management information systems, engineering) and have information security as a research specialization. Moving forward, salient features in the present research refer to multiple analytic output characteristics of information security, including key authors, sources, affiliations, and countries as reflected in research literature of the specialty. The term "key" is meant to denote those particular characteristics (e.g., author, source) that have the greatest publication output.

In this study, the concepts "emergence" and "evolvement" are both considered in relation to time as a central variable. Two fundamental notions implicit within the emergence and evolution of a phenomenon is growth and change (Tabah 1999). Moreover, the growth and change of scholarly domains have been investigated by researchers (e.g., May 1966; Price 1965) in dynamic terms with time being a key variable. It is only through the lens of time that scientists can view scholarly domains tracking their movements from the past to the present and plotting future trajectory. The growth and change of science domains have been argued by some researchers (e.g., Kuhn 1970) to correspond to points along a cyclical growth pattern of normal science and revolution; while other researchers (e.g., Moravcsik and Murugesan 1979) have empirically substantiated such claims finding positive correlations between the growth patterns of science domains with that of citation patterns.

In the context of this study, domain is synonymous with all meso and macro size scholarly divisions such as the afore-discussed specialty, field, or discipline. Contributing domains will be defined according to their respective sources (e.g., journals, conference proceedings, books), as research (e.g., Besselaar and Leydesdorff 1996) has suggested that journal-to-journal citations are well-established operational indicators for intra-domain organization and interaction. The scholarly journal, as discussed by Garvey and Griffith (1967)

and Mikhailov, Chernyi, and Giliarevskii (1984), is a formal communication vehicle for transmitting information in the scholarly world in the form of published articles. Furthermore, Chu (1991) and Small and Griffith (1974) have argued that the journal is a central mode for scholarly communication and an important source of data for investigations into scientific specialties. Furthermore, Chu (1991, 28) argued that the scientific journal is "the most common medium for storing" scientific information. As of late, the use of scientific journals for formal communications has only grown with importance and volume since the widespread development of the Internet and digital publishing (van Raan 2001). The use of books will aim to support a view of contributions from the humanities (e.g., law, policy) which are less prone to publish in scholarly journals and conference proceedings for more applied sciences (e.g., computer science, engineering).

The present study defines the intellectual structure of information security as distinct sets of accumulated co-citations and co-words, and the relationships within and among such sets (Leydesdorff and Vaughan 2006). These sets are considered to correspond to different schools of thought and research topics within the information security specialty. Various schools of thought and research topics within the information security specialty, for example, information security policy, Internet privacy, malicious software, trusted systems, cryptology (Abrams, Jajodia, and Podell 1995) will be presented in clusters and maps. Clusters are groups of highly co-cited documents or co-words that can be distinguished as a distinct set due to some shared property or underlying meaning. A map of scholarly research is a spatial depiction of the linkages among scholarly elements (e.g., authors, documents, research topics, specialties, fields, disciplines) as reflected in some codified, quantifiable properties of scholarly publications within a given period that shows its research fronts and topics.

4.3 Scope

While every effort was made to present a comprehensive scientometric/bibliometric investigation on information security as a specialty, a boundary was established when dealing with closely related concepts to maximize the benefits of a local view while gathering sufficient data to establish the context and relationships of the information security specialty. Therefore, two techniques were used to set the criteria for the inclusion of data. Firstly, a limited number of terms, argued by researchers (e.g., Blyth and Kovacich 2006; Maconachy al., 2001; Solms and Niekerk 2013; Whitman and Mattord 2009) to carry similar meanings to that of information security were used to search for the bibliometric data. These terms are as follows: information assurance, cyber security, computer security, communication security, and network security. Secondly, all of the documents indexed by Scopus from the highest contributing sources specifically geared towards publishing information security articles were included to expand the pool of bibliometric data. The reasoning behind the inclusion of the information security publications is that it is clear that documents published by journals (e.g., IEEE Security and Privacy) with the specific purpose of producing information security articles are related to information security research. The present study was restricted to what the Elsevier's Scopus database covers. A more detailed description of Scopus is offered in the Methodology chapter. Furthermore, not all documents, citations, journals, and words were included but only those over a minimum threshold will be used for the study in regards to time constraints and to maximize a clear view of the specialty by reducing noise.

5. Methodology

5.1 Methodology Justification

Scientometrics was used as the methodology for the present dissertation. Scientometrics has had a long and successful history in addressing research questions concerning the intellectual profile, structure, and dynamics of scholarly specialties (e.g., Braun et al. 2001; Leydesdorff 2001; Morris and Martens 2008; Price 1961, 1963, 1965; Tabah 1999). Compared to other methodologies (e.g., historical research, Delphi studies) used in science policy research that typically center on highly subjective data (e.g., Ding, Chowdhury, and Foo 2001; Rip 1988), scientometrics provides an established framework to orchestrate the use of a wide range of robust techniques to collect and analyze quantitative, as well as qualitative data.

Methods of the type that proscribe gathering the personal views of a small number of experts in a scholarly domain as a means to describe the respective scholarly domain present highly biased views; moreover, such methods make it difficult to gather data from a substantially large and diverse sample of researchers. In contrast, Eom (2003, 13) suggested that bibliometric techniques provide "unobtrusive, precise, and objective characteristics" specifically designed to study aspects of scholarly domains such as profile, structure, and dynamics.

Traditionally, scientometric research has mainly focused on bibliometric data such as publication and citation data (Garfield 1979b; Price 1965). The present study continued with the scientometric tradition by collecting both publication and citation data on the information security specialty using the Scopus database and applying bibliometric analyses that include co-citation analysis. Scientometric studies employing bibliometric analyses such as co-citation analysis techniques have been used on many occasions to study scholarly specialty profiles (e.g., Bajwa, Yaldram, and Rafique 2013; Rorissa and Yuan 2012; Sanz-Casado et al. 2013), structures

(e.g., Small and Griffith 1974; White and Griffith 1981), and dynamics (e.g., White and McCain 1998). More recently, information science scholars (e.g., Otte and Rousseau 2002) have argued that network analysis provides an additional strategy for studying social structures by analyzing co-citation data. Network analysis has been used in bibliometric studies on a number of occasions (e.g., Park and Leydesdorff 2008; Zhu and Guan 2013).

Though leading to many successful studies, some researchers (e.g., Edge 1977; MacRoberts and MacRoberts 1986, 1989, 1996; Rice et al. 1989; Smith 1981) have argued on a number of occassions that the use of co-citation data alone can present validity problems due to the multitude and subtlety of motivations for citation (Chu 2005). Many researchers (e.g., De Bellis 2009; Braam, Moed, and van Raan 1991; Moed 2005; van Raan and Tijssen 1993) have proposed that co-citation analysis and co-word analysis are complementary techniques. Specifically, van Raan and Tijssen (1993) reported that co-word analysis is relevant for studying scholarly domains where co-citation data may be limited, or where citation practices prevent such data from properly representing a scholarly domain. Furthermore, the retrieval rate for co-citation analysis compared to that of co-word analysis is much less (Raan and Tijssen 1993). In other words, co-word analysis can present a map of a scholarly specialty based on the majority of original publications in the dataset, whereas co-citation analysis does so to a far more limited degree. Focusing on the fact that relationships between co-words are substantially different from that between co-citations, certain authors (e.g., Callon, Law, Rip 1986; Morris and Martens 2008; van Raan and Tijssen 1993) suggest that co-words are a more objective measure of document similarity than co-citations. van Raan and Tijssen (1993, 177) argued, “Words are the foremost carrier of scientific concepts, their use is unavoidable and they cover an unlimited intellectual space”.

Anticipating validity concerns with the citation data and acknowledging the value that a mixed methods approach presents, the present study used the method of co-citation analysis supplemented by co-word analysis. Combining these complementary techniques facilitates cross validation and provides multiple perspectives by which to view the information security specialty.

5.2 Data Sources

The information security specialty literature is assumed representative in the research documents contained in the Scopus database. The decision to use Scopus was based on a number of factors. Research (e.g., Falagas et al. 2008; Kulkarni et al. 2009) indicated that Scopus offers wider coverage than the Web of Science, the only other major citation database in existence. It also outperforms other types of open access sources (e.g., Google Scholar) in terms of accuracy, coverage and consistency. Scopus article records include all of the relevant bibliographic information (e.g., Author name, Year, Affiliation country) needed for this study in addition to corresponding citation data. Moreover, Scopus offered export functionality designed to assist researchers with extracting document records for further analysis using third-party software.

The Scopus fact sheet, found on its Website, states that Scopus contains 50 million records in, 21,000 titles and from, 5,000 publishers. As a highly interdisciplinary database, Scopus covers research spanning from the natural sciences to the arts and humanities; such wide-ranging coverage is essential for this study as the information security specialty includes a broad range of researchers from various scholarly perspectives ranging from the humanities (e.g., law, policy) to science and technology (e.g., computer science, engineering). Moya-Anegon et al. (2007) presented evidence suggesting that Scopus is stronger than the Web of Science in the area of science and technology, particularly relevant for the information security research specialty,

since information technology has taken a prominent role in information security. In regards to geographical coverage, researchers (e.g., Moya-Anegon et al. 2007, 21) found that Scopus has expansive “homogenous global coverage". Another reason for this investigation not to choose Web of Science is that the present researcher does not have access to it.

Information security research is often tightly held by organizations for security purposes. Therefore, formal communications (e.g., research reports) of classified nature presented a constraint and was not included in this study. Often classified information relates to the most up-to-date national security and proprietary information security techniques and strategies. However, non-classified scholarly sources presented sufficient information security literature for analysis when dealing with a dataset that spans many years. The issue of classified research documents appeared to present the most limitations with regard to current government and proprietary documentation.

Novel research methods in the information science field, for example, altmetrics could have been used to study social web data pertaining to the information security specialty. However, the present researcher decided to forgo the inclusion of social web data, since "it is more oriented towards applications than utility to science" and "is used by the general public and may be used by academics differently from the ways in which they cite in scholarly publications." (Stud and Thelwall 2014, 1131).

5.3 Data Collection

There are three phases to the data collection procedures in this study. The first phase, illustrated in Table 5.1, relates to the bibliometric data.

Table 5.1 Phase 1: Bibliometric Data Collection

Procedures	Tasks
Document Search	• Query Scopus database using the following terms and their variations: information security, information assurance, cyber security, computer security, communications security, and network security • Query Scopus database for all documents indexed by Scopus from sources titles on information security • Set search filter to only collect articles, conference papers, and books • Specify record fields for data exporting
Aggregation, Cleansing & Identification of Top Cited Documents	• Combine the retrieved datasets • Remove duplicates & perform cleansing • Ranking documents by citation frequency • Identify top 100 highly cited documents
Frequency Ranking	• Author Name • Source Title • Year • Affiliation • Affiliation Country • Subject Area

The initial bibliometric data was collected via a Scopus database search set for each term listed in Table 5.1 (e.g., "information security"). The search terms were collected from a literature review and compiled by the current researcher to represent the various facets of the information security specialty. One of the search terms, "cyber security", was combined via the search string disjunction (i.e., "OR") to its spelling variation, "cybersecurity". The search produced one retrieved dataset for each chosen term. The various sets were aggregated into one comprehensive dataset.

Another search was conducted based on the records collected in the previous step to obtain all of the documents indexed by Scopus from the highest producing information security publication sources (e.g., Computers and Security, IEEE Privacy and Security, Journal of Computer Security). This set and the one of search terms were combined for removing duplicates and any results that are not in the form of articles, conference papers, and books. It is common for studies to collect data using keywords based on taxonomies. However, this current study's data collection technique (i.e., combining the information security taxonomy with documents from all high producing information security publication sources) is unique. The resultant dataset contained 58,908 bibliographic records relating to the information security specialty and spanning from 1972 to 2014. As noted by many researchers (e.g., Bayer, Smart, and McLaughlin 1990; Eom 2009), it is very important to cast a "wide net" when gathering bibliometric data. Therefore, the aforementioned variety of search terms and specific source titles in information security were used in order to improve recall. Limiting the retrieval of bibliometric data can lead to problems of validity and a limited view of the specialty. If not careful, as McCain (1990a) reported, important yet unforeseen research in ancillary domains at the outskirts of the research specialty may be excluded. The present study took the objective approach in selecting data by not using predetermined subjective lists and not limiting the initial data search in regards to date range (Eom 2009).

Specifically, the following information is obtained from each Scopus record gathered for this study: author name, document title, keywords, source title, year, affiliation, country, and abstracts. The abstracts are used later in the study to assist in interpreting and analyzing data in addition to serve as a data source for co-word analysis.

The final dataset was ranked by document citation frequency (i.e., author name + year + document title) and only the top 100 highly cited documents (see Appendix B) were selected to build a co-citation matrix. In addition, separate frequency rankings of the entire dataset were done on selected fields (e.g., publication frequency of authors) to ascertain salient features of the information security specialty.

The second phase, displayed in Table 5.2, addresses the procedures for computing the co-citation data.

Table 5.2 Phase 2: Co-Citation Data Collection

Procedures	Tasks
Co-Citation Data Search	• Use Bibexcel to automatically query the dataset conjoining each document and yielding a frequency by which the pair is co-cited in the set
Construct Co-Citation Matrix	• Build a 100 X 100 co-citation matrix in Bibexcel • Input co-citation frequencies at the intersection of documents in the matrix • Export matrix to Excel • Input highest co-citation frequencies in the diagonal cells of the matrix

The co-citation data was computed using Bibexcel software created by Olle Persson. Bibexcel creates files for further processing by parsing and extracting select record fields (e.g., cited documents) and constructing files containing only the particular field (Astrom et al 2009). The select records (e.g., 100 most highly cited documents) were identified using Bibexcel functionality. A Bibexcel algorithm was run conjoining each of the 100 most highly cited document references (e.g., "Document A" AND "Document B", "Document A" AND "Document C") and establishing the frequency by which each pair of documents is co-cited in the entire dataset. The co-citation measure quantitatively calculates the similarity between two

documents in terms of subject matter/topic. Co-citation is calculated by counting how many times, for example, documents A and B are cited together in other documents. That is, if document A and B are both cited within document C, D, and E, then documents A and B have a co-citation frequency of three. Furthermore, an underlying assumption of bibliometrics is that there is a positive correlation between co-citation frequency and subject relationship (i.e., higher co-citation frequency indicates a stronger subject relationship). The resultant co-citation frequencies were automatically inputted into a co-citation matrix file constructed by Bibexcel containing the respective co-citation count at the intersection between each document and producing a co-citation matrix. The matrix was exported to Excel for further refining and preparation.

As indicated earlier, there are 100 key (i.e., most highly cited) information security documents published between 1972 and 2014 in Scopus, which led to a 100 X 100 co-citation matrix. Diagonal cells in the matrix were filled with the highest value in a particular row or column. The logic behind the diagonal cell treatment is as follows: these cells display the degree to which a document co-cites itself. As a document is identical to itself, thus a diagonal cell should contain the highest co-citation frequency received, instead of putting a zero or leaving the cell blank (White and Griffith 1981). The product of phase two was an Excel file containing a matrix of co-citation frequencies, which illustrates the degree that two documents are related and provides the raw data for multivariate and network analyses to be discussed in the succeeding section.

Table 5.3 outlines the third phase of data collection procedures for the co-words.

Table 5.3 Phase 3: Co-Word Data Collection

Procedures	Tasks
Word Extraction	• Use Bibexcel to extract keywords from titles, keywords, and abstracts from the bibliometric dataset created in Phase 1
Normalize Keywords	• Export keywords into Excel and Notepad for further preparation • Combine and sort keywords alphabetically • Edit for synonyms and homonyms • Rank keywords based on frequency in descending order • Select the top 100 most frequently occurring words for matrix construction
Co-Word Data Search	• Employ Bibexcel to query the dataset pairing each of the 100 most frequently occurring words and computing frequency of each pair throughout the set
Construct Co-Word Matrix	• Build a 100 X 100 co-word matrix file in Bibexcel • Export matrix to Excel • Input highest co-word frequencies in the diagonal cells of the matrix

The bibliometric data collected from Scopus was revisited in this phase to undergo word extraction and co-word frequency computing via Bibexcel. Words were extracted and compiled from the document title, keyword, and abstract fields in the records. The inclusion of abstract keywords in the dataset increased the difficulty of data collection, but meanwhile enhanced validity in that it expanded the raw dataset for co-word extraction while authors and indexers might have chosen keywords based on titles. Some researchers (e.g., Leydesdorff 1997) have cautioned about the inaccuracy of word analysis when aggregating words using full-text across sets of documents, because the issue of accuracy might surface when a word is taken out of context. Yet, proponents have leveled such criticisms by persistently arguing that words are traditional carriers of scientific information (Callon and 1986; Courtial 1998), and research

indicated that the indexer effect is not a significant problem (Callon and 1986; Courtial 1994; Law and Whittaker 1992).

The extracted keywords were exported to Excel and Notepad when the file size exceeded Excel's limits, where they were combined and sorted alphabetically for screening. The keywords were ranked by frequency in descending order, and a threshold was established to obtain words of high frequency. Considering the parameters of this study, the top 100 most frequently occurring keywords (see Appendix C) were selected to create a 100 X 100 co-word matrix. Heeding the warnings of Hu et al. (2013), the present researcher identified and edited synonyms and homonyms. The overall co-word dataset of 100 individual words was automatically queried via the Bibexcel algorithm to search for each possible word pair and correspinding frequency by which it co-occurs across the entire dataset. In other words, if words A and B are both used in documents C, D, E, and F, then words A and B were considered to have a co-word frequency of four. The resultant co-word frequency was inputted into a Bibexcel matrix, which was exported to Excel for further refining and preparation. Similar to the co-citation data collection procedures above and based on the same logic, diagonal cells in the matrix were filled with the highest value in a particular row or column. The co-word frequencies indicate the level of relatedness between the two words as far as they are embedded in the given set of documents (van Raan and Tijssen 1993). According to Ding, Chowdhury, and Foo (2001, 819-820), “the higher co-occurrence frequency of the two words means the closer relationship between them” and this is considered a measure of intellectual structure.

5.4 Data Analysis

The present study employed four phases of data analysis, each corresponding to the four research questions posed in Chapter 4. The first three phases focused on the bibliometric data

using the records exported from Scopus, Excel, and descriptive statistics, while the fourth phase centered on the co-occurrence data with a variety of multivariate approaches via IBM's SPSS and Pajek – a bibliometric application for constructing network maps. The result of the fourth phase was a number of highly cited document and frequently used keyword clusters representing the research topic or subject group (i.e., intellectual structure) of the information security specialty. In addition, cluster and cluster label creation was guided by the present writer's examination of document titles, keywords, abstracts, full documents (e.g., textbooks and articles), and consultation of expert opinions (e.g., Dissertation Committee members). In some cases, the entire document was thoroughly studied when there was difficulty in deciphering its topic from the bibliographic information only.

Phase one analyzed the bibliometric data for the key features of the information security specialty by delineating author(s), keywords, publication source, affiliation, and country. Each record field, representing each key feature, was ranked in descending order according to its output frequencies. In phase two, the timeline of the information security specialty, based on the output of the entire dataset between 1972 and 2014, was plotted with corresponding frequency of publications for each year in the dataset displayed for revealing the emergence and development of the information security specialty.

The third phase took a view of scholarly domains, as represented by their respective publication sources (e.g., journals), which contributed to the information security specialty. Contributing domains were established by considering the subject areas Scopus professional indexers assigned to publication sources, as well as the present researcher's examination of the sources. The Scopus assigned subject areas generally correspond to scholarly domains. The current researcher also created new ones or made adjustments, where necessary, for a more

concise and accurate account. The resultant scholarly domains contributing to the information security specialty along with their proportions were charted for easy visual interpretation. The results addressed the third research question by showing which scholarly domains contribute to the information security specialty.

The fourth phase is intended to identify the intellectual structure underlying the information security specialty. The relationships among documents as well as keywords within the information security specialty were visualized via the co-citation and co-word data respectively. The SPSS software package was utilized to run factor, cluster, and multidimensional scaling (MDS) analyses on the co-occurrence matrices. Moreover, co-occurrence network maps developed based on graph theory were built using the Pajek network analysis application. The analysis processes were very similar for both the co-citation and co-word data. Nevertheless, it should be noted that co-citation analysis remained the primary technique in that co-citation frequencies are more representative of the dataset than co-word counts. Co-word analysis, in contrast, would be a technique for supplementing the co-citation examination. The specific analysis procedures and configurations are described in Appendix I.

Factor analysis was selected as one of the analytical techniques in this research, because Eom (2009) argued that factor analysis in conjunction with co-citation/co-word matrix data could be used to determine the fundamental intellectual structure of a scholarly domain. Cluster analysis was utilized as it can give a similar yet unique perspective compared to factor analysis. The process for cluster analysis is different from that of the factor analysis in that cluster analysis starts with treating each document/variable as a single cluster and then continuously groups neighboring clusters until all form a final, single cluster, while factor analysis allows individual documents/variables to load on to multiple factors. Last, but not the least, multidimensional

scaling was selected as an analytical technique for the reason that it would help uncover concealed structures among the data by drawing clear pictures of their associations on a two or three dimensional map. The aforementioned multivariate techniques are tested methods for co-occurrence data reduction and each puts forth a different perspective. Namely, factor analysis reduces the dataset to a number of factors, cluster analysis to a number of clusters, and MDS to two or three dimensional maps. The construction of a network map, on the other hand, provides a more visual account of the relationship among the co-occurrence pairs and also helps interpret what the multivariate techniques yield.

Factor analysis is a set of statistical techniques whose distinctive capability is data-reduction. Kim (1975, 24) describes factor analysis as follows:

> Given an array of correlation coefficients for a set of variables, factor analytic techniques enable us to see whether some underlying pattern of relationship exists such that the data may be 'rearranged' or 'reduced' to a smaller set of factors or components that may be taken as source variables accounting for the observed interrelations in the data.

Factor analysis was accomplished by taking the dataset and compressing the large amount of variables within it (e.g., individual documents or words) to a smaller set of fused dimensions (i.e., factors) representing research subspecialties/topics/schools of thoughts. Furthermore, Eom (2003) explained that the variables (e.g., documents, keywords) are to be viewed as dependent variables that are functions of the set of latent factors (i.e., subspecialties/topics). The factor analysis process illustrates how each document/keyword loads (i.e., contributes) to particular factors. Researchers (e.g., Conway and Huffcutt 2003) have described factor analysis as a technique used to organize data (e.g., documents, keywords) along factors (i.e., shared underlying variables) as a means to make the data more manageable. In line with White and Griffith's (1981) recommendations, SPSS was set to run orthogonal factor analysis and rotation

varimax solution. Among the SPSS output, a Scree test was used as an indicator of the appropriate number of factors (Culnan 1986).

Similar to factor analysis, Hair et al. (1992) also described cluster analysis as a data reduction technique. As suggested by McCain (1990), the current researcher used Ward's method for clustering. In the cluster analysis process, similar variables (e.g., documents, words) were grouped into clusters based on the established criterion (e.g., correlation coefficients of the co-occurrence matrix). Moreover, the aforementioned co-occurrence matrixes were transformed by the SPSS software into correlation matrices that were used to gauge the similarity or distance between the variables (McCain 1990). The clustering algorithm grouped the highly cited documents into sets based on shared quantitative properties of the data, and the current researcher presents each group based on an interpretation of the semantic commonalities among the group members.

According to Schiffman, Reynolds, and Young (1981), MDS is a set of statistical techniques/procedures that are used to generate two/three-dimensional images of data. The MDS procedures produce clustering between similar groups of documents/keywords graphing them along geometric points in space based on shared properties (White and Griffith 1981; McCain 1984). The co-occurrence frequency values are to correlate to the similarity or dissimilarity between the documents/keywords as depicted in geometrical terms. The MDS output presents spatial illustrations of the complex variables demonstrating their underlying relationships on multidimensional maps. The MDS maps facilitate visual interpretation of the complex data.

Lastly, Easley and Kleinberg (2010) explain network analysis as using graph theory to uncover network structure based on the properties of given objects. Network analysis uses terms like graph, node, link, and edge. For example, network analysis allows one to graph nodes (e.g.,

highly cited documents) based on shared aspects between those nodes (e.g., frequency by which the two highly cited documents appear within a dataset). The shared appearance of these two highly cited documents is shown by a line (i.e., link) which physically connects the two nodes in the graph. The graph represents the intellectual space that comprises information security and the complex system of interconnecting highly cited documents is outlined using edges (i.e., particular sets of connected nodes within the overall graph that share a distinct property compared to the rest of the network). These edges can be analyzed to draw distinctions about the intellectual structure of the information security specialty.

5.5 Methodological Limitations

Although a number of limitations have already been discussed in previous sections, there are still some that need to be addressed. The chosen scientometrics methodology and the inclusion of its techniques (e.g., co-citation and co-word analysis) introduce some notable obstacles for validity and reliability.

In addressing the limitations of scientometrics, Rip (1988) suggested that one ought to be cautious generalizing the idea that science domains can be uniformly measured based on publication output. Some science domains (e.g., physics, chemistry) produce research publications as a primary output, while other applied science domains or humanities domains may not. Additionally, Rip pointed to possible database biases in relation to developing countries and language. In regards to Rip's last point, Scopus has sufficient international coverage to minimize such biases. However, Rip's former concerns are valid when considering a research specialty such as information security that is heavily oriented around applied science and technology and in some cases, humanities research. Conference papers indexed in Scopus are to be included in the dataset to support the applied science and technology aspect of information

security. Digital publishing has made it easier for technical publications of the type that applied science and technology produce to come to be included in databases such as Scopus; while, books are also to be included to support humanities research. The separation of signal from noise, according to Rip, should also be an area of concern as most techniques used to set cutoff thresholds based on citation frequency or word occurrence frequency are arbitrary. The present research used the substantial amount of prior co-occurrence research that has been produced over the last few decades as the basis to set a threshold.

One of the major objectives set forth by this research is to use bibliometric data to produce an up-to-date profile and map of the information security specialty for science policy makers. Yet, there is a lag time, as Bjork (2013) reports, ranging from nine to 18 months involved with publishing peer reviewed scientific research. However, conference papers have a much shorter publication timeline and research shows that disciplines (e.g., computer science) that heavily contribute research to information security predominately use conference papers as a means of scholarly communication (Fortnow 2009; Franceschet 2010). While acknowledging this inherent limitation, such a variable was dealt with by not limiting the bibliometric data in regards to a set period. Moreover, the most current 2014 publications indexed by Scopus are also to be included as the timeframe of this research allows. Another issue with time relates to the difficulty of capturing a view of the information security specialty bearing in mind that scholarly domains are active entities. This issue was dealt with by selecting bibliometric techniques specially designed to cope with change. The author has considered multiple bibliometric techniques, including bibliographic coupling. According to Garfield (2001, 3), co-citation analysis and bibliographic coupling both "prove to be accurate markers for the emergence of new topics". Nevertheless, Garfield (2001, 3) goes on to say, "bibliographic coupling is retrospective

whereas co-citation is essentially a forward-looking perspective". Therefore, co-occurrence techniques (e.g., co-citation and co-word) were selected over bibliographic coupling, since they are considered "forward-looking" techniques capable of changing with time as new works are produced citing different documents and using different words resulting in a reconstituted landscape of information security.

Some authors have pointed to intrinsic limitations with using citation data leading to problems with validity and reliability (e.g., Edge 1977; MacRoberts and MacRoberts 1986, 1989, 1996) and technical difficulties with accuracy (Moed 2005; Seglen 1998). A central problem with the validity and reliability of co-citation analysis, according to Edge (1977), stems from the belief that citation data, a quantitative unit, can stand alone and usurp more qualitative data (e.g., expert interviews). According to White (1990), Edge's suggestion is false and his tone should be reconsidered, since co-citation analysis proponents (e.g., Eom 2009, 13) have clearly argued that co-citation analysis works best as a "supportive quantitative tool". Considering such suggestions, the present study combined multiple techniques (e.g., co-citation analysis and co-word analysis) and different types of data (e.g., documents and words).

Moed (2009, 170) pointed to a number of limitations involved with bibliometric data, including variations in author affiliation names, incomplete access to institutional affiliation and affiliation country, and "subfield classification system based on journal categories". The first three issues highlighted by Moed were dealt with by using a single database (i.e., Scopus) which attempts uniformity in regards to such bibliographic information. Nevertheless, variation within publication sources may exist in relation to the way in which bibliographic information is displayed and Scopus indexing practices inherently limit this study. Nevertheless, meticulous and comprehensive screening of bibliographic information was employed to address this issue.

The fourth issue argues that using the journal as a unit for analysis when deciphering contributing domains prevents a more granular view of sub-specialties, especially in an interdisciplinary specialty. This was not be a problem, since the researcher is to examine the publication sources based on multiple facets (e.g., published documents within the source, source title keywords, Website review) allowing this study to take a more thorough account. Garfield (1979b) had similar concerns to that of Moed (2005) in regards to multiple authors, since databases had only indexed first authors. Limits pertaining to first authors were not an issue as the present study is to avoid such complications by focusing on publications themselves in the co-citation analysis and at present, Scopus indexes all authors. The reader should note, however, that the presence of multiple authors is an inherent limit for deriving key authors (covered in RQ 1), since at present there is no agreed upon standard to assign value to authors in documents that contain multiple authors.

MacRoberts and MacRoberts (1989) and Smith (1981) raised additional concerns about citation data, namely citation bias, negative citations, self-citations, and synonyms and homonyms. In regards to self-citations, Scopus has increased its functionality to include options to exclude author self-citations. Citation behavior, discussed in Nicolaisen (2007), has been observed to vary in regards to citation techniques and motivations. Nevertheless, citation bias is not an issue in this study, because prior research indicates (e.g., Pilkington and Meredith 2009; Price 1965) that large sample sizes, such as the one in this study, reduce any significant impact posed by such variations. Negative citations are not an issue in this study, since negative citations primarily influence research that assigns qualitative value to citation counts. Moreover, such studies assume citations as positive indication of peer acknowledgment of quality. The current study used citations to measure similarity in terms of the topic/subject matter covered in

research documents, not quality. The researcher in this study approached the issue of synonyms and homonyms by careful examination and preparation of the data.

Finally, mapping the intellectual landscape of a scholarly domain has unavoidable limits to consider as De Bellis (2009, 142) pointed out, “maps do not faithfully reproduce a landscape, nor can they be trusted as truly objective representations of an outer reality”. In other words, a map is a scaled model and can never be the actual object/concept it purports to represent. A model is a human construction underscored by its maker’s selection of what to include and leave out, thus, removing an object’s/concept’s properties from its respective context. Nevertheless, such inherent limits should not preclude such endeavors, for the reason that quantitatively painting a big picture of a scholarly domain presents benefits that other subjective methods cannot. Rip (1988, 260) suggested that in comparison to objective reviews (e.g., the one to be taken in this dissertation), subjective reviews of scholarly domains "do not picture the state-of-the-field, but are accounts of it, as it were the story about it as the authors want to tell it". In other words, expert accounts and reviews are specifically curtailed to particular audiences, intending to persuade readers of the narrow perspective of the scholarly domain as the author views it. Expert reviews were not chosen as a method, because of their highly unreliable nature. Borner, Chen, and Boyack (2003, 180) explain the risk of using expert reviews by referring to a well-known Indian legend regarding the blind men and the elephant:

> Six blind men were trying to find out what an elephant looked like. They touched different parts of the elephant and quickly jumped to their conclusions. The one touching the body said it must be like a wall; the one touching the tail said it was like a snake; the one touching the legs said it was like a tree truck, and so forth.

Not only is the information security specialty large like the elephant and difficult to grasp through narrow subjective evaluation, it is in constant flux. Therefore, methodologically

reducing such complexity into an objective, easy to understand visual depiction based on a combination of quantitative data guided by qualitative inference will serve as a manageable decision support tool.

6. Results and Analysis

6.1 Overview

The present chapter reports research findings of the scientometric study of the information security specialty using 58,908 records published from 1972 to 2014. The subsequent sections are organized by the four research questions formulated for this study. In the first section, the first research question was dealt with by tabulating the bibliometric properties of the data with reagrd to authors, source titles, author affiliations, countries, and years. Identifying these key features of the information security research literature highlighted its salient properties and facilitated the creation of a specialty profile. The next section corresponded to the second research question as it analyzed the total year-wise publication output of the information security documents showing the emergence and evolution of the information security specialty over time. The succeeding section approached the third research question by investigating the scholarly domains that contributes to information security literature by examining and categorizing source titles. The last section approached the forth research question pertaining to the intellectual structure of the information security specialty. The specialty's intellectual structure was studied using co-citation and co-word analyses. Furthermore, the multivariate and network analyses facilitated the development of a scheme representing the intellectual structure of information security as it presents itself via its formal research literature.

6.2 Salient Features of the Information Security Specialty

The present section is composed of four subsections each addressing a different bibliometric property of the information security dataset. The bibliometric properties under examination are authors, source titles, author affiliation in terms of academic institutions, and

author affiliation with respect to country. Together, these bibliometric variables make up the information security specialty profile.

6.2.1 Key Authors and Their Publication Output

The descriptive analysis of author publication output is a good starting point to reveal the salient properties of the information security research specialty. Table 6.1 lists the 100 authors and their respective number of publications (f).

Table 6.1 Top 100 Authors and Their Publication Output

Author Name	**f**	**Author Name**	**f**	**Author Name**	**f**	**Author Name**	**f**
Ma, J.	124	Zhou, J.	47	Bradbury, D.	38	Guan, X.	32
Furnell, S.	105	Won, D.	47	Li, J.	38	Kim, T.H.	32
Highland, H.J.	93	Hwang, M.S.	47	Li, T.	37	Yang, W.	32
Susilo, W.	91	Ning, P.	46	Yoon, E.J.	37	Kotenko, I.	32
Bertino, E.	88	Cohen, F.	46	Hinde, S.	37	Boneh, D.	32
Jajodia, S.	87	Yoo, K.Y.	45	Cuppens, F.	36	Basin, D.	32
Feng, D.	82	Blobel, B.	45	Chen, Z.	36	Sandhu, R.	32
Perrig, A.	69	Goucher, W.	45	Yupapin, P.P.	36	Wu, J.	31
Forte, D.	67	Bishop, M.	44	Power, R.	36	Li, C.T.	31
Chang, C.C.	65	Backes, M.	44	Von Solms, R.	35	Samarati, P.	31
Deng, R.H.	64	Eloff, J.H.P.	44	Goedert, J.	35	Katzenbeisser, S.	31
Yang, Y.X.	63	Gritzalis, D.	44	Zhou, W.	35	Massacci, F.	31
Cao, Z.	59	Liu, P.	43	Wang, H.	35	Xiao, Y.	31
Mu, Y.	58	McDaniel, P.	43	Song, D.	34	Cuppens-Boulahia, N.	31
Sadeghi, A.R.	57	Lee, C.C.	43	Safavi-Naini, R.	34	Ahn, G.J.	31
Keromytis, A.D.	56	Zhang, L.	42	Yung, M.	34	Goldberg, I.	30
Kruegel, C.	53	Gritzalis, S.	42	Li, N.	33	Jha, S.	30
Zhang, H.	52	Vigna, G.	41	Camenisch, J.	33	Savola, R.	30
Sakurai, K.	52	Gold, S.	41	Lin, C.	33	Dai, Y.	30
Imai, H.	52	Reiter, M.K.	41	Xiang, Y.	33	Crispo, B.	30
Tsudik, G.	52	Sun, H.M.	40	Potter, B.	33	Obaidat, M.S.	30
Everett, C.	50	Meinel, C.	39	Li, Y.	33	Allaert, F.A.	30
Preneel, B.	50	Van Oorschot, P.C.	39	Zhang, Y.	32	Fang, B.X.	30
Varadharajan, V.	49	Lee, W.	38	Kirda, E.	32	Thuraisingham, B.	30
Bao, F.	48	Lee, D.H.	38	Guo, L.	32	Capkun, S.	30

As shown in Table 6.1, the top 100 seminal authors made extensive contributions to the information security specialty, each published at least 30 documents and together they published 4,399 documents within the 58,908 dataset. It should be noted that Scopus records author last names combined with first initials. With some nationalities such as Chinese, this practice can be problematic since there are only about several hundred last names for China's over 1.3 billion people and some common last names (e.g., Zhang) could be shared by more than 100 million people.

The top 15 key authors are responsible for approximately 25% of the 4,399 total publications in Table 6.1. Author output is seen varying from the highest output (e.g., Ma = 124) to the lowest (e.g., Capkun = 30). Researchers (e.g., Clark 1957; Cole 1992; Price 1963) have indicated that there is a positive correlation between publication quantity and quality. Thus, the 15 most productive authors also appear to be the leading researchers in the information security specialty.

Table 6.2 details the top 15 authors' affiliations, countries, and publication subject areas as extracted from Scopus records. With the exception of Highland from social sciences and Susilo, Cao and Mu from Mathematics the rest of the most prolific authors in information security all have academic backgrounds in computer science and engineering. From a geographical point of view, the majority of authors are from the United States and China. Furthermore, there are some authors presented in Table 6.2 from other countries (e.g., Australia, United Kingdom, Italy), but to a less extent. Two out of the 15 author affiliation institutions are private companies, namely H.J. Highland's association with Compulit, Inc and D. Forte with DFLabs. Compulit, Inc provides litigation support via digital services (e.g., digital forensics) to law firms, while DFLabs offers information security consulting services to organizations. The

majority of the other author affiliations are nonprofit research organizations such as universities and labs.

Table 6.2 Mini-Profiles of the Top Authors

Author Name	Affiliation	Country	Subject Areas
Ma, Jianfeng	Xidian University, State Key Laboratory of Integrated Service Networks	China	Computer Science, Engineering
Furnell, Steven M.	Plymouth University Centre for Security Communications, Centre for Security, Communications and Network Research	United Kingdom	Computer Science, Engineering
Highland, Harold Joseph	Compulit, Inc.	United States	Computer Science, Social Sciences
Susilo, Willy	University of Wollongong, School of Computer Science and Software Engineering	Australia	Computer Science, Mathematics
Bertino, Elisa.	Purdue University	United States	Computer Science, Engineering
Jajodia, Sushil	George Mason University, Center for Secure Information Systems	United States	Computer Science, Engineering
Feng, Dengguo	Chinese Academy of Sciences, Institute of Software, Trusted Computing and Information Assurance Laboratory	China	Computer Science, Engineering
Perrig, Adrian	Carnegie Mellon University, CyLab	United States	Computer Science, Engineering
Forte, Dario Valentino	DFLabs	Italy	Computer Science, Engineering
Chang, Chinchen	Asia University Taiwan, Department of Computer Science and Information Engineering	China	Computer Science, Engineering
Deng, Robert	Singapore Management University, School of Information Systems	Singapore	Computer Science, Engineering
Yang, Yixian	Beijing University of Posts and Telecommunications, National Engineering Laboratory for Disaster Backup and Recovery	China	Computer Science, Engineering
Cao, Zhenfu	Shanghai Jiaotong University, Department of Computer Science and Engineering	China	Computer Science, Mathematics
Mu, Yi	University of Wollongong, School of Computer Science and Software Engineering	Australia	Computer Science, Mathematics

Whiteman and Mattord (2012) discuss people, processes, and technology as foundational pillars of an information security framework. Yet, the view in Table 6.2 of the leading

researchers and their backgrounds appears to indicate a focus on technology while there is little sign of seminal researchers who specialize with people or processes. This contradicts the findings of Dlamini, Eloff, and Eloff (2009) who used survey research and concluded that in 2005 and 2006 there was a shift in focus for information security researchers from technical perspectives to strategic governance and regulation.

Table 6.3 displays the highest cited documents for each of the top 15 authors published in the overall dataset collected for this study. The emphasis on technically related research observed in Table 6.2 is further supported by observations in Table 6.3 with a deeper inspection into leading author documents. Each publication can be analyzed with regard to its title to get an overall sense of its subject matter/topic emphasis. Though debatable, research has generally asserted that the nature of highly cited documents is such that they have a close subject association with the documents citing them (De Bellis 2009; Garfield 1955). It is for this reason that the technical disposition of these highly cited documents of the most prolific 15 authors demonstrates that the greater set of citing documents should also be of a technical nature. It should be mentioned that Highland, the sole author among the most productive 15 from the social sciences, likewise has his top cited document focusing on data encryption, a technically related subject.

Table 6.3 Highest Cited Documents of the 15 Most Prolific Authors

Author Name	Key Document	Cited By
Ma, Jianfeng	2004. "A New Authentication Scheme with Anonymity for Wireless Environments." *IEEE Transactions on Consumer Electronics* 50 (1): 231-235.	94
Furnell, Steven M.	2007. "Authenticating Mobile Phone Users using Keystroke Analysis." International Journal of Information Security 6 (1): 1-14.	64
Highland, Harold Joseph	1997. "Data Encryption: A Non-Mathematical Approach." *Computers and Security* 16 (5): 369-386.	29
Susilo, Willy	2010. "Attribute-Based Signature and its Applications." *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*: 60-69.	39
Bertino, Elisa.	2009. "Security Analysis of the SASI Protocol." *IEEE Transactions on Dependable and Secure Computing* 6 (1): 73-77.	39
Jajodia, Sushil	2003. "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks." *ACM Transactions on Sensor Networks (TOSN)* 2 (4): 500-528.	433
Feng, Dengguo	2009. "An Improved Smart Card Based Password Authentication Scheme with Provable Security." *Computer Standards and Interfaces* 31 (4): 723-728.	69
Perrig, Adrian	2003. "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks." *INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies*. 3: 1976-1986.	366
Forte, Dario Valentino	2007. "Security Standardization in Incident Management: The ITIL Approach." *Network Security* 2007 (1): 14-16.	7
Chang, Chinchen	2009. "An ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem." *Computers and Security* 28 (3-4): 138-143.	63
Deng, Robert	2004. "Anonymous Secure Routing in Mobile Ad-Hoc Networks." *29th Annual IEEE International Conference on Local Computer Networks, IEEE*: 102-108.	78
Yang, Yixian	2010. "An Efficient Protocol for the Private Comparison of Equal Information Based on the Triplet Entangled State and Single-Particle Measurement." *Optics Communications* 283 (7): 1561-1565.	43
Cao, Zhenfu	2007. "Simple Three-Party Key Exchange Protocol." *Computers and Security* 26 (1): 94-97.	107
Mu, Yi	2008. "Cryptanalysis of Simple Three-Party Key Exchange Protocol." *Computers and Security* 27 (1-2): 16-21.	57

In addition to shedding light on the profile of the information security specialty, what has been learned about the 15 seminal authors would help academic institutions produce quality information security research programs. Moreover, academic institutions looking to fill faculty positions might consider the top 100 authors in Table 6.1 as viable candidates. Private and public organizations seeking research consultants may want to take note of these authors and their

respective affiliations. Government intelligence organizations looking to keep an eye on the latest developments in information security might consider keeping track of the research activities of theses prolific scholars.

6.2.2 Key Publication Sources

Publication sources play two roles in this study: identification of key publication sources to inform information security researchers, and the investigation of subject make-up of the information security specialty. The former role is discussed in this section, and the latter will be covered in section 6.4. Table 6.4 presents key publication sources along with associated frequencies in the dataset for this study. It is immediately obvious that the source that published the largest number of documents in information security, *Lecture Notes in Computer Science,* accounts for 18.1% of the total included in Table 6.4. What is more, *Lecture Notes in Computer Science* has more than twice as many publications as the source with the second highest output (i.e., *Computers and Security* 7.8%).

Table 6.4 Key Source Titles in Information Security

Source title	f	%
Lecture Notes in Computer Science Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics	3781	18.1
Computers and Security	1632	7.8
Proceedings of the ACM Conference on Computer and Communications Security	1611	7.7
Proceedings 2010 3rd IEEE International Conference on Computer Science and Information Technology Iccsit 2010	1389	6.6
Journal of Information Science and Engineering	1379	6.6
IEEE Transactions on Information Forensics and Security	805	3.8
Communications in Computer and Information Science	706	3.4
Network Security	682	3.3
Proceedings of SPIE the International Society for Optical Engineering	586	2.8
IEEE Security and Privacy	583	2.8
Proceedings International Carnahan Conference on Security Technology	536	2.6
Computer Fraud and Security	535	2.6
International Journal of Network Security	478	2.3
Security and Communication Networks	461	2.2
ACM International Conference Proceeding Series	443	2.1
International Journal of Security and Its Applications	421	2.0
Proceedings International Conference on Networks Security Wireless Communications and Trusted Computing Nswctc 2009	393	1.9
Journal of Computer Security	365	1.7
Information Management and Computer Security	354	1.7
5th International Conference on Information Assurance and Security IAS 2009	353	1.7
Studies in Health Technology and Informatics	335	1.6
IEEE Transactions on Dependable and Secure Computing	326	1.6
Proceedings Annual Computer Security Applications Conference Acsac	316	1.5
Information Security Technical Report	303	1.4
Proceedings IEEE Symposium on Security and Privacy	301	1.4
Applied Mechanics and Materials	285	1.4
1st International Conference on Multimedia Information Networking and Security Mines 2009	280	1.3
Nswctc 2010 the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing	271	1.3
Advanced Materials Research	255	1.2
2nd International Symposium on Electronic Commerce and Security Isecs 2009	254	1.2
Proceedings IEEE Military Communications Conference MILCOM	253	1.2
Infosecurity	242	1.2
Total	20914	100

Information security is not the sole subject area *Lecture Notes in Computer Science* publishes. While, the vast majority of the other sources that are most prolific in the area of information security are specifically tailored towards the topic of information security. This prompted a further examination by the current author to uncover how it is that a source title not dedicated to information security research could produce the greatest number of information security publications in this study's dataset. Other studies (e.g., Baskaran 2013) focusing on major source publications in information security have also found *Lecture Notes in Computer Science* being the top ranked title. Established database services (e.g., Scopus, OCLC's WorldCat) consider *Lecture notes in Computer Science* a single journal/series, yet a further look reveals that, unlike other source publications, *Lecture Notes in Computer Science* is a collection of assorted conference proceedings and monographs. Regardless of its nature, it is clear that *Lecture notes in Computer Science* can be a valuable resource for information security publications so it is included in the list of key sources.

Table 6.4 suggests that the technically oriented scholarly societies IEEE and AMC maintain importance within the information security specialty. Publications emanating from these two societies go through a peer reviewed process in which publication agenda setting criteria are steered by their respective editorial boards who are generally selected from the technical academic disciplines of computer science and engineering. Table 6.4 is composed of 32 of the most productive source titles that were found to contribute publications to this study's dataset. Six of the 32 top producing source titles come from the IEEE Society and two are ACM source titles. The second highest contributing source title in Table 6.4 is *Computers and Security* with 1,632 publications in Scopus between 1972 and 2014 accounting for 7.8% of the total number of publication (i.e., 20,914) displayed in Table 6.4. *Computers and Security* is the offical

journal of the InterNational Committee for Technology Standards (INCITS), a United States based research organization dedicated to constructing information technology standards. The INCITS is also a part of the International Federation for Information Processing (IFIP), which has worldwide membership and seeks to set global standards. Moreover, *Computers and Security* publishes articles geared towards process and technically oriented issues for information security (e.g., audit control, data integrity, and computer security).

Infosecurity is the least contributing source title in this study's dataset with 242 publications published in Scopus between 1972 and 2014. Upon further examination, the current author found that Scopus only indexed *Infosecurity* between the years 2007 and 2011. Moreover, *Infosecurity* was, indeed, prolific averaging 71 publications per year despite its position on the list in Table 6.4. *Infosecurity* is a United Kingdom based source title that is mainly distributed throughout Europe. According to Scopus, its broad topic coverage ranges from process-oriented research in business, management and accounting to more formal research with computer science applications.

Their appears to be 13 out of the 32 source titles dedicated to conference proceedings, indicative of the information security specialty being an applied research domain with close ties to computer science and engineering. Interestingly, two of the 32 most productive source titles (i.e., *Applied Mechanics and Materials* and *Advanced Materials Research*) lean towards the materials science and engineering academic disciplines. These two source titles have a heavy research focus intersecting nanotechnology and computer security. Another point of interest is the presence of *Studies in Health and Informatics* among the top 32 most productive source titles in information security. Its existence on the list implies that there is a significant research focus on securing health and medical related information.

In a related study, Dlamini, Eloff, and Eloff (2009) used their expert knowledge to determine that *Computers and Security*, *Computer Fraud and Security*, *IEEE Security and Privacy*, and *Information Management and Computer Security* were the most prominent sources for information security research during 2005 and 2006. According to Table 6.4, the current research confirms the findings Dlamini, Eloff, and Eloff reported.

Wallace and Bonzi (1985) suggest that overall journal publication output positively correlates to journal quality and citation frequency. The aforementioned source list can, therefore, be a useful tool in a number of ways, namely helping information security researchers in identifying core sources for submitting their manuscripts, assisting scientists to locate related publications while drafting their own research reports, and supporting acquisition librarians in their selection of periodicals for collection development.

6.2.3 Top Contributing Author Affiliations

Similar to authors and publication sources, author affiliations (e.g., academic institutions, research laboratories) have been the subject of scientometric research. In particular, Mcallister and Narin (1983) uncovered a significant positive correlation between the publication output of academic institutions and government research grant funds received, while Anderson, Narin, and Mcallister (1978) also observed a significant positive correlation between a university's publication output and citations made to those documents.

Figure 6.1 points out the top author affiliations within information security in terms of academic institutions. The 46 institutions listed in Figure 6.1 were identified within the present study based on the high number of publications that they contributed to the overall dataset. In total, the 46 institutions contributed 11,880 publications to this study's dataset. The variation of publications that were contributed by each institution ranges from Xidian University's 543

publications to Southeast University's 164. Among all the affiliations listed in Figure 6.1, the majority are located in China and the United States. In addition, China outnumbers all other countries, including the United States, in terms of author affiliations. However, China's dominance or even presence is entirely absent in the top source titles Table 6.4 list. This disparity is likely because the Chinese government requires its scientists and scholars to publish in source publications indexed by such non-Chinese services as SCI (Science Citation Index), SSCI (Social Sciences Citation Index), and EI (Engineering Index). Chinese authors would be rewarded with promotion, monetary awards and more if their manuscripts are published in, for example, a SCI indexed source title.

Xidian University's predominate subject focus is engineering and to a lesser degree computer science. According to Scopus, it mostly contributes publications to Chinese journals (e.g., *Tien Tzu Hsueh Pao Acta Electronica Sinica*), but also some western source titles (e.g., *Lector Notes in Computer Science*). The IEEE is another author affiliation (see Figure 6.1) that has a main research interest in engineering and to a lesser extent computer science. IEEE is the largest professional association and originates from the United States. Authors that produce research for the IEEE typically concentrate on emerging technology trends. A more detailed look into Scopus shows that the author affiliations (see Figure 6.1) Wuhan University with 403 publications and Purdue University with 383 are much more diverse academic institutions in terms of their subject focus. Another notable top 10 affiliation is Carnegie Mellon University, which houses the Computer Emergency Readiness Team (CERT) at its Software Engineering Institute. CERT was established in 1988 by Carnegie Mellon University to study computer security threats. It also serves as a vital asset for the United States' Department of Homeland Security on issues.

The list of top contributing affiliations is mainly composed of nonprofits (e.g., universities and professional associations). However, there are also a number of prominent institutions from private industry as well, for example, the two institutions IBM Thomas J. Watson Research Center and Microsoft Research. The IBM Thomas J. Watson Research Center dates back to the early 1960s, before the development of modern information security (see Appendix A) and it is the largest engineering research center in the world. In general, IBM has been around since the early 1900s and it was a major technology producer for the United States government during WWII. The highest cited document (i.e., Jain, Ross, and Pankanti 2006) produced by the IBM Thomas J. Watson Research Center was cited 297 times and it aimed at investigating biometric authentication techniques. It was published in *IEEE Transactions on Information Forensics and Security*.

On the other hand, Microsoft Research started during the early 1990s. Microsoft was a major factor in the emergence of modern information security as it moved computer technology into the mainstream of society with the mass development and distribution of its Window operating system and associated software for personal computers. The Windows operating system has been the most widely used in the world for decades making it a popular target for computer threats. It is for this reason that Microsoft Research is heavily involved with advancing information security technology. Microsoft's top cited document (i.e., LaMacchia, Lauter, and Mityagin 2007) was published in *Lector Notes on Computer Science* and it was cited 123 times. The article's primary research topic was cryptographic key management.

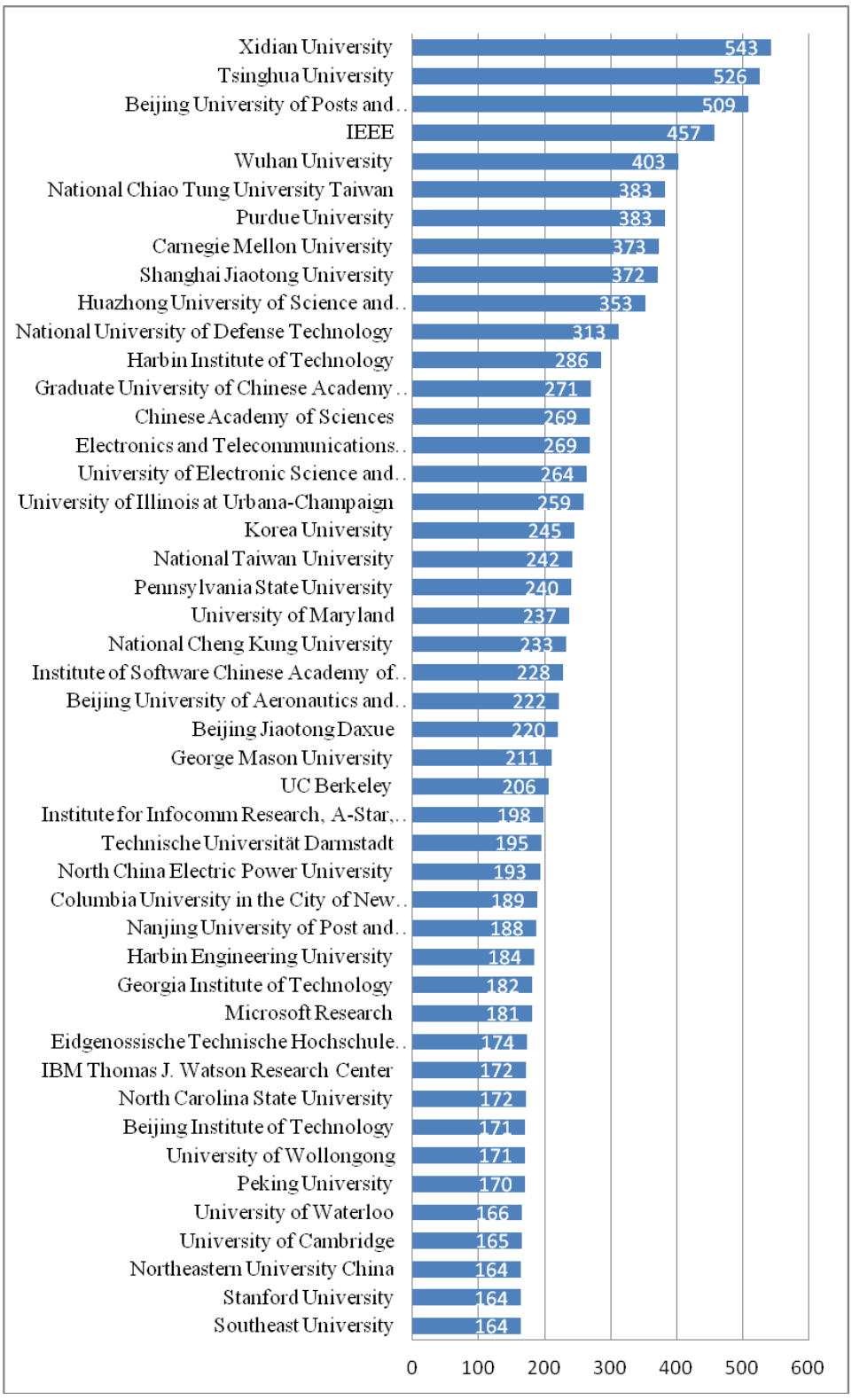


Figure 6.1 Top Contributing Affiliations of the Information Security Specialty

Other governments who wish to stay competitive in information security should take note and support their respective academic institutions in their own countries. Figure 6.1 can be used by public and private organizations to retain research services from the most qualified academic institutions. Furthermore, researchers looking to seek employment among the top academic institutions in the information security domain perhaps can view this figure as a rating guide. Lastly, information security students deciding on universities to attend may draw upon this analysis to decipher universities with quality specializations in information security.

6.2.4 Key Author Countries

The scholarly domain of information security has widespread implications for national and international policy and science. More precisely, information security has taken center stage in national and international media coverage, national defense debates and strategies. Therefore, governments and those with national information security interests (i.e. most national and multinational organizations) have a stake in understanding the information security domain from a geographical/national point of view. National science policy stakeholders, as argued by Leydesdorff (1987), seek to adjust the cognitive dimensions of scientific development by steering scholarly domains via institutional factors (e.g., funding). In addition, research (e.g., Leydesdorff 2004) suggests that an understanding of scientific productivity by country can be used by national science managers to test the outcome of efforts to influence scholarly research.

Figure 6.2 highlights the 15 most productive countries that contributed to this study's dataset. The most salient feature appears to be the corresponding percentage of output shared by China and the United States (i.e., the greatest contributing nations). Together, China and the United States account for over half of the output. Another significant feature is the variation between China and the United States and the other nations. The third highest contributing

percentages (i.e., Taiwan, China; United Kingdom) are close to five times smaller than that of the two largest. Figure 6.2 shows that the top 15 producing countries range from China's 13,848 information security publications to Switzerland's 622.

With regard to cryptography research productivity, Baskaran (2013) found that China, United States, and Russia all led as the highest producers of research literature from 2000 to 2011, respectively. Baskaran argued that there is a positive connection between economic activity and publication production. The present study confirms Baskaran's findings that China and the United States are among the most prolific information security research producers. However, there is a significant diverengence between the findings in this present study and those presented in Baskaran (2013). That is, Baskaran observed that Russia closely followed China and the United States as the third greatest producer of research on cryptography, whereas the results of this current study indicates that Russia is not among the top 15 information security research publication producers listed in Figure 6.2. Moreover, research (Clarke and Knake 2010) has argued that Russia is among the world's top cyber security powers. This anomaly prompted further investigation, yet no clear evidence pointing to a reason for the inconsistency could be found. The current author, however, suggests that one probable cause could be the level of secrecy implemented by the Russian government surrounding information security research.

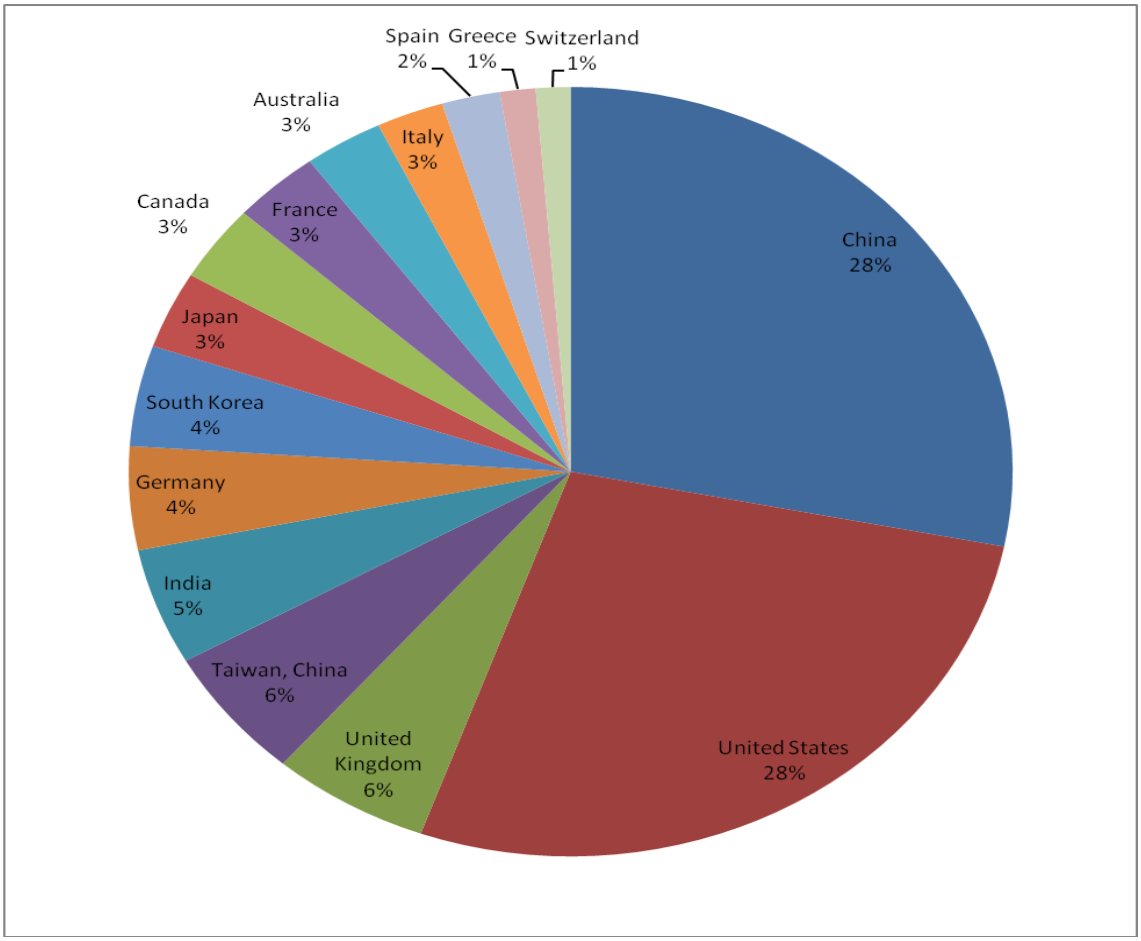


Figure 6.2 Key Countries and Distribution of Their Research Publications

The present author looked into the diverse contributions from the various countries in terms of the research topics from their most highly cited articles. The most cited document from India (i.e., Kumar and Zhang 2006), for example, was cited 113 times according to Scopus and proposed new bimodal biometric security techniques. On the other hand, Germany's most highly cited document (i.e., Scarani et al., 2009) within the current study's dataset was cited 352 times and centered on the topic of cryptographic key distribution. South Korea had its highest cited publication (i.e., Chebrolu, Abraham, and Thomas 2005) cited 163 times focusing on intrusion detection systems. One commonality among all of these countries is that the majority of their articles were published in source titles from the United States.

The dual prominence of China and the United States also impelled a more detailed investigation of the publication profile of these two top countries.

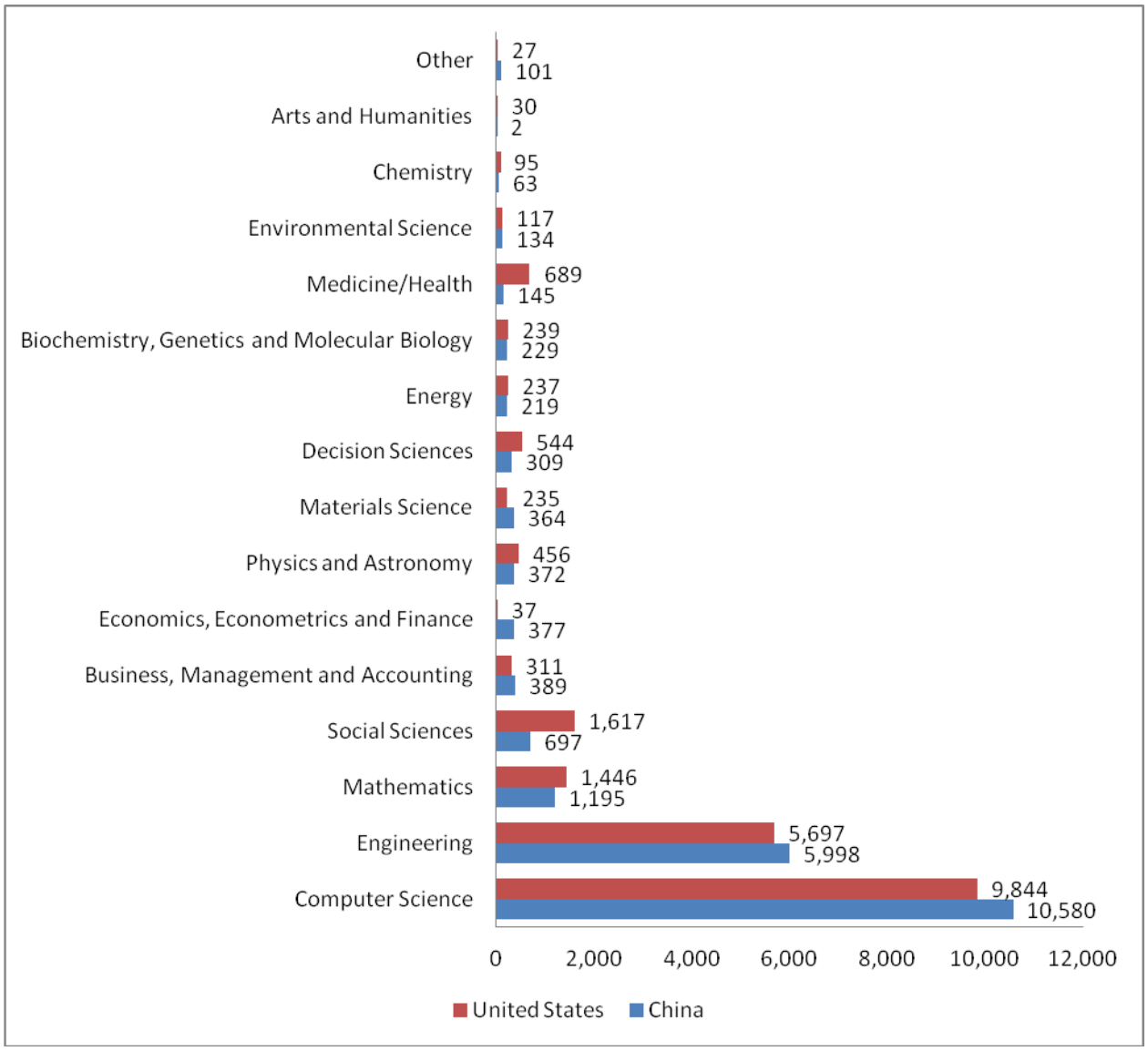


Figure 6.3 Research Output Comparison of China and the United States by Contributing Domain

Figure 6.3 points out the similarities and differences between Chinese and American information security publications in terms of contributing domains. The contributing domains in Figure 6.3 were based on Scopus' indexing of each article in terms of academic subject. The United States appears to have a more pronounced focus in the areas of mathematics, social

sciences, decision sciences, and medicine/health; while, China centers on computer science and engineering. Moreover, the United States is seen contributing to the information security specialty in more diverse ways, in particular with publications from less technically oriented scholarly domains (e.g., social sciences and medicine/health).

A more detailed review of the data suggests that one potential reason for the variations between these two countries is that the United States has a greater focus on cyber security and China on network security. When parsing the entire dataset using only the particular search term, “Cyber Security” the United States contributes substantially more (i.e., over 14 times more) research publications than China. While at the same time, when looking at this study's dataset from the perspective of only the search term, "Network Security" China produces approximately 69% more research publications than the United States. As an area of research, cyber security is primarily concerned with studying the protection of electronic computing systems that support social institutions, for example, critical infrastructure (Solms and Niekerk 2013). Furthermore, it is much more inclusive of research from the social sciences that highlight, for example, the impact of cyber attacks against organizations (e.g., Smith and Rupp 2002). On the other hand, network security articles (e.g., Sun, Yu, and Han 2006) typically approach technical network issues within the engineering sciences using formal techniques and are less concerned about the social context.

In other words, this study's data suggests that the United States' focus on cyber security is indicative of its more diverse coverage in terms of the contributing scholarly domains, while China's main focus on network security accounts for its publications centering on the more formal sciences of engineering and computer science. Researchers (e.g., Clarke and Knake 2010) have pointed out the severe vulnerabilities that cyber threats pose to United States' critical

infrastructure. This vulnerability has led the United States government to encourage research on cyber security and in turn, many diverse scholarly domains have begun contributing research.

The Chinese and American governments likely play a role in promoting their countries becoming top producers of publications on information security. For example, Mohrman (2008) reports on the Emerging Global Model (EGM), a market driven strategy instituted and adapted to higher education and research by the Chinese government. The Chinese government's acceptance of the EGM places multiple pressures on Chinese researchers and academic institutions, namely "increased access, higher research productivity, new expectations for self-funding, and greater autonomy coupled with more government scrutiny and evaluation" (Mohrman 2008, 29). Moreover, research (e.g., Yoshihara 2001) shows that China has been heavily involved with national information security interests for well over a decade. Similarly, United States (2014) government directives clearly specify information security as a central focus for national security. Therefore, it would be very useful for policy makers to look to ascertain and judge their funding strategies, as well as observe the information security research activities of their counterparts in other nations.

In summary, the information security specialty's salient features were shown to include 100 authors that published 30 or more research documents. The highest three contributing authors were Ma, Furnell, and Highland. The specialty's highest contributing source titles were mostly from the United States and led by *Lecture Notes in Computer Science* and *Computers and Security* along with a significant amount of source titles coming from professionals organizations such as *IEEE* and *ACM (e.g., Proceedings of the ACM Conference on Computer and Communications Security*, *IEEE Transactions on Information Forensics and Security*). The most productive author affiliations (e.g., Xidian University, Tsinghau University) were generally

observed as coming from China. In regards to counrty-wise top producers, China and the United States drastically stood out as the most productive. Moreover, the current author observed a variation between these two high contributing countries. The United States had an emphasis on cyber security and produced a significant amount more research documents from the social sciences, while China produced more engineering and computer science publications that focused on network security.

In addition to observing the information security specialty's top producers, a look at the composition of the entire dataset presents a fuller picture of the specialty. The entire dataset included 69,171 contributing authors, which is on average approximately 1.2 documents per author. The top 100 most prolific authors (see Table 6.1) accounted for 4,399 of the documents in the dataset. The full dataset also contained publications from a total of 7,649 different source titles (i.e., 7.7 documents per source title), while the majority of the most prolific source titles (see Figure 6.1) were from the United States and concentrated on engineering and computer science. In total, there were 19,407 various author affiliations (i.e., on average three documents per affiliation) of which most were universities from China and the United States, but some were prominent research centers from private companies (e.g., IBM and Microsoft). The dataset contained a wide range of contributing countries; that is, 138 countries producing on average 427 documents per country. Nevertheless, more than half of the dataset was composed of publications from China and the United States.

6.3 Emergence and Evolution of the Information Security Specialty

The present section moves to the second research question by taking a dynamic and holistic view of the dataset bringing to light the growth of the information security specialty in terms of publication production over time. The entire dataset spans over 41 years with 58,908

information security research records included. Figure 6.4 is partitioned into six distinct periods marked by significant publication activity within the information security specialty.

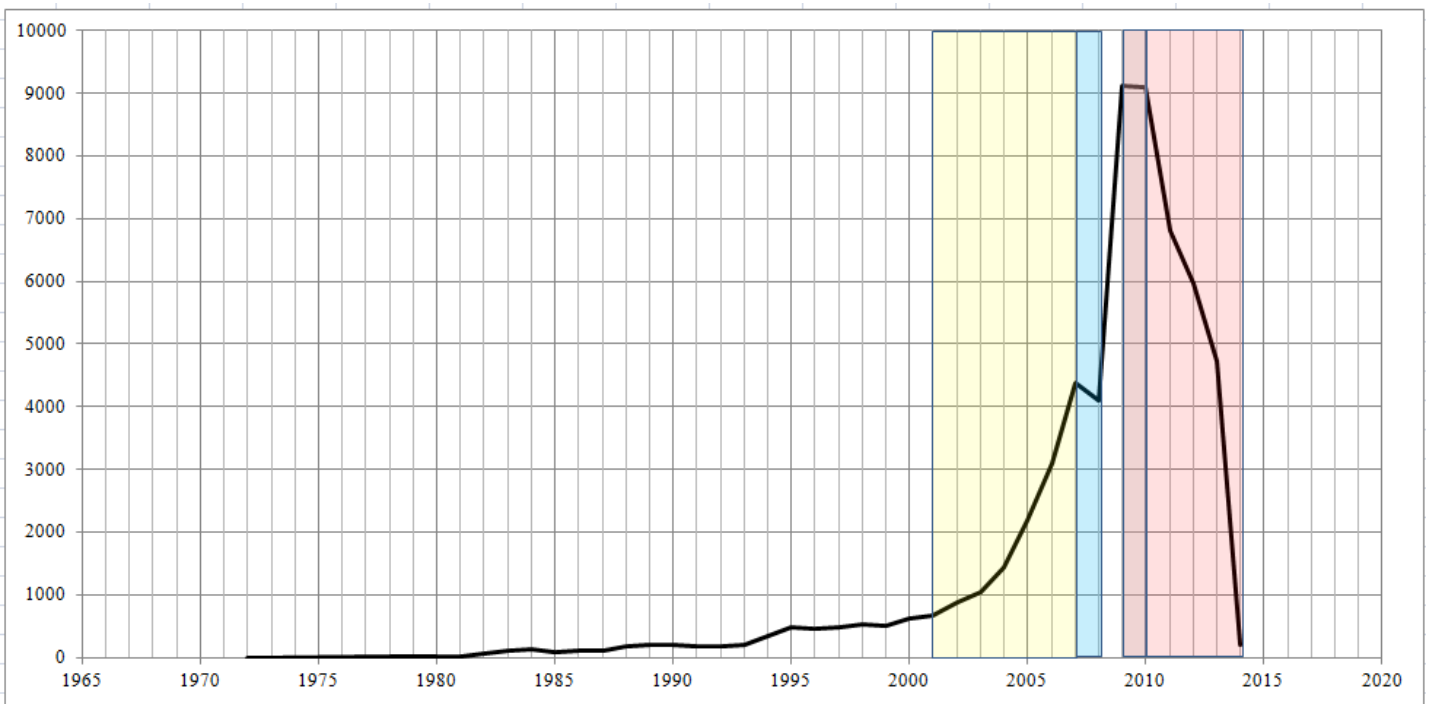


Figure 6.4 Growth of Publications on Information Security

Prior research indicates that the growth of scholarly literature correlates to the change and evolution of a specialty (Cole and Zuckerman 1975; Price 1961; Tabah 1999). The first and longest period under analysis spans from 1972 to 2001 and it is observed slowly growing from a single publication in 1972 to 675 publications by 2001. Research on time-sharing (e.g., Roberts 1986) and multi-user environments (e.g., Anderson 1972) are among the research topics covered in articles published during the 1970s. Publication growth increased slowly during the first few decades of the dataset since computer technology was mainly concentrated in business, government, and academic settings. The second period, 2001 to 2007 marks an exponential climb to 4,384 publications in 2007, an increase of 549%. Personal computers and the Internet became readily available to the public during the 1990s and this drove heavy capital investment,

particularly in the United States' stock market, into the development of new online ventures. One reason for the drastic rise in information security publication productivity during this period (i.e., 2001-2007) was likely macro economic influences; that is, the heavy global financial investment in Internet and computer ventures otherwise known as the Dot-Com Bubble (Kraay and Ventura 2007). Another plausable influence was probably micro economic influences (i.e., internal corporate and government information security R&D investments). The following period (i.e., 2007-2008) reveals a slight drop to 4,107 publications. The sudden drop in publication productivity might be due to the Great Recession, which happened in 2007. Salamon, Geller, and Spence (2009) reported that by 2008 the recession had a pronounced negative impact on all sectors, in specific nonprofits and education sectors that traditionally support research.

Nevertheless, the subsequent period, namely 2008-2009, appears to be the sharpest incline over a single year with a 122% increase to 9,123 publications. The current author has chosen to expand the discussion on the United States and China because together they contributed over 50% of the information security publications in this study's dataset during 2009. Research (e.g., Langevin et al., 2008) indicated that many major cyber attacks occurred against the United States in the years leading up to 2007. Consequently, the United States President, George W. Bush, put forth the Comprehensive National Cybersecurity Initiative (CNCI), which took effect in 2008. The CNCI specifically laid out an initiative directing the coordination and redirection of R&D efforts towards national cybersecurity. Thus, a more detailed look at this study's dataset showed that United State's information security publications rose over 90% from 2008 to 2009.

While the increase in publication productivity was, indeed, very high for the United States during this period, China's publication growth far outpaced even that of the United States.

China's number of information security publications went from 829 documents in 2008 to 2,218 by 2009, a rise of approximately 267%. According to Shao and Shen (2011), China's rise in scholarly publishing during this period is a direct result of economic incentives. Shao and Shen describe China's academic institutions as being paid for publication productivity by a government rating system that started around this period. Yet, the authors go on to point out their concern about the quality of such publications since the primary motivation was economic.

The year between 2009 and 2010 was steady and showed no noteworthy variation. The greatest decline, however, occurred between the years 2010 and 2013 dropping 52% from 9,802 to 4,727 publications. Three out of the four top producing countries (i.e., United States, India, and United Kingdom) showed only a slight drop in publication production, while China accounted for the vast portion of publication decline dropping 46% between 2010 and 2011. Perhaps, China's decline during this period also reflects a high degree of sensitivity to that of the downward shifts in other countries. The trajectory continued to drop into 2014, though it is difficult to draw conclusions based on up-to-date output counts because the data collection for the current study was completed in February 2014.

In a related study, Baskaran (2013) plotted the publication output of research on cryptography. Baskaran observed 180% rise in publication output from 2000 to 2011, while the present study has found that overall information security research, including research on cryptography, rose 986% for the same period.

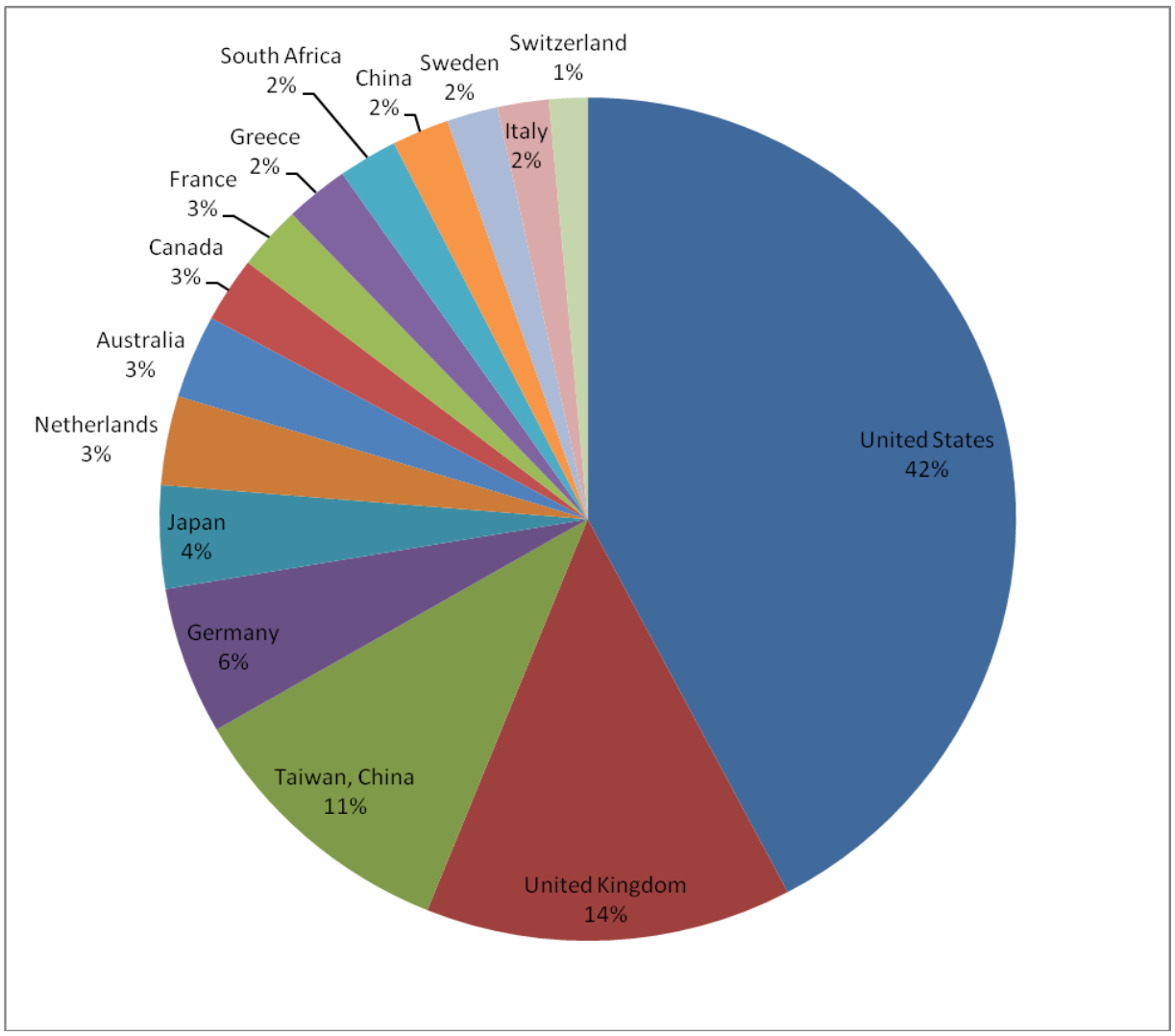


Figure 6.5 Publication Output by Country: 1972-2001

Modern information security had its impetus with the development of computer technology. Nations that were involved with computer technology from early on played a central role in information security publications. The United States and United Kingdom were responsible for the development of the first computers (Leeuw and Bergstra 2007). Conversely, Figure 6.5 indicates that nations not historically involved with the development of computer technology contributed very little to information security research during the early period. One such significant observation is the limited contributions from China (2%). Chu (1991) discussed

the stagnation of Chinese science and technology research during the Cultural Revolution (1966-1976). It was not until political change occurred in China during 1968 that government policies started supporting scientific and technological research, in particular international science and technology research exchange grew during the mid-1980s leading to the drastic growth in scholarly publications.

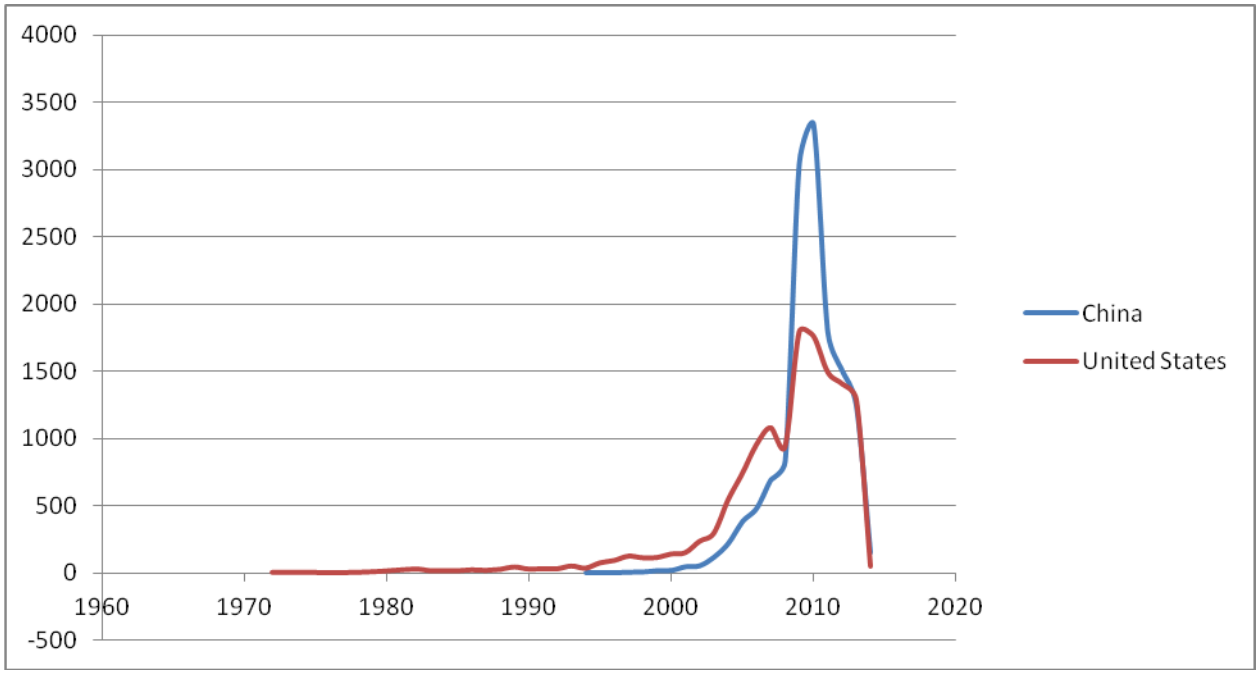


Figure 6.6 1972-2014 China and United States Publication Output Comparison

Figure 6.6 is another illustration comparing China and the United States with regard to information security publications. The United States maintains its overall high-level of information security publication output from its historical involvement (i.e., early 1970s to early 1990s), while China can be observed surging with publication output to a much greater extent than the United States during more recent years (e.g., 2008 to 2010). Furthermore, Figure 6.6 displays a significant drop in publication output post 2010 for both China and the United States. This decline was also observed by Baskaran (2013) with research publications in the specific

topic area of cryptography. The current author was able to attribute the publication slowdown to fewer conference proceedings being published within the dataset during this period. Moreover, article and book publications remained relatively stable, while conference proceedings dropped considerably after 2010. The unstable economic conditions brought on by the Global Recession likely reduced the extent to which institutions were willing to invest in information security conferences leading to fewer conference proceeding publications.

Some researchers have correlated explosive growth in literature to world events. For example, in their study of the contemporary terrorism research specialty, Reid and Chen (2007, 42) concluded:

> The multidisciplinary field of contemporary terrorism is experiencing explosive growth largely driven by the heightened global war against terrorism. This has spawned numerous research communities, new research centers (e.g., UK New Security Challenges Programme and US Department of Homeland Security Centers of Excellence), and increased US Federal Research and Development (R & D) funding.

Although not a primary focus for information security research, the potential for cyber terrorism was a primary factor for the United States to invest in R&D initiatives on cybersecurity (Department of Homeland Security 2009). The period between 2001 and 2007 is filled with other information security events that potentially drove information security publication growth. Some authors (e.g., Glenny 2011) underscore the drastic rise of international cybercrime during this period and others (e.g., Carr 2010) point to an increase in state sponsored operations against public and private computer systems. For example, according to William Lynn (2010), former Deputy Secretary of Defense for the United States, in 2008 the United States Department of Defense was the victim of the largest information security breach to its date. Lynn went on to explain that this incident, termed Operation Buckshot Charlie was the impetus behind the United States government's massive shift towards investing in information security. The timeline for

Operation Buckshot Charlie, adjusting for lag time, can also be observed (see Figure 6.6) correlating to an increase in information security publications for the United States between 2008 and 2010. Furthermore, there appears to be parallel growth trends between China and the United States after 1997, short of a few fluctuations with the United States. Both the fluctuation of the United States between 2007 and 2008 and the drop off in publication output in the entire time period of 1972-2014 are two points that should be followed up by future research. Unfortunately, no research could be found to shed light on these major downward shifts. Yet, it may be the case that information security research output suffered due to the Global Recession of 2009, which has had widespread implications over the last several years.

In a prior classic study on the growth of scientific literature, Menard (1971) examined multiple specialties relating to geology and physics and was able to develop a categorization scheme of publication growth based on three distinct patterns. The first growth pattern was defined by slow growth and it was observed correlating to stable fields that were large and older (e.g., acoustics, optics, invertebrate paleontology, glacial geology). The second pattern, termed growth fields, differentiates from the first as it was underscored by rapid growth and its publication output would double between five and ten years (e.g., solid-state physics, geophysics, paleoecology). The third growth pattern features cyclical fluctuations between peak and trough levels of productivity (e.g., astrogeology, petroleum geology). The information security specialty appears to deviate from all of Menard's patterns. Figure 6.4 indicates that the research output pattern of the information security specialty is best described by long slow growth followed by a steep incline, and a sharp drop.

6.4 Key Contributing Scholarly Domains

The third research question aims to explore what scholarly domains contribute to the information security specialty. Based on prior studies (e.g., Besselaar and Leydesdorff 1996; Leydesdorff and Goldstone 2014) Research Question 3 was approached by focusing on the source titles of the 58,908 records collected for the current study. Figure 6.7 displays the distribution of scholarly domains that publish research literature on information security. The scholarly domains in Figure 6.7 were derived from Scopus' classification of subject areas. However, Scopus assigned some source titles multiple subject areas if they were found to cover more than one. The present author found that many of those subject areas could be aggregated into the main scholarly domains presented in Figure 6.7 giving readers a more manageable view of the information security specialty.

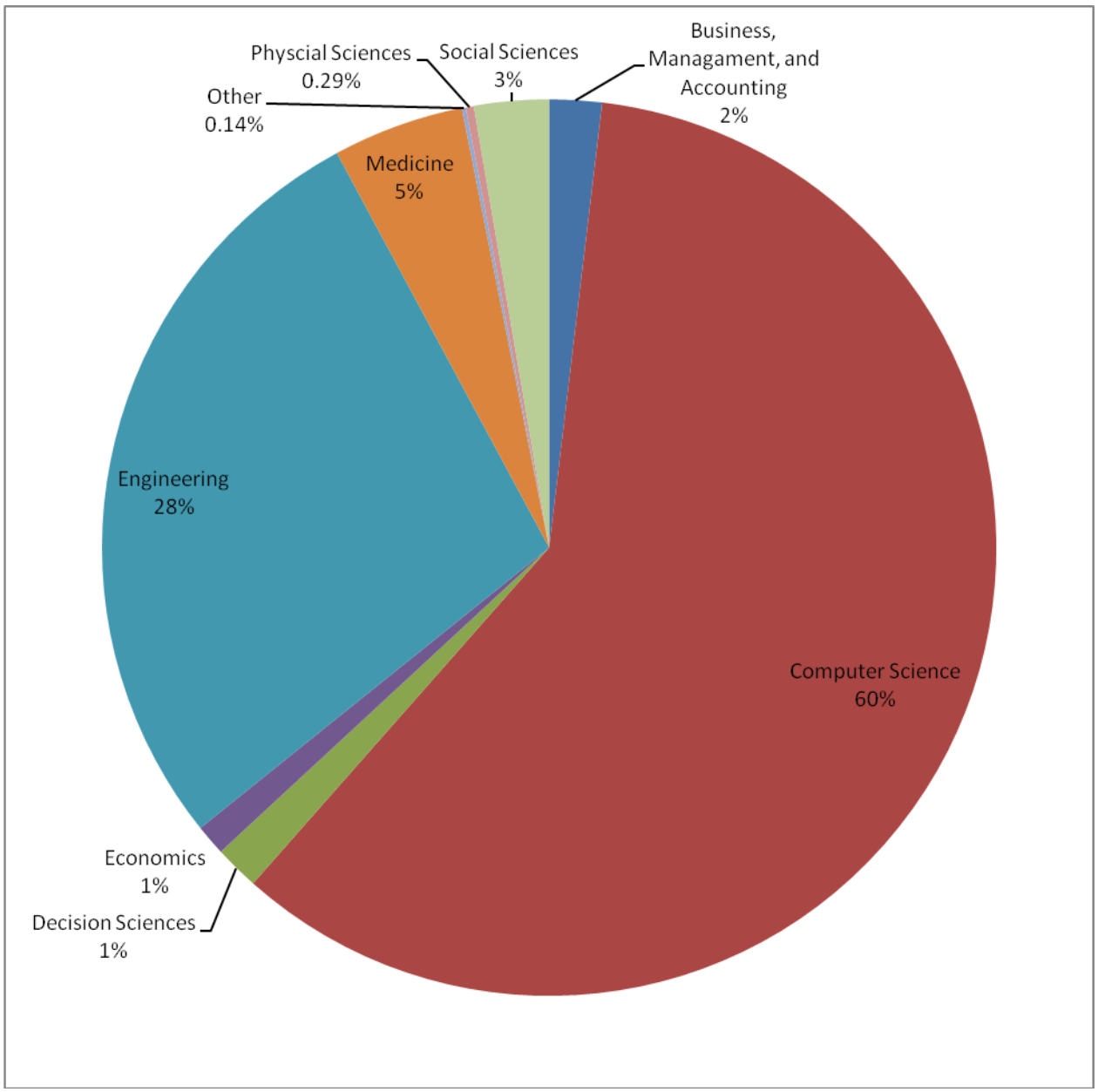


Figure 6.7 Contributing Scholarly Domains at the Source Publication Level

As demonstrated in Figure 6.7, eight scholarly domains contribute research publications to the information security specialty. Computer science is clearly the greatest contributor, while physical sciences (e.g., chemistry, geography) appear to contribute the least. The prominence of computer science as a contributing scholarly domain was expected as information security scholars (e.g., Whiteman and Mattord 2009) had argued that modern information security started

with the advent of the computer. The second highest contributing scholarly domain is engineering. It should be noted that there is a substantial history of engineers in information security research, particularly in communications security and cryptology (e.g., Shannon 1949), merging abstract theory with practical design to solve real-life information security problems.

The small share of business, management, and accounting source titles is unexpected considering organizations with an interest in enterprise systems security have a substantial stake in information security. Likewise, in their content analysis of information security conference papers Botha, Tshepo, and Gaadingwe (2006) were troubled by the imbalance between contributions to information security from technical and nontechnical fields. The authors went on to state: "An inclination to technical aspects of security was apparent. It was also uncovered that there were, in our opinion, some key topics, which received little or no mention in the series such as business continuity and auditing. Such observations are alarming." (255). This finding suggests that research policy managers need to focus their efforts on expanding the influx of research publications from the social sciences and some less technical applied sciences (e.g., business, management, and accounting) if, as Solms (2001) recommended, the information security specialty is to be approached in a "holistic" manner.

The Mitre Corporation (2010) performed a study on behalf of the United States Department of Defense to investigate and develop a framework for a science of security (i.e., a science of cyber-security). The Mitre researchers developed their framework by drawing on various fields, namely economics, meteorology, medicine (in particular immunology), astronomy, and agriculture. Economics has many applicable theories dealing with competing agents (e.g., game theory) that can assist information security researchers making predictions

about threats and adversary behaviors. Researchers at the Mitre Corporation further argued that meteorology presented highly useful models that could forecast patterns of threats.

Moreover, medicine and immunology, as reported by the Mitre Corporation (2010), can lend to information security research in two main ways: First, to use public health based containment models to deal with large outbreaks of computer viruses and other malicious software analogous to the way outbreaks of illnesses (e.g., H1N1) are handled; Second, to study the ways in which biological immune systems defend against attacks by bacteria and viruses. According to researchers at the Mitre Corporation (2010), such knowledge can be transferred into computer security. Astronomy, closely related to physics, provides the tools to observe the large-scale interactions of objects in cyberspace as it does in physical outer space. Lastly, agriculture would bring benefits to information security research in that it routinely uses techniques to protect large amounts of crops from attacks by bad pests (e.g., harmful insects) via biological control (i.e., breading good pests to eliminate the bad pests) leading to a healthy agricultural environment. These same control techniques (i.e., creating good computer programs to seek out and destroy bad computer programs) can be adapted and applied to information security (Mitre Corporation 2010). Figure 6.7 confirms that three of the five fields the Mitre Corporation discussed were contributing scholarly domains while medicine is the most important among the three.

With an extensive literature review, Siponen and Oinas-Kukkonen (2007) found that the main methodologies and techniques applied in information security R&D came from mathematics. There is apparent overlap between computer science and mathematics. Additionally, Siponen and Oinas-Kukkonen's (2007) observations are consistent with what Figure 6.7 presented in that the current author has also noted an overemphasis that information

security specialty placed on technical domains by ignoring contributions from disciplines that involve more qualitative research techniques (e.g., psychology, sociology, semiotics, and philosophy).

Solms (2001, 505) identified 13 dimensions necessary in the information security specialty.

- The strategic/corporate governance dimension
- The governance/organizational dimension
- The best practices dimension
- The ethical dimension
- The certification dimension
- The legal dimension
- The insurance dimension
- The personal/human dimension
- The awareness dimension
- The technical dimension
- The measurement/metrics (compliance monitoring/real time IT audit) dimension
- The audit dimension

Considering the findings of this study, scholarly domains that typically deal with the particular dimensions presented by Solms (2001) appear deficient. Specifically, scholarly domains (e.g., philosophy and law) that are likely to focus on the ethical and legal dimensions of information security did not show up in Figure 6.7. Moreover, scholarly domains that would likely be involved with certification and awareness (e.g., education) are also not seen as significant contributing domains. The reason for this is that traditionally the information security specialty has relied on developing reactionary technical patches to information security threats and vulnerabilities rather than approaching information security from a systemic perspective by strengthening the entire information security system including system users and professional information security practitioners (Solms 2001).

6.5 Intellectual Structure of the Information Security Specialty

Multivariate and network analyses were performed on the co-occurrence data (i.e., co-citations & co-words) to address Research Question 4: What is the intellectual structure of the information security specialty? This dissertation research defines intellectual structure in terms of the topic/subject matter composition of the information security specialty as derived from its bibliometric data. The intellectual structure is an emergent feature of the information security specialty; that is, it is a property of the specialty as a whole rather than merely the sum of its topics. From this perspective, the current author attempts to pull together through analysis and discussion the research topic clusters into a coherent picture of the information security specialty as a whole.

6.5.1 The Information Security Specialty's Intellectual Structure: A Co-Citation perspective

Based on the cluster dendrogram (see Appendix E), the cluster solution was determined to be eight in conjunction with the results from the MDS and factor analysis. Nonetheless, the factor analysis results will not be reported in detail here, since cluster analysis, MDS, and network analysis appeared to be more suitable than factor analysis when the variables under analysis (i.e., highly cited documents and frequently occurring words) carry explicit meaning on their own (Chu 1991). An evaluation of the co-citation data for clustering required that document abstracts, titles, and keywords be closely examined along with the cluster analysis' resulting dendrogram to develop the cluster solution. In relation to the MDS, only the two-dimensional map proved to be interpretable. Kruskal's S-Stress value for the MDS solution was 0.32. The S-Stress value is in line with McCain's (1990b) suggested standard (i.e., greater than 0.2). The R-squared (i.e., the goodness of fit measure) value was 0.65 indicating that the dimensionality had little impact on the mapping solution when changing dimensions.

Clusters represent the intellectual structures that compose the information security specialty. The cluster members were identified by the first author's last name of each highly cited document and the year if one authored more than one document in the top 100 set. The cluster labels were created and based on the examination of the bibliometric data in combination with the aforementioned procedures (e.g., information security literature review, expert consultation, close examination of the 100 most co-cited documents). Compounded labels represent clusters that have seemingly different topics, but share an underlying connection (e.g., methodology, definitions, professional association, overlapping topics). These underlying connections are explained in the discussion of each cluster. Nevertheless, the present research proceeded in line with standard cluster labeling methods by naming labels based on the highest loading documents and/or the most salient topic(s) interpreted directly from cluster documents (McCain1990).

The co-citation relationships of the 100 most cited information security research documents appear to form eight distinct clusters shown in Table 6.5.

Table 6.5 Co-Citation Data Cluster Solution for Information Security

Information Security Management	**Cryptographic Applications to Common Protocols**
Bulgurcu	Abadi2002
Campbell	Armando
Cavusoglu	Blanchet
D'Arcy	Lowe
Dhillon	Meadows
Gordon	Paulson
Herath	Burrows
Straub1998	Needham
Straub1990	Dolev
Intrusion Detection Systems	**Sensor Network Security**
Eskin	Akyildiz2002b
Lee	Chan
Lippmann	Eschenauer
McHugh	Du
Paxson	Liu
Trusted Computing, Virtualization, and Taint Checking	Zhu2003
Klien	Perrig
Lie	Akyildiz2002a
Ristenpart	Zhu2004
Barham	Zhou
Dunlap	**Cryptographic Applications to Privacy and Access Control**
Enck	Cham1985
Newsome	Cham1981
Authentication Techniques and Attack Analysis	Goldreich
Hwang	Rivest
Messerges	Shamir1979
Lamport	Diffe
Lin	Elgamal
Raya	Kobitz
Boneh2001	Menezes
Foster	Denning
Xiong	Sandu
Josang	Ferraiolo
Stoica	Abadi1993
Ammann	Reiter
Sheyner	Yu
Valdes	Avizenis
Gu	**Formal and Theoretical Cryptography**
Stone-Gross	Boneh2005
Jung	Goyal
Dodis	Boneh2003
Halderman	Boneh2004
Chen	Groth
Cox	Waters
Ateniese2006	Boneh2008
Bellare2003b	Goldwasser1984
Jonsson	Rackoff
Steiner	Cramer
Rosenberg	Bellare1993
	Goldwasser1988
	Fiat
	Pointcheval
	Paillier

The subsequent sections present a discussion of each cluster displayed in Table 6.5 with respect to its composition, authors, subject matter, and position within the information security specialty. Due to its large size, only cluster dendrogram excerpts are shown from the full one, which can be found in Appendix E. Moreover, relevant and magnified portions of the network graph are included within the discussion of the clusters when appropriate. The MDS map and full network graph are presented and discussed in section 6.5.1.9 (see Figure 6.16 and Figure 6.17, respectively). Having two vantage points, a view of the whole information security specialty with all its component parts next to each other and another view of each component separated from the whole, gives the current author a greater set of positions by which to draw conclusions.

6.5.1.1 Information Security Management

The cluster analysis dendrogram excerpt displayed in Figure 6.8A identifies the first main cluster of top cited documents. These documents are listed in Table 6.5 and labeled Information Security Management.

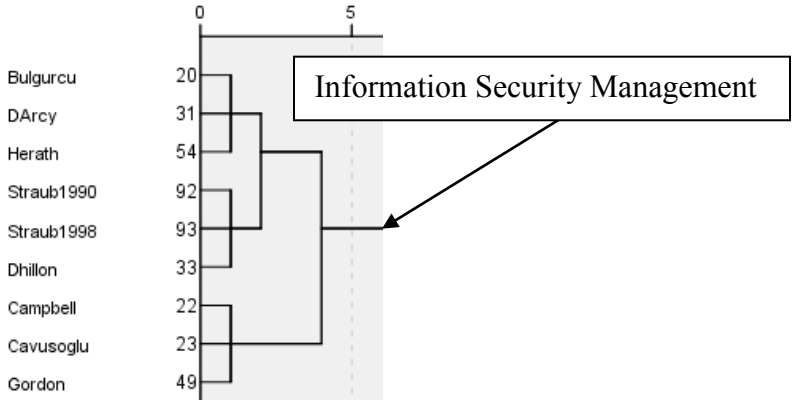


Figure 6.8A Information Security Management: Cluster Dendrogram View

The nine documents that constitute the Information Security Management cluster compose 9% of the top cited 100 documents and their subject matter generally revolves around the socio-organizational perspectives of the general business community. Whitman and Mattord

(2011) explain that information security management plays a vital role in today's business world. Moreover, it aims to keep businesses competitive and facilitate their making a profit by protecting information assets. This is in contrast to the more technically oriented roles that employ an organization's information security strategy via technology. The Information Security Management cluster interacts with the rest of the clusters as its researchers generally focus on orchestrating an overall strategy that includes technology to protect information assets. Information security strategies are typically developed using a variation of the system development life cycle (Whiteman and Mattord 2009).

None of the authors within this cluster appeared among the list of 100 most productive authors (see Table 6.1) suggesting that the information security management topic might be less active compared to the other clusters. Nevertheless, one of the documents (i.e., Straub and Welke 1998) is among the top 15% of the 100 highest cited documents (see Appendix D). The two-dimensional MDS spatial plot of the documents in this cluster reveals their distinct accumulation in the top-right portion of the MDS map (see Figure 6.16) showing their relative isolation from the clusters (i.e., Formal and Theoretical Cryptography, Cryptographic Applications to Privacy and Access Control, and Cryptographic Applications to Common Protocols) that use more formal research techniques. The network graph (see Figure 6.8B) shows these documents coming together in a distinct clique. Moreover, the network graph excerpt (see Figure 6.17) indicates that Information Security Management is one of two tightly-knit regions nested within the larger network graph, again being distinguished from the clusters containing the more technical and formal clusters. Yet, the small size of the Information Security Management cluster is surprising considering the essential role of management for information security. The network graph (see Figure 17) shows that the topic of information security management does, however, have

substantial research interaction with the more formal cluster topics in the graph's center mass (i.e., Cryptographic Applications to Privacy and Access Control, and Cryptographic Applications to Common Protocols).

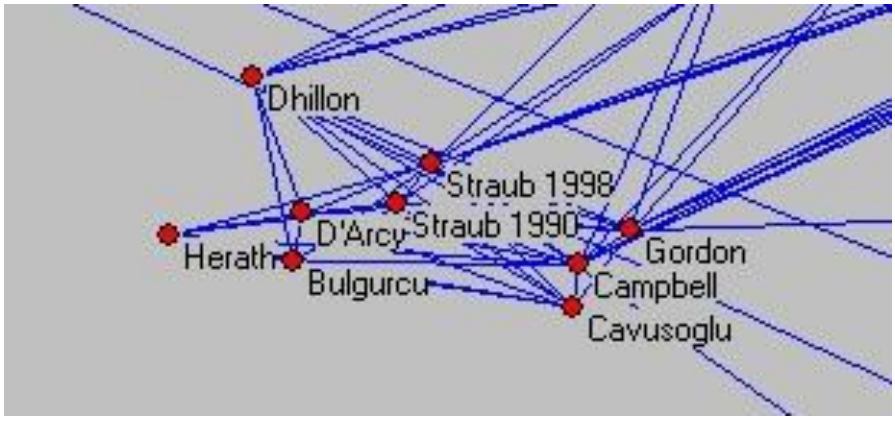


Figure 6.8B Information Security Management: Network Graph Perspective

The Information Security Management cluster can further be divided into three sub-clusters containing three documents each. The first sub-cluster includes Bulgurcu, Cavusoglu, and Benbasat (2010), D'Arcy, Hovav, and Galletta (2009), and Herath and Rao (2009). All of the documents in the first sub-cluster are published in management information systems journals, they were published within a year of one another, and they share a common research focus on system user behavior. In particular, Bulgurcu, Cavusoglu, and Benbasat (2010) investigated the psychological and procedural driving forces behind the security policy compliance of organizational employees. Bulgurcu, Cavusoglu, and Benbasat used the Theory of Planned Behavior, a rational-based approach to explain their findings. D'Arcy, Hovav, and Galletta (2009) similarly studied user behavior in the context of organizational information systems. However, D'Arcy, Hovav, and Galletta centered on the impact that knowledge of security countermeasures had on an employee's intention to misuse the system. In other words, the researchers used General Deterrence Theory to suggest that an employee's knowledge of severe

penalties for system misuse will result in reduced cases of misuse by that employee. Herath and Rao (2009) also contributed to organizational research on policy compliance from a behavioral perspective using similar theories and methods. Specifically, the authors used the Decomposed Theory of Planned Behavior along with an empirical investigation of the organizational commitment of employees to security compliance.

The second sub-cluster is composed of Straub (1990), Straub and Welke (1998), and Dhillon and Blackhouse (2001). The primary commonality among these documents is their aim at studying risk management in information systems security. In line with the previous sub-cluster, these documents are all published in management information systems journals. Straub (1990) and Straub and Welke (1998) both examined organizational risk management with a focus on control strategies (e.g., awareness, investment) by information systems managers. Dhillon and Blackhouse (2001) performed a survey of socio-organizational research in the information systems security field. Moreover, Dhillon and Blackhouse placed significant emphasis on risk management in information systems security.

Similar to the previous two sub-clusters, the third sub-cluster is made up of three documents, namely Campbell, Gordon, Loeb, and Zhou (2003), Cavusoglu, Mishra, and Raghunathan (2004), and Gordon and Loeb (2002). These three articles all placed information security within the sphere of economics. Campbell, Gordon, Loeb, and Zhou (2003) and Cavusoglu, Mishra, and Raghunathan (2004) studied the financial impact, particularly in the stock market, of information security breaches. Gordon and Loeb (2002) also shared the economic perspective with the two previous articles, but tended to weigh the financial impact on companies of decisions to invest in security verses monetary losses from security breaches. Although coming from an economic perspective, Gordon and Loeb aligned with the previous

sub-clusters as it focused on dealing with security by managing the organization through investment.

The Information Security Management cluster can be distinguished from the other clusters with its focus on process oriented techniques and methods. Moreover, it tends to prioritize the balancing of the people, processes, and technology involved with information security as opposed to merely focusing on the technology.

6.5.1.2 Intrusion Detection Systems

The second distinct cluster of top cited documents to be identified is labeled Intrusion Detection Systems. Standard intrusion detection systems (IDS) typically work by searching for known threat signatures; that is, recognized patterns of malicious code or behavior recorded from previously uncovered attacks. This relatively small but tight cluster accounts for only 5% of the top 100 cited documents. One author, (i.e., Lee) who is listed among the top 100 most prolific authors (see Table 6.1), authored one of the documents contained in this cluster (i.e., Lee and Stolfo 2000).

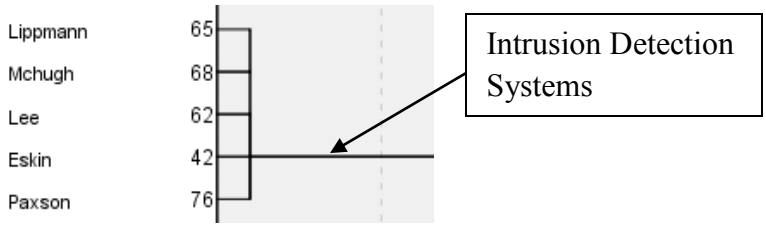


Figure 6.9A Intrusion Detection Systems: Cluster Dendrogram View

In line with the dendrogram excerpt (Figure 6.9A), the MDS map (see Figure 6.16) illustrates the close physical proximity of the Intrusion Detection System cluster documents suggesting each document is of a similar subject matter. Additionally, this cluster appears next to that of the previously discussed cluster (i.e., Information Security Management), which upon a

closer look reveals a subject overlap with regards to employing intrusion detection systems in an information security management scheme.

Likewise, the network graph in Figure 6.11B points to the Intrusion Detection System cluster as a single clique standing apart from a central mass structure. Among its links, the Intrusion Detection Systems clique can be seen connected to Valdes (see Figure 6.17), a document located on the far left side of the graph, another document that was found to deal with intrusion detection systems. Valdes and the two documents that are closely connected to Valdes (i.e., Ammann and Sheyner) are too few to have been considered an independent cluster, yet their topics all revolve around various types of attack analyses techniques. The Intrusion Detection Systems cluster, as well as the three documents it is connected to via Valdes (see Figure 6.17) all participate in research that studies different types of penetration attacks and ways in which to detect such attacks. This makes the topic of attack analysis diverse and far researching.

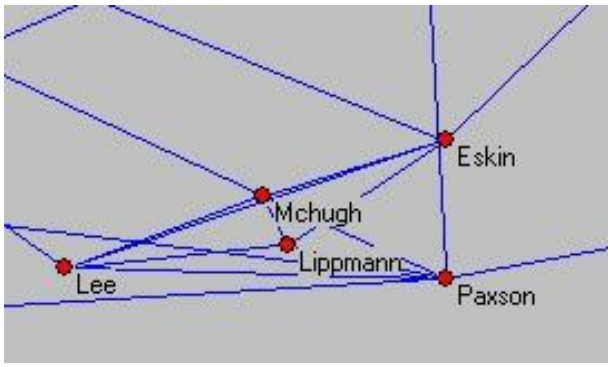


Figure 6.9B Intrusion Detection Systems: Network Graph Perspective

The research presented in Eskin et al. (2002), Lee and Stolfo (2000), and Paxson (1999) all aim to develop models for detecting unauthorized persons or devices roaming a network or computer system. These articles mostly used formal methods that involved logic programming. McHugh (2000) performed a critical review of a major study sponsored by DARPA that was

performed at the Lincoln Laboratory at MIT on intrusion detection systems. McHugh's article identified a number of shortcomings with the MIT study. Lippmann et al. (2000) reported on the development of a test bed for intrusion detection systems. According to Lippmann et al., further research needed to focus on developing detection capabilities for novel types of penetration attacks.

6.5.1.3 Trusted Computing, Virtualization, and Taint Checking

The third cluster (see Figure 6.10A) contains seven of the top cited documents. This cluster combines three topics: trusted computing, virtualization, and taint checking. Trusted computing refers to building security into the computer system itself. It is design oriented as it attempts to develop hardware and software that constrains system behavior in such a way that compromising security violates system design. In line with trusted computing virtualization and taint checking both highlight software design within the context of information security. Many organizations are utilizing the ability of large servers supported by companies leasing out virtual space in their cloud to reduce the overhead costs that comes with investing in one's own computer infrastructure. The technique of virtualization allots space within the cloud to organizations so that only lightweight and less expansive computer infrastructure needs to be acquired. Taint checking, on the other hand, is a software solution to common security threats (e.g., code injection). It is based on tracing and alerting computer software when suspicious web programming variables attempt to behave and interact in a potentially malicious way with other variables (Newsome and Song 2005).

The documents within this cluster include three authors (i.e., Boneh, Mitchell, Song) that appear within the list of the top 100 producing authors (see Table 6.1). Having multiple authors

appear as both high producers and highly cited indicates a fair level of prominence for the topics covered in this cluster.

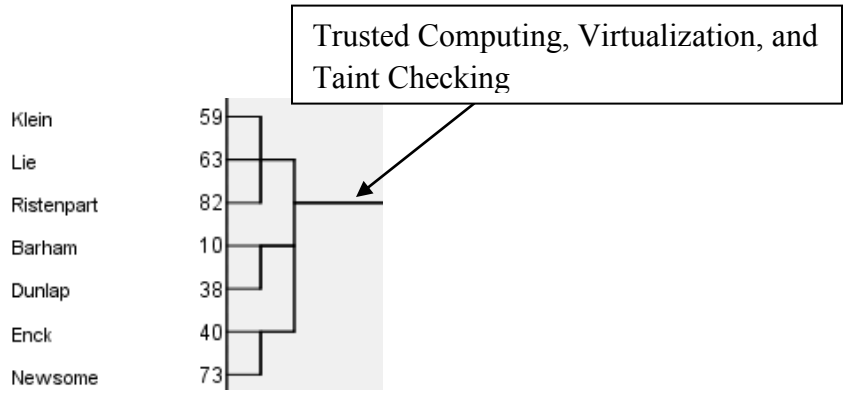


Figure 6.10A Trusted Computing, Virtualization, and Taint Checking: Cluster Dendrogram View

In terms of the MDS map, Figure 6.16 shows this cluster as moderately tight and it can be seen residing in close proximity to the two previous clusters (i.e., Information Security Management and Intrusion Detection Systems). Within the network graph (see Figure 6.17), these three clusters are distinguished from the center mass as they orbit along its periphery. At the same time, the network graph excerpt (see Figure 6.10B), however, illustrates that this cluster is not tightly knit and only has a few links to the central mass of the graph (see Figure 6.17). In particular, Enck et al. (2010) is seen isolated from the rest of the documents except for its sole link to Newsome and Song (2005), another document that studies taint checking. The reason for the isolation of Enck et al. (2010) is likely due to its focus on applying taint checking to the novel area mobile computing security. Considering its relatively new publication date (i.e., Enck et al. 2010), the topic of mobile computing security has not had the time to become a foundational security topic such as cryptography, which has been researched for centuries. Klien et al. (2009) appears pivotal in linking the two pairs of documents Barham et al. (2003), Dunlap et al. (2002), Lie et al. (2000), and Ristenpart et al. (2009), which are connected based on

covering overlapping topics (i.e., software and hardware solutions) and publishing in similar journals (i.e., *Operating Systems Review*).

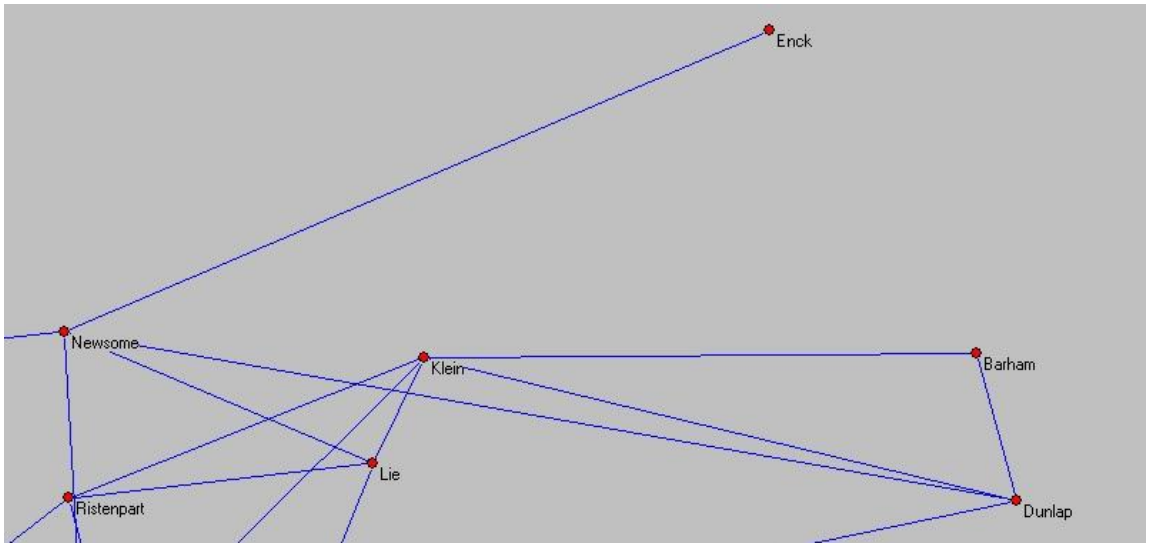


Figure 6.10B Trusted Computing, Virtualization, and Taint Checking: Network Graph Perspective

The Trusted Computing, Virtualization, and Taint Checking cluster can be broken down into three sub-clusters with different research focuses. The first sub-cluster, Klien et al. (2009) and Lie et al. (2000) deals with trusted computing. Klien et al. (2009) reported on the development and design of secure and reliable computer systems by focusing on operating system kernels as the link between hardware and software interaction. Lie et al. (2000) approached trusted computing by creating a processor with a tamper resistant secure architecture. The second sub-cluster includes three of the top cited documents that deal with virtualization. In particular, Ristenpart et al. (2009) investigated the risk that companies face when using virtual machines based in the cloud. The researchers argued that while cloud virtualization allows companies to purchase the exact computing capacity they require, it also leaves them vulnerable to cross-virtual machine attacks from attackers moving laterally within the same cloud. Barham

et al. (2003) presented a secure system that provided virtual machine services in a secure manner. Whereas, Dunlap et al. (2002) illustrated that virtualization can be used to off-set the limitations of system loggers in light of typical limits posed by relying on operating systems to log events during attacks. Enck et al. (2010) and Newsome and Song (2005) approached the use of taint checking in their research. Specifically, Enck et al. (2010) employed taint analysis techniques to provide privacy protection for those that use third party applications on their smart phone. Newsome and Song (2005) presented research on using taint analysis to prevent computer overwrite attacks.

In the larger context of information security, trusted computing, virtualization, and taint checking are hardware and software solutions to information security. They attempt to remove the burden of security from people and place it on system design. Researchers that study the topics within this cluster (i.e., trusted computing) should exchange information with other clusters (i.e., Information Security Management). Information sharing is pivotal especially with technology design in order to establish proper requirement specifications needed to address the security issues that present themselves in real-world situations. Users and organizations are the primary stakeholders in the information security system design process (Whiteman and Mattord 2009). The network graph (see Figure 6.17) seems to suggest that scholarly communication between this cluster and the rest are sparse compared to that of the other clusters (i.e., Formal and Theoretical Cryptography, Cryptographic Applications to Privacy and Access Control, and Cryptographic Applications to Common Protocols, and Sensor Network Security clusters).

6.5.1.4 Authentication Applications and Attack Analysis

The Authentication Applications and Attack Analysis group is the largest cluster being composed of 25 top cited documents. The cluster is formed around research pertaining to

authentication applications and attack analysis. The cluster documents were too dispersed to be outlined within the network map. However, the cluster appears in the center of the MDS map (see Figure 6.16) and spans all four quadrants indicating the diversity of its documents. The cluster analysis dendrogram (see Figure 6.11) reveals it as a higher-level cluster. In other words, the author took a broader vantage point in selecting this cluster of documents.

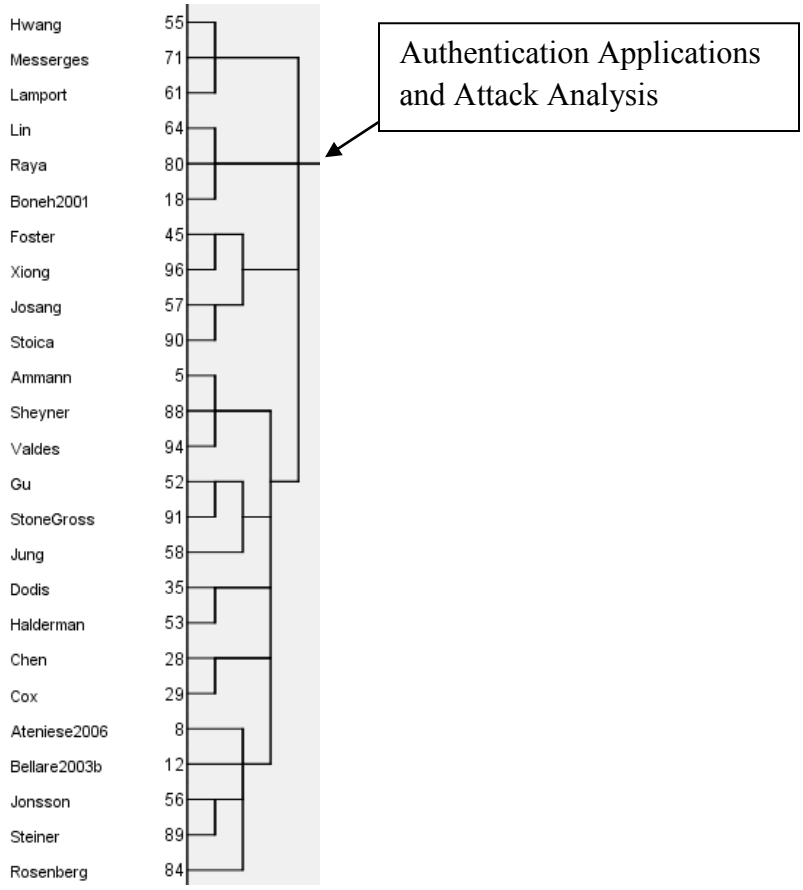


Figure 6.11 Authentication Applications and Attack Analysis: Cluster Dendrogram View

Whiteman and Mattord (2011) describe authenticity as an aspect of information that is of vital importance. To be authenticated means that the information must be real and not fallacious. For example, Whiteman and Mattord illustrate this by referring to a regulatory agency that has been given two differing sets of financial records on a firm under investigation. The regulators

must be able to authenticate which of the two records is legitimate. On the other hand, attack analysis is used by researchers to uncover vulnerabilities within systems by studying previous attacks records and/or orchestrating red team attacks (i.e., mock attacks). There are nine contributing authors (i.e., D. Boneh, J.P. Hubaux, M.S. Hwang, S. Jha, C. Kruegel, D. Pointcheval, X. Shen, G. Tsudik, G. Vigna) to these documents that are listed among the top 100 key authors (see Table 6.1). Though the number of prolific authors is high, the authors' research documents do not have a strong connection to one another. There are seven distinct sub-clusters within the group of 25 documents.

The first sub-cluster is composed of Hwang and Li (2000), Messerges, Dabbish, and Slaon (2002), and Lamport (1981). These top cited documents with authentication applications, for example, Hwang and Li (2000) and Messerges, Dabbish, and Slaon (2002) investigated information security with smart cards, while Lamport (1981) presented a formal scheme for strengthening the use of passwords for user authentication with remote system access. The second sub-cluster centers on applications with identity-based authentication techniques (e.g., Boneh and Franklin 2001) and vehicular ad hoc networks (e.g., Lin et al., 2007; Raya and Hubaux 2007). The third sub-cluster includes five of the top cited documents dealing with security applications for distributed computing systems. Foster, Kesselman, and Tuecke (2001) approached grid computing with an emphasis on security through intergrid protocols. Likewise, Rosenberg et al. (2002) published a seminal report on Internet protocol standards. Xiong and Liu (2004), Josang, Ismail, and Boyd (2007), and Stoica et al. (2007) also approached the construction of distributed system security applications, however, from a peer-to-peer Internet perspective. The fourth sub-cluster deals with network security techniques using graph-based approaches (e.g., Ammann, Wijesekera, and Kaushik 2002; Sheyner et al., 2002) and

probabilistic alert correlation (e.g., Valdes and Skinner 2001). Similarly, Jonsson and Olovsson (1997) appear to contribute to the cluster by proposing an attack model based on a quantitative perspective. While, the fifth sub-cluster is composed of documents (e.g., Gu et al., 2008; Stone-Gross et al., 2009; Jung, Krishnamurthy, and Rabinovich 2002) covering issues with botnets and denial of service attacks. The sixth sub-cluster contains research on applications to strengthen encryption keys for biometrics (e.g., Doidis et al., 2004) and resist cold boot attacks (e.g., Halderman et al., 2004). The seventh sub-cluster is composed of two documents (i.e., Chen and Wornell 2001; Cox et al., 1997) both of which center on investigating the application of watermarking for intellectual property protection. Ateniese et al. (2006), Bellare et al. (2003b), and Steiner, Tsudik, and Waidner (2000) can be placed in an eighth sub-cluster based on a commonly shared formal approach to the application of cryptography in distributed systems. Though diverse in methods all of the documents within this cluster aimed at either studying authentication techniques or different attack scenarios.

6.5.1.5 Cryptographic Applications to Common Protocols

A look at the dendrogram (see Figure 6.12A) suggests that the Cryptographic Applications to Common Protocols cluster is composed of nine documents and two sub-clusters. However, upon closer examination of the documents, there appears to be a single promient shared research topic. All of the nine articles (i.e., Abadi and Rogaway 2002; Armando et al., 2005; Blanchet, Abadi, and Fournet 2005; Lowe 1996; Meadows 1996; Paulson 1998; Burrows, Abadi, and Needham 1989; Needham and Schroeder 1978; Dolev and Yao 1983) reported research addressing the security of common protocals with a particular emphaisis on formal cryptography methods. Protocols enable the proper exchange of information and instructions between computers and often are the target of exploitation by malicious actors. Cryptographic

encryption standards provide a way to protect information exchange over a network via the use of secure protocols (e.g., HTTPS).

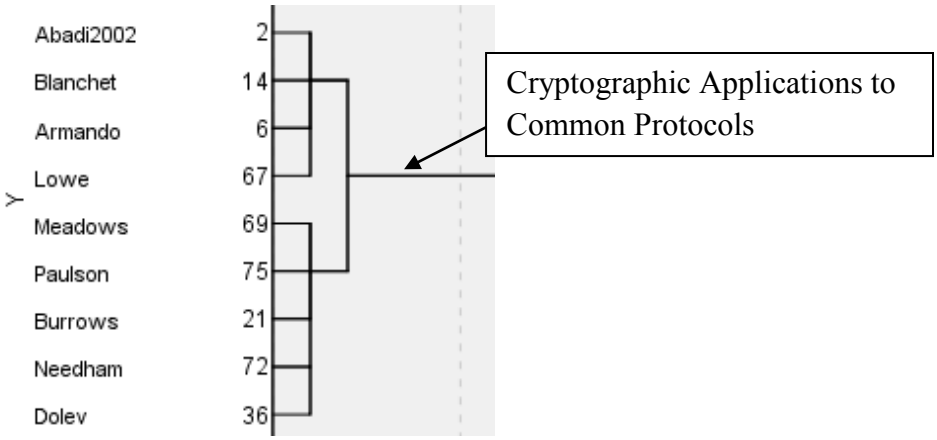


Figure 6.12A Cryptographic Applications to Common Protocols: Cluster Dendrogram View

The current author found it surprising that only one author (i.e., D. Basin) from Armando et al. (2005) is among the 100 top producing authors (see Table 6.1) considering the substantial role played by cryptography and protocols in information security literature. The MDS map in Figure 6.16 displays this cluster as amassed in the bottom-right portion of the MDS map intertwining with the Sensor Network Security cluster. Their closeness reflects the heavy involvement of cryptographic techniques and protocols in securing distributed networks, particularly the vulnerable sensor networks.

Furthermore, the network graph in Figure 6.12B also identifes this cluster as a tight-knit clique located among the central mass of top cited documents, which indicates that its documents are highly connected to the other clusters that have a central interest in cryptography (i.e., Formal and Theoretical Cryptography and Cryptographic Applications to Privacy and Access Control).

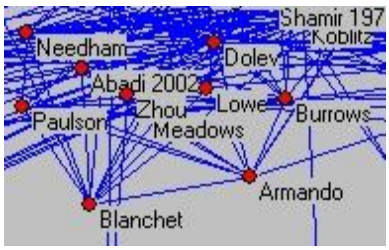


Figure 6.12B Cryptographic Applications to Common Protocols: Network Graph Perspective

The current researcher took a more detailed look at the present cluster and found that many of the authors (e.g. Abadi, Blanchet, Meadows, Dolev) coauthored information security research publications with the other authors within the cluster. Such close interaction between these has produced a cornerstone for the information security specialty. Furthermore, the documents were also found to range in publication year from 1978 to 2008 showing consistency with the research topic (i.e., cryptographic applications to common protocols).

6.5.1.6 Sensor Network Security

The next cluster consists of 10 top cited documents (see Figure 6.13A) and the dendrogram displays a relatively uniform cluster of documents labeled Sensor Network Security. Two documents in this cluster are among the top ten highest cited documents (see Appendix B) while four authors of the documents (i.e., S. Jajodia, P. Ning, A. Perrig, D. Song) in the present cluster are listed among the 100 most productive authors (see Table 6.1). These two indicators underscore the high activity and attention that the topic of sensor network security is getting as of late. Sensor networks are distributed networks that mostly use wireless technology to communicate information about the envionrment from dispersed nodes to a central command and control center. Its applications include military use (e.g., remote intelleigence gathering in combat zones), civilian law enforcemnt (e.g., street cameras), and geology (e.g., seismic activity recorders).

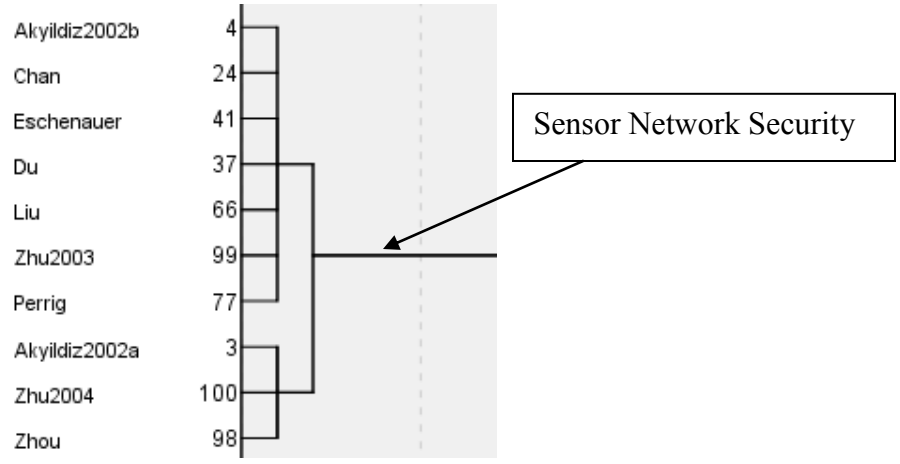


Figure 6.13A Sensor Network Security: Cluster Dendrogram View

According to the MDS map (see Figure 6.16), the Sensor Network Security cluster appears spatially close and overlaps with the Cryptographic Applications to Common Protocals and Cryptographic Applications to Privacy and Access Control clusters. This confrims that in many cases the topic cryptography is strongly related to network security. The network graph in Figure 6.13B shows the Sensor Network cluster as a moderately dense reigon on the perimiter of the graph's center mass. The network graph (see 6.17) highlights the present cluster as also being highly connected to the other clusters that make up the graph's middle portion (i.e., Cryptographic Applications to Common Protocols, Cryptographic Applications to Privacy and Access Control, and Formal and Theoretical Cryptography).

Figure 6.13B Sensor Network Security: Network Graph Perspective

Unlike many of the other clusters (e.g., Authentication Applications and Attack Analysis), all of the documents in the present cluster put forth research soley on the topic of

sensor networks. This suggests strong cohession for the authors and the subject matter. In particular, Akyildiz et al. (2002b) laid out a basic discussion of the concepts involved with sensor networks. Akyildiz, Su, and Sankarasubramaniam (2002a) and Zhou and Hass (1999) surveyed issues related to the broad range of sensor network applications (e.g., military, transportation, health). From another perspective, Chan, Perrig, and Song (2003), Eschenauer and Gligor (2002), Du et al. (2005), and Liu, Ning, and Li (2005) approached the issue of encryption key management in sensor networks. While, Perrig (2002) and Zhu, Setia, and Jajodia (2003) investigated secure protocols for sensor networks. Zhu et al. (2004) proposed three authentication techniques for military sensor network applications.

6.5.1.7 Cryptographic Applications to Privacy and Access Control

Sixteen top cited documents make up the Cryptographic Applications to Privacy and Access Control cluster. This cluster is further composed of two sub-clusters (see Figure 6.14A). Four of the documents in the present cluster (i.e., Deffie and Hellman 1976; Menezes, Oorschot, and Vanstone 1996; Rivest, Shamir, and Adleman 1978; Shamir 1979) are among the top five most cited documents in the overall dataset (Appendix B). Three of the four documents (i.e., Deffie and Hellman 1976; Rivest, Shamir, and Adleman 1978; Shamir 1979) are classic cryptography articles that advanced the concept of public key encryption. The fourth document (i.e., Menezes, Oorschot, and Vanstone 1996) is a heavily used textbook covering the full range cryptography with an emphasis on public key systems. The central location of these four documents in the network graph in Figure 6.17 underscores their pivotal role in the information security specialty. Moreover, two of the documents in this cluster (i.e., Reiter and Rubin 1998; Sandhu et al., 1996) contain authors (e.g., M.K. Reiter and R. Sandhu) that are among the top 100 key authors in terms of productivity. Nevertheless, it should be noted that the authors of the

top three cited documents (see Appendix B) are not among the highest 100 producing (see Table 6.1) indicating that productivity does not always imply an author is highly cited.

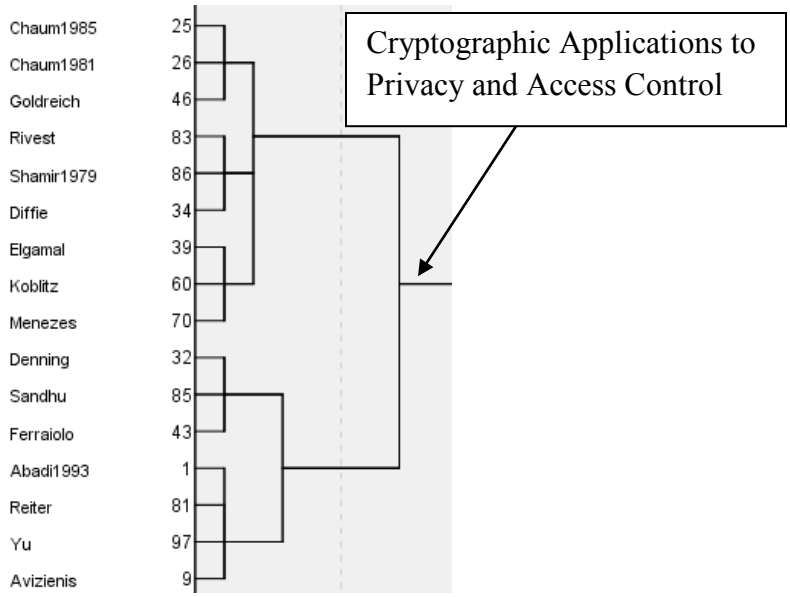


Figure 6.14A Cryptographic Applications to Privacy and Access Control: Cluster Dendrogram View

The MDS view displayed in Figure 6.16 reveals that the Cryptographic Applications to Privacy and Access Control cluster spans across the bottom half of the map illustrating that cryptography has broad coverage in the information security specialty. One of the sub-clusters can be spatially distinguished from the other as it sits somewhat isolated in the bottom left quarter of the map, yet the authors among this portion (e.g., Chaum, Deffie, Rivest) of the subcluster are highly regarded classic researchers. Perhaps, their isolation is because their classic documents tend to be older. The other sub-cluster overlaps with the two previous clusters, namely Cryptographic Applications to Common Protocols and Sensor Network Security.

The network perspective (see Figure 6.17) suggests that the current cluster makes up the majorty of the network's central mass and is highly integrated with the other clusters, in

particular the two previous clusters (i.e., Cryptographic Applications to Common Protocols and Sensor Network Security). Its central position means that the Cryptographic Applications to Privacy and Access Control cluster is the most important component of the information security specialty, since it acts as a junction point pulling together the majority of the specialty's substructures.

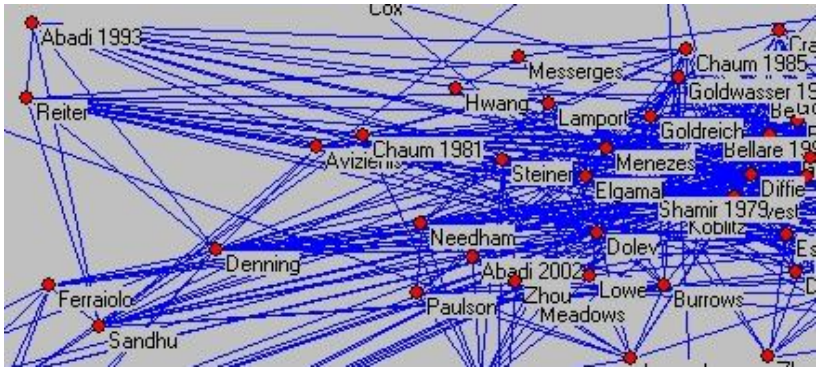


Figure 6.14B Cryptographic Applications to Privacy and Access Control: Network Graph Perspective

The two sub-clusters that make up the present cluster were examined and it became obvious that one sub-cluster primarily dealt with crypotographic applications to privacy while the other covered issues of access control. Except for Avizienis et al. (2004), both sub-clusters mainly present research of a formal mathematical nature.

The documents by Chaum (1985; 1981) approached private email communication and intersected with Goldreich, Micali, and Wigderson (1991) in terms of cryptographic techniques. Avizienis et al. (2004) supplied a process oriented reference paper establishing clear definitions for dependable and secure computing. As mentioned earlier, Shamir (1979) and Deffie and Hellman (1976) provided cryptography researchers with foundational techniques in formal theory (e.g., Deffie and Hellman 1976) and further researchers in this cluster (e.g., Rivest, Shamir, and Adleman 1978) provided practical application. The second sub-cluster nested within

the main cluster is constructed of documents that study access control. Specifically, Sandhu et al. (1996) and Ferraiolo et al. (2001) presented role-based models. Yu, Winslett, and Seamons (2003) introduced a model based on automated trust negotiation and Reiter and Rubin (1998) looked to protect privacy on the Web by embedding Internet users into a crowd that performs Internet searches for them making them anonymous.

6.5.1.8 Formal and Theoretical Cryptography

The second largest cluster (i.e., Formal and Theoretical Cryptography) includes 19 of the top cited documents and it should be noted that most of its documents (e.g., Bellare, Micciancio, and Warinschi 2003a) are published in sources that primarily focus on formal research in cryptology (e.g., *Advances in Cryptology—Eurocrypt*). Thus far, the two large clusters Cryptographic Applications to Privacy, Access Control and Formal and Theoretical Cryptography, and Cryptographic Applications to Common Protocols account for 40% of the co-cited dataset underscoring the significant position of cryptography as a research topic in the information security specialty. The clustering of the six highly cited documents (i.e., Bellare and Rogaway 1993; Boneh, Boyen, and Shacham 2005; Goldwasser and Micali 1984; Goldwasser, Micali, Rivest 1988; Pointcheval and Stern 2000; Waters 2005) is demonstrated with the dendrogram (see Figure 6.15A). These six documents are among the top 15 highest cited documents in the overall dataset underlining their stature in the information security literature corpus. Three of the authors among the documents (i.e., Boneh, Camenisch, and Waters) also appear on the list of top 100 publishing authors (see Table 6.1). This low number of key authors is surprising considering that this cluster contains the second highest number of top cited documents, further evidence that productivity and citedness do not always go hand-in-hand.

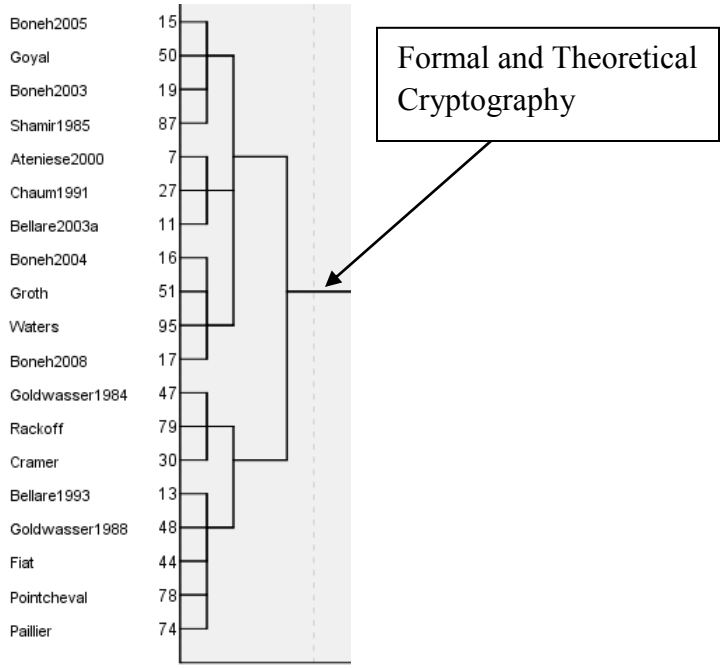


Figure 6.15A Formal and Theoretical Cryptography: Cluster Dendrogram View

The MDS map in Figure 6.16 displays this cluster as mostly located in the top left quarter of the MDS map distinguishing its subject matter from that of the other clusters. Unlike the other clusters, there seems to be no spatial overlap with the rest of the clusters. Yet, the entire left portion of the MDS map, including the current cluster, appears to contain the majority of research that deals with a highly formal (i.e., mathematical) technquies.

The network graph in Figure 6.17 highlights the Formal and Theoretical Cryptography cluster located slightly off center. It appears to be the most dense region (see Figure 6.15B). What is more, this cluster has the greatest amount of connections in the graph, predominantly with Cryptographic Applications to Privacy and Access Control. Together, these two clusters make up the central hub of the graph underlining the prominent role of their intersecting subject matter (i.e., cryptography).

Figure 6.15B Formal and Theoretical Cryptography: Network Graph Perspective

The most prominent sub-cluster within this cluster consist of 11 documents that focus directly on the topic of formal proofs for digital signatures (i.e., Ateniese 2000; Bellare, Micciancio, and Warinschi 2003; Boneh et al., 2003; Boneh and Boyen 2008; Chaum 1991; Boneh, Boyen, and Shacham 2004; Fiat and Shamir 1987; Goldwasser, Micali, and Rivest 1988; Pointcheval and Stern 2000; Shamir 1985; Waters 2005). The remaining documents deal with broader problems of encryption, mostly formal research on public key encryption schemes (e.g., Bellare and Rogaway 1993; Boneh, Boyen, and Goh 2005; Cramer and Shoup 2003; Fiat and Shamir 1987; Goyal et al., 2006; Grot and Sahai 2008; Paillier 1999; Rackoff and Simon 1992). Goldwasser and Micali (1984) contributed to the present cluster from a slightly different perspective by examining and developing an alternative to public key encryption via complexity theory.

6.5.1.9 Information Security Specialty's Intellectual Structure: Co-Citation Analysis Summary

The current author will now move the discussion focus to the entire co-citation perspective, including all clusters. The MDS map (see Figure 6.16) and the network graph (see 16.7) present two very different views of the information security specialty. The MDS map shows the clusters as accumulating around the outskirts of the map with a gaping hole in the center. The lone document maintaining a position in the center is Stoica, illustrating its isolation in terms of topic. This shape is also indicative of a diverse set of subject matter interests that

have enough variation to stand spatially apart. Moreover, the partition between MDS Dimension 1 and Dimension 2 establish the entire left two quarters as containing the more classic literature on cryptography, while the bottom right quarter is concentrated on newer applications of cryptography in the area of distributed network security. Thus, three quarters of the MDS map appear to enclose documents that in some way include cryptographic research. The remaining portion in the top right quarter, on the other hand, mostly deals with process-oriented research that centers on information security management or the development and design of information security technology. Consequently, Dimension 1 reflects document/cluster relevance to Social Oriented research topics, whereas Dimension 2 corresponds to Technical Oriented research topics.

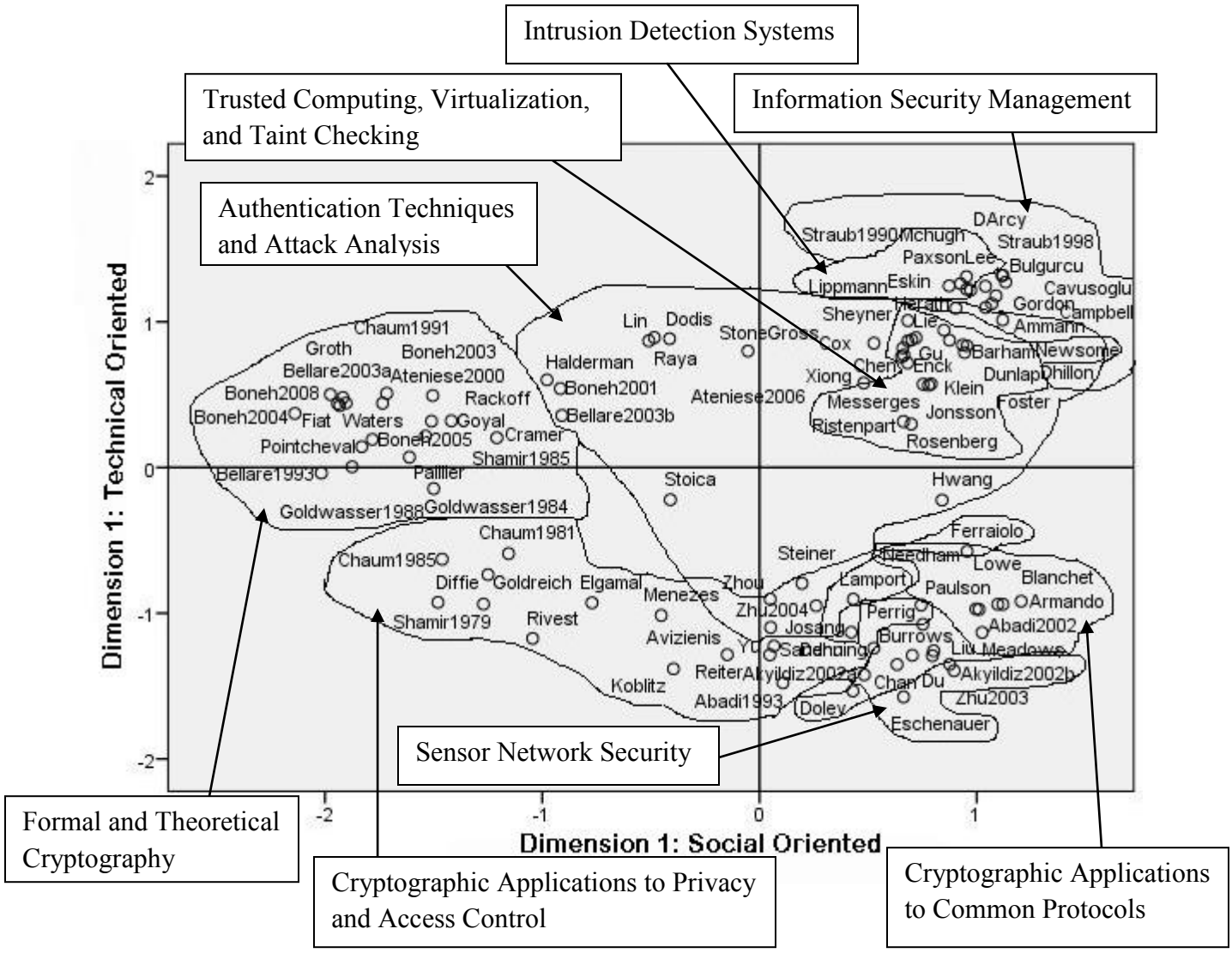


Figure 6.16 Information Security Specialty: MDS Map View

The view of the network graph (see Figure 6.17) is very different from that of the MDS map. The center of the network graph is filled with a densly packed mix of four clusters: three dealing with cryptography (i.e., Cryptogrpahic Applications to Privacy and Access Control, Cryptogrpahic Applications to Common Protocols, and Formal and Theoretcial Cryptography) and one centered on Sensor Network Security. The center mass indicates that the documents within the four constituent clusters are highly linked together and, therefore, constitute the base of the information security specialty. The classic literature within the center mass (e.g.,

Chaum1981, Chaum 1985, Diffie, Riverst, Shamir1979) are among the highest cited docuemnts in the entire dataset and have long been considered the basis for modern cryptography. This is not unexpected considering information security research from early on to modern times has heavily revolved around cryptology (see Appendix A). Nevertheless, the information managemnt school of thought is also clearly positioned in the network graph (see Figure 6.17) as a counter wieght to the more formal domain of cryptology.

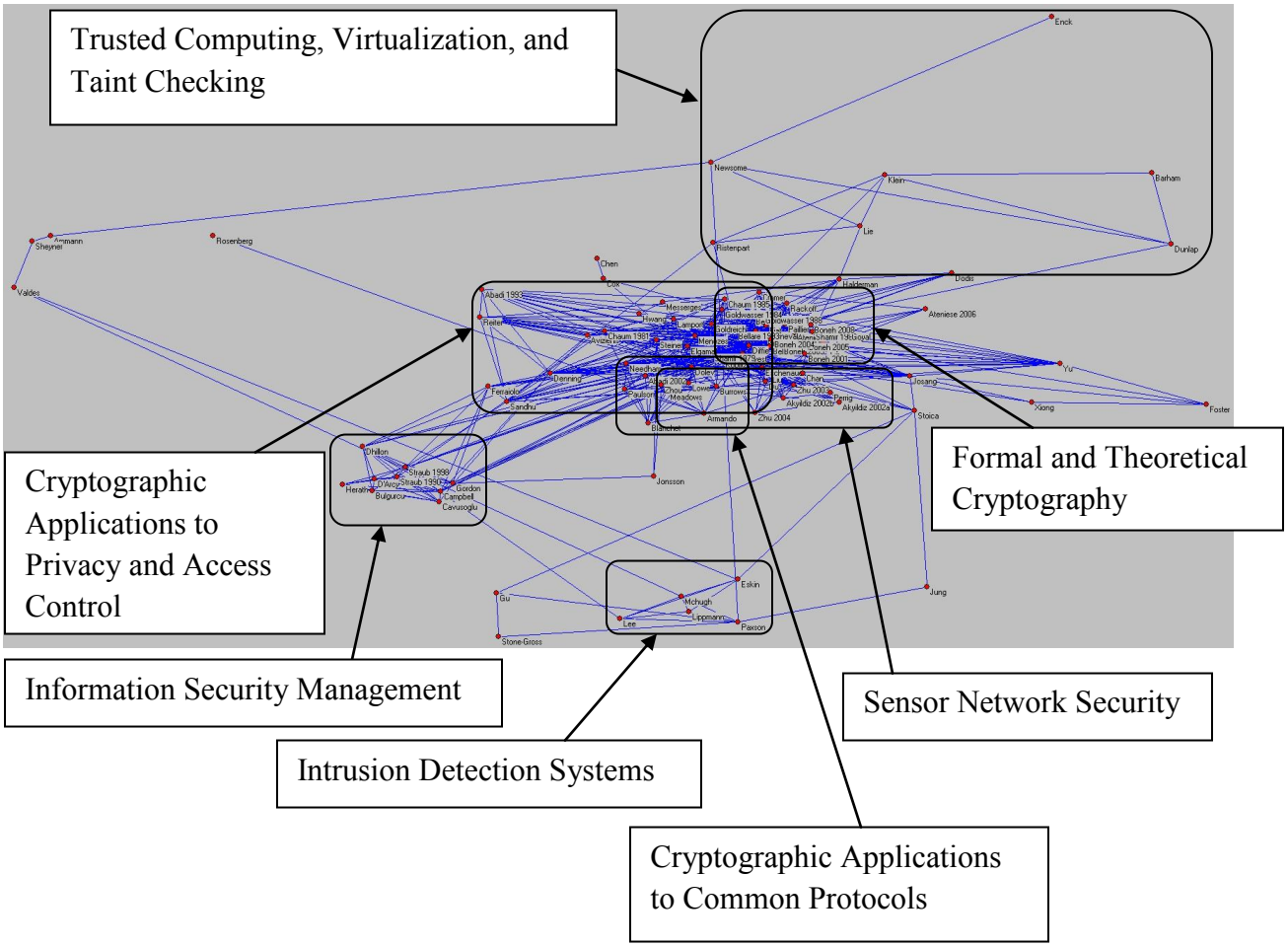


Figure 6.17 Information Security Specialty: Network Graph Perspective

Consequently, the present author can state that the information security specialty maintains two dominant groups: 1) the formal methods school of thought that primarly focuses on crytpography and 2) the process oriented school of thought that tends towards research on

management and organizational issues. In additon, it should be pointed out that there are some peripheral topics that are less promient with reagrd to their overall influence on the specialty as a whole, yet they show up as clear clusters (i.e., Intrusion Detection Systems and Trusted Computing, Virtualization, and Taint Checking). The MDS map suggests that these two areas gravitate towards the process oriented school of thought.

6.5.2 The Information Security Specialty's Intellectual Structure: A Co-Word Perspective

The present section discusses the results of the co-word analysis. As stated before, the co-word analysis is a secondary technique used to complement the co-citation analysis in guiding the discovery of the information security specialty's intellectual structure. Moreover, not all of the co-word results from the multivariate techniques are presented, but only those that the author found shed further light on the co-citation analysis results. In particular, the current research primarily focuses on the co-word network map (see 6.18A) because it was found to have the greatest explanatory power. Clusters were mainly established through examination of the network graph considering the extent to which the highest 100 frequently used words co-occurred throughout the entire dataset and the sematic relationship between the words. In other words, the more times two words were used together within a document the closer the words appear in proximity to one another. The current author interpreted a cluster as a group of words appearing physically close to one another and sharing some discernible semantic commonality. The present author used information security research literature (e.g., Cooper et al., 2010b; Whitman and Mattord 2011, 2012) and the IEEE Taxonomy (2013) and Thesauri (2013) for examining the semantic nature of the words. Furthermore, the frequencies of each word (see Appendix C) suggested the level of its importance in each cluster and that of the cluster to the information security specialty.

In regards to the co-word MDS solution, Kruskal's S-Stress value for the MDS solution was 0.15. The R-squared (i.e., the goodness of fit measure) value was 0.95. The analysis produced four co-word clusters, mostly gleaned from the network analysis, represented by their labels in Table 6.6 and further illustrated and discussed with regard to the MDS analysis.

Table 6.6 Co-Word Data Cluster Solution

Cryptographic Applications to Computer Network Security	**Education and Awareness**
Access control	Education
Applications	Learning
Architecture	Students
Attack	Training
Authentication	**Industrial Applications**
Bandwidth	Cloud
Communications	Cyber
Computer Crime	Electronic Commerce
Computer Science	Enterprise
Cryptography	Grid
Design	Infrastructure
Encryption	Integration
Environment	Malware
Internet	Monitoring
Internet Protocols	Platform
Intrusion	Servers
Detection	Smart
Key	Strategies
Malicious	Trust
Management	**Medical Records Privacy**
Methodology	Anonymity
Mobile	Computer Security
Public Key Cryptography	Confidentiality
Requirement	Cyber Security
Surveillance	Systems
Topology	Humans
Web	Information Security
Wireless	Information Systems
Wireless Telecommunications Systems	Information Technology
	Management
	Medical Records
	Privacy
	RFID
	Software
	Standards
	United States

Figure 6.18A presents the co-word data from a network graph perspective. A visual inspection uncovers the four clusters. The most significant cluster (e.g., Cryptographic Applications to Computer Network Security) shares a stark similarity with the school of thought derived from the co-citation analysis.

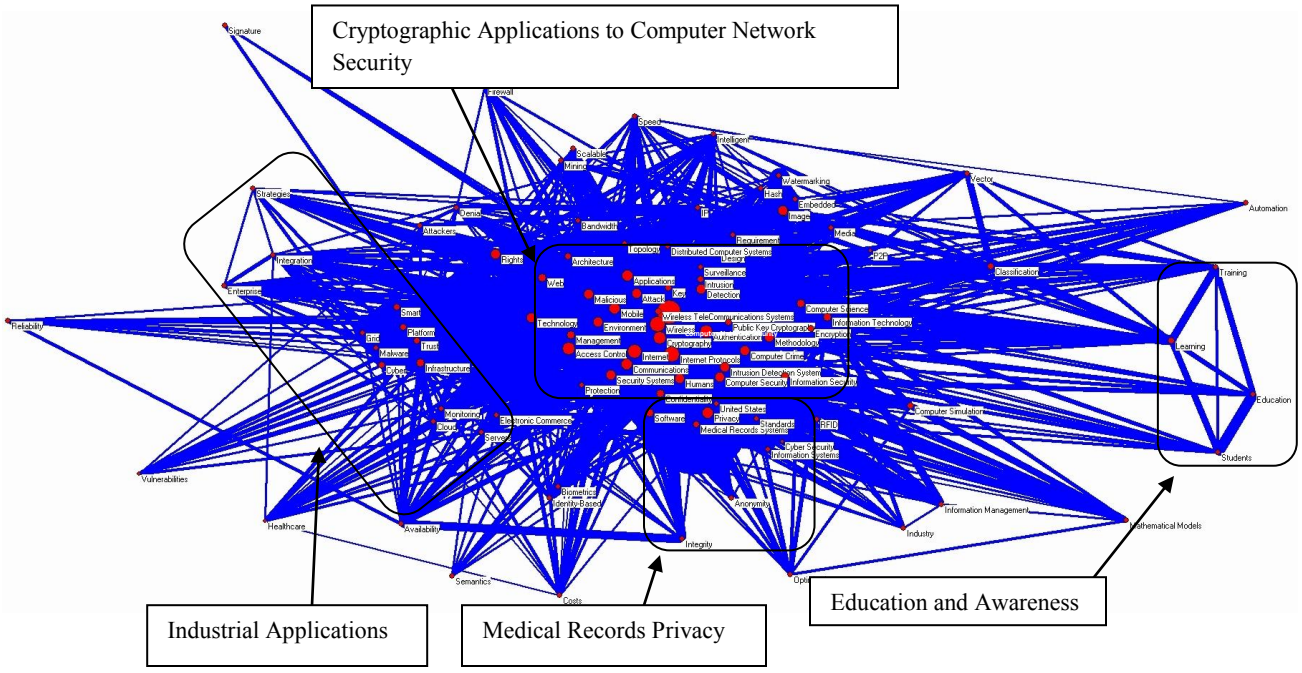


Figure 6.18A Information Security: Network Graph of Co-Word Data

The accumulation of words in the network graph's central mass clearly indicates that there is a heavy research focus in the information security specialty on protecting computer networks via cryptographic applications. It should be noted that the term Computer Network Security appears directly at the center of the network graph and it is the most frequently used word (i.e., 27,279 times) in the entire dataset. The term Computer Network Security is used 100% more than that of the second highest word among the top 100 most frequently used words (e.g., Wireless - 12,027 times), another network related word, and approximately 23 times more than the least frequently used word on the list (e.g., Firewall - 1,187 times). Similarly, the word

Cryptography can be seen in Figure 6.16 positioned close to the center and next to Computer Network Security, suggesting that the two words have significant overlap within the dataset. Cryptography, similar to Computer Network Security, is among the top five most frequently used words in the dataset (i.e., Cryptography - 8,800). Indeed, the IEEE Thesauri suggests that these two terms fall within the sphere of the broader term Communication Security. The current researcher chose to use the terms themselves to represent the cluster, since this represents the cluster more directly. Network security stands out as a common theme among the words presented in the Cryptographic Applications to Computer Network Security cluster. Furthermore, over half of the most frequently used words are included in this cluster suggesting that cryptographic applications and network security are major research topics in the information security specialty.

The Medical Records Privacy cluster, located along the bottom portion of the network graph in Figure 6.18A, contains the word Privacy, which is among the top 10% most frequently occurring words. The word Privacy's close proximity to the terms Medical Records Systems, United States, and Standards suggests that this cluster represents information security research that focuses on the medical records systems within the United States. In addition, the significant use of the word Privacy within the dataset (i.e., 6,128 times) and its close proximity to the term United States and medical records likely points to an emphasis by researchers on issues of privacy rights regarding United States medical records systems. United States legislation has provided legal standards such as the Health Insurance Portability and Accountability Act (HIPPA) by which medical information must be secured. The movement of United State's federal policy in this direction, such as HIPPA, likely led to this research focus.

The Industrial Applications cluster is located along the left perimeter of the network graph in Figure 6.18A. The combination of words within this cluster (e.g., Smart, Grid, Infrastructure, Enterprise, Platform, Malware, Cyber) seems to relate to the protection of larger critical infrastructure type industrial systems. According to Solms and Niekerk (2013), Cyber Security can be distinguished from the broader domain of information security in its emphasis on the protection of society via the protection of its computer systems. Hence, the word Cyber is observed in close proximal relation to the words Infrastructure, Smart, and Grid. Furthermore, the presence of the words Cloud, Electronic Commerce, and Enterprise underscore this cluster's focus on information security applications to industry. Many major institutions, particularly enterprise and electronic commerce, are moving to the cloud for cost savings and computer efficiency.

The Education and Awareness cluster (see Figure 6.18A) displays a clear focus on an area of research argued by information security researchers (e.g., Bradley and Wijekumar 2004; Cooper et al., 2010b) to be central to the information security specialty. Though the number of words are fewer in this cluster (e.g., Training, Learning, Education, Students), their semantic relatedness is clear. It is interesting to note their distinct isolation from the center mass of the network graph. This cluster is less integrated than the rest of the clusters indicating that education and awareness research is segregated from the central topics in the information security specialty.

Figure 6.18B displays the MDS map in which the four clusters from the network graph are laid out spatially. Although the clusterd are not as tightly knit, details about them beyond the network graph are revealed within the MDS map. For example, the Medical Records Privacy cluster is clearly shown as an accumulated group high on both Dimension 1 and Dimension 2.

The Education and Awareness cluster overlies other words such as Methodology and Classification. The Industrial Applications cluster, displayed mostly low on both Dimension 1 and Dimension 2, can be observed slightly overlapping the line into the top left quarter. The entire bottom half (i.e., low on Dimension 2) of the MDS map contains the Industrial Applications, Education and Awareness, and Medical Records Privacy clusters distinguishing it from the top half (i.e., high on Dimension 2) of the map that primarily includes the Cryptographic Applications to Computer Network Security.

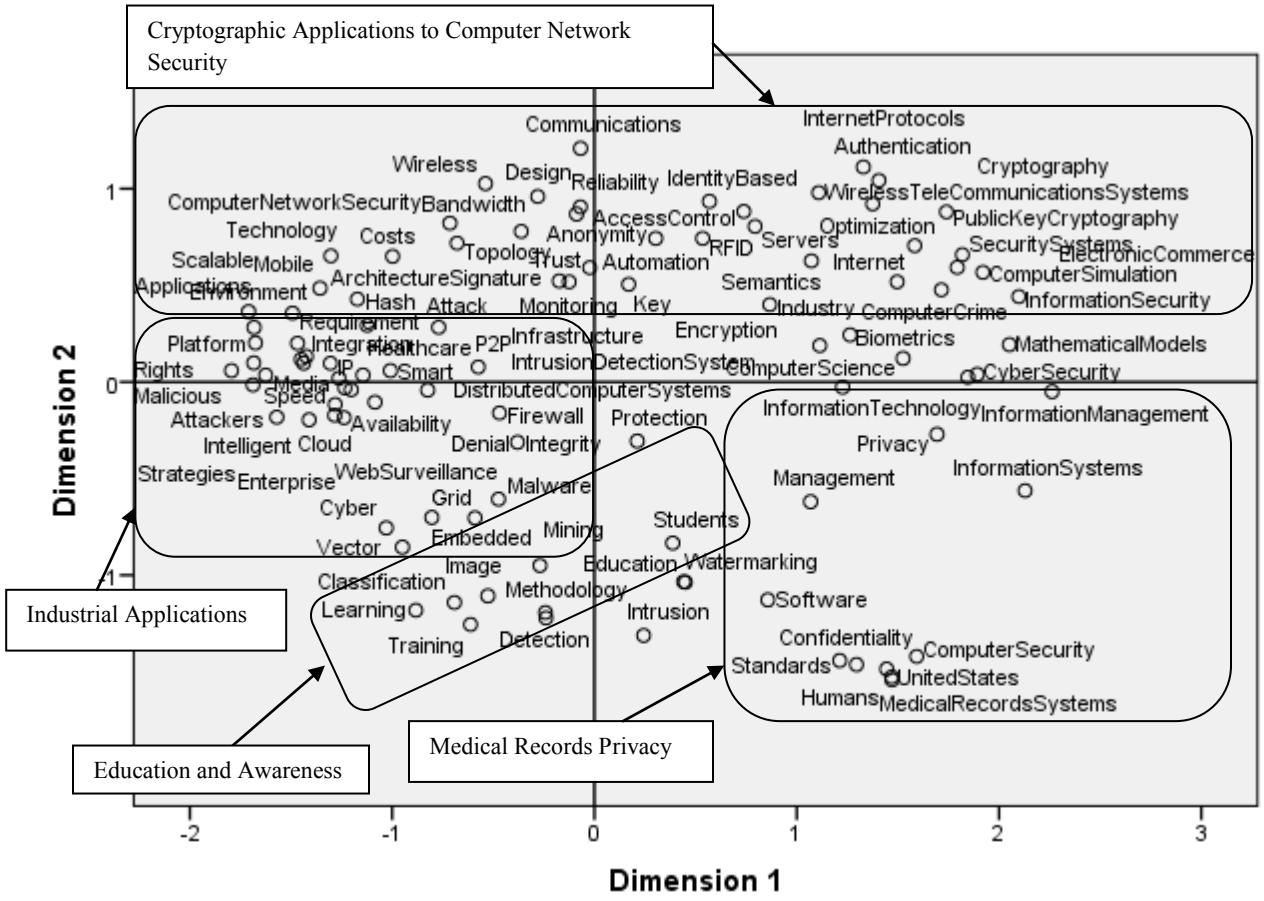


Figure 6.18B Information Security: MDS Map of Co-Word Data

Findings from the co-word analysis support the co-citation analysis with regard to the information security specialty's focus on cryptography and network security. What is more, the

co-word analysis has expanded this study's view of the information security specialty by recognizing additional research topics (i.e., education and awareness, industrial applications, medical records systems, and privacy).

6.5.3 A Discussion of the Information Security Specialty's Intellectual Structure

This section will discuss the identified co-citation and co-word clusters that represent the information security specialty's intellectual structure. Table 6.7 presents the co-citation and co-word cluster solutions side-by-side. Both types of data are indicators of the shared subject matter/topic by which they correspond. The co-citation clusters appear to be more precise with regard to the research topic because the units of analysis are documents. In contrast, the co-word groups are based on words only although they can facilitate direct interpretation of higher-level research topics (e.g., Education and Awareness).

Table 6.7 The Intellectual Structure of the Information Security Specialty: A Comparison

Co-Citation Cluster	Co-Word Cluster
Authentication Techniques and Attack Analysis Cryptographic Applications to Common Protocols Cryptographic Applications to Privacy and Access Control Formal and Theoretical Cryptography Information Security Management Intrusion Detection Systems Sensor Network Security Trusted Computing, Virtualization, and Taint Checking	Cryptographic Applications to Computer Network Security Education and Awareness Industrial Applications Medical Records Privacy

As Table 6.7 indicates, the co-citation clusters Cryptographic Applications to Common Protocols, Cryptographic Applications to Privacy and Access Control, and Formal and Theoretical Cryptography fall in line with the co-word cluster Cryptographic Applications to

Computer Network Security. These clusters mostly represent the highly formal research area of cryptography with specific applications to various information security services (e.g., common protocols, privacy, access control, networks). Cooper et al. (2010b, 52) described the research area of cryptography as encapsulating "basic theoretical concepts, mechanisms, algorithms and protocols". Moreover, the authors explain that the research domain of cryptography covers a broad range of cryptography applications (e.g., networking, wireless protocols, secure emails, car keys, critical infrastructure), mathematical preliminaries (e.g., probability theory, linear algebra), and public key systems. Furthermore, the co-citation and co-word analyses illustrated the central role of network security in the information security specialty.

The Information Security Management and Education and Awareness clusters seem to have conceptual overlap with their research focus revolving around system users in the organization. Whitman and Mattord (2011) argued that humans play a pivotal role in the information security equation. Moreover, Whitman and Mattord present information security management as including an understanding of managing the people, information assets, and processes in a balanced way that optimally protects the information. Processes act as the interface between people and information assets. Thus, a focus on processes that coordinates people and information assets is the primary means to manage information security risk. Often this is done by attempting to manipulate user risky behavior by enhancing penalties of noncompliance, and by educating the user making him/her more aware of the threats. Organizational perspectives are largely driven by the economic impact that information security breaches pose to organizations.

Authentication Techniques and Attack Analysis, and Intrusion Detection Systems are two research areas that include analyzing threat patterns, launching mock penetration attacks (i.e., red

team attacks) against one's own systems, and constructing applications based on findings to identify and prevent security breaches. Cooper et al. (2010b) described these topics under the umbrella heading Attack/Defense, which included such sub-topics as understanding threats and vulnerabilities, types of attacks, types of attackers, and defense mechanisms.

The Industrial Applications and Medical Records Privacy clusters underscore the practical, front-line use of information security research. Lewis (2006) discusses the prominent role that information security plays in the economy and in national security, as it is intricately tied to large industries. Lewis also suggested that this is a matter of national security, since the United States is a heavily networked society. Research into these topics often seeks to quantify the complex cascading impact of large-scale security breaches and develop processes for protecting and responding to such breaches. Furthermore, the United States has moved to place medical records in electronic format for more efficient transmission. Laws such as HIPPA have likely contributed to growing the research focus intersecting information security and medical records, largely an issue for medical organization records managers. Medical records system security requires bringing together process oriented information management and policy research with that of the more formal technical research on secure system architecture.

The Sensor Network Security cluster suggests a significant focus on society's use of sensor technology to expand computer interfaces to applications of surveillance (Akyildiz, Su, and Sankarasubramaniam 2002a; Akyildiz et al., 2002b). According to Akyildiz et al. (2002b), sensor network research is a research front with a lot of potential applications for military and intelligence reconnaissance, law enforcement and border control, and traffic management. Sensor networks are nodes, which are often physically distributed, to obtain input (e.g., motion, chemical or biological, video, audio) from a particular environment for surveillance purposes.

Sensors record information from the environment before sending it back to a command and control center for analysis. Often these networks are left dispersed in hostile areas and are prone to information security threats. Therefore, researchers within the information security specialty have been pursuing research on protecting the integrity of these forward operating sensor networks from enemy manipulation.

The Trusted Computing, Virtualization, and Taint Checking cluster contained three approaches to information security. Trusted computing refers to the inclusion of design constraints to hardware and software that prevent the computer from executing tasks that deviate from secure operations. For example, this cluster includes a research document by Lie et al. (2000) that presented the construction of copy and tamper resistant software so that the computer system would have built-in physical constraints to prevent malware from rewriting its software code.

7. Conclusions and Recommendations for Future Research

Very few studies had been conducted on the information security specialty as a research domain, especially from a scientometric perspective with both quantitative as well as qualitative techniques and on the large scale performed in this dissertation research. The few related studies, however, did not consider the information security specialty as a whole and mostly used qualitative methods (e.g., personal knowledge of the field). The information revolution has presented society with ever-mounting challenges to information security, thus the time was ripe for a comprehensive look at the past and present state of information security as an emerging research specialty with a more objective approach. The current study is an original endeavor to explore and describe the profile, dynamics, and intellectual structure of the information security specialty based on 58,908 records of its research documents over an approximate 42-year period. Below are the conclusions the present researcher draws from what has been presented so far.

7.1 Conclusions

The historical prevalence of the United States in information security research shows its considerable impact on the specialty in terms of both publication output and citation counts. Moreover, the present study finds that China contributes a disproportionally large number of information security research publications, prolific authors, and subsequently author affiliations. Yet, a further look at the highly cited documents of the specialty reveals that although China produces a high amount of information security documents Chinese authors have little impact on the information security specialty in terms of citations. It appears that at least in this current study quantity does not necessarily equal quality.

Information security, as a specialty, experienced an upward trajectory in the decade of 2001-2010 after a long period of slow but steady growth (i.e., 1972-2001). This explosive growth

was perhaps the result of an economy/society that has quickly shifted from a focus on industrialization to informationalization. The wide use of computers, the advent of the Internet, and their penetration into all sectors of modern society and people's personal lives are the catalyst for the rapid growth observed in the present study.

Although computer science and engineering are the two largest contributing disciplines to the information security specialty, there appears to be a dichotomy between the technical and social domains. Since, information security management is one of the two major cornerstones of the information security specialty. This view is established when accounting for both the productivity of each domain as well as its number of citations. Even though there is a disproportionate higher number of documents being produced from technical domains as opposed to socially oriented domains, the difference between the use (i.e., citedness) of each domain's respective documents is much less. The improved understanding that information security is a holistic enterprise requiring the orchestration of people, technology, and processes is the cause of researchers keeping one foot in the social domain (i.e., eliciting user needs, adjusting organizational processes) and the other foot in the technical domain (i.e., producing technology solutions).

In addition to the aforementioned conclusions, the most significant one lies in the identification of the intellectual structure underlying the information security specialty. In particular, the landscape of the specialty appeared to be mostly dominated by formal research in the areas of cryptography and network security. Other significant topics, particularly involving process-oriented research, were observed covering information security management in organizational contexts. Surprisingly, there was a lack of research on threats posed by insiders, which some researchers (e.g., Bishop and Gates 2008) have argued is one of the more substantial

information security threats. The most significant subject matter areas were cryptography, network security, and information security management. Smaller segments of research were identified such as emerging research fronts (e.g., sensor network security, intrusion detection systems) and less prominent security applications (e.g., medical records systems). Furthermore, methodological distinctions are evident between literature that used formal techniques (i.e., mathematical proofs), process-oriented techniques (i.e., design and development), and social investigative techniques. The distinction of methods is a result of information security remaining at the level of a research specialty as opposed to a discipline. In other words, students are learning information security in the context of the discipline in which their degrees are being conferred (e.g., computer science, criminology). The nature of the information security literature did not point to a unified scholarly program in which multiple methods, research problems, and solutions fall. Nonetheless, information security will likely move in this direction as the domain matures.

7.2 Recommendations and Future Research

The present study lends to future research in a number of ways, specifically by 1) removing the limits described in the earlier chapters and 2) the use of novel data sources (e.g., clicks, downloads, time viewed) as employed in altmetric research.

There were some limitations discussed in Section 5.5, that if adjusted for with adequate time and resources (e.g., sole use of Scopus, natural language keywords, traditional research techniques), could serve to improve developing a clearer and more accurate view of the information security specialty's intellectual structure. In particular, the present researcher suggests that future studies consider using the Web of Science to extract document records. It is principally strong, when compared to Scopus, with coverage of the social sciences and

humanities potentially lending to a well-rounded view of the information security specialty. Prospective studies also may find that using controlled vocabulary (i.e., specific terms supplied by experts to index document records) would improve precision and reduce noise with respect to data retrieval. Moreover, the threshold of 100 highly cited documents and 100 most frequently used keywords were used to cope with the limits imposed by the visualization techniques (e.g., MDS, network graphs). Therefore, subsequent studies should expand the threshold to include more data, which will likely lead to a fuller picture of the specialty.

Bibliometric data and traditional citation databases are not the only sources of data by which to study the intellectual structure of a specialty. Other more timely techniques take into account the diverse variety of ways in which information moves throughout science and society in general. Web applications have had a major impact on the way science is communicated and measured. Many journals are now solely published online and their content is enhanced with Web technology that allows readers to readily interact with research documents and other researchers with a few clicks of their computer mouse. Altmetrics is an alterative research technique with great potential for studying the information security specialty. According to Thewall et al. (2013), altmetrics uses a combination of traditional citation data combined with online metrics (e.g., clicks, downloads, time viewed, references in blogs and tweets). Altmetrics would allow for a view of information security that goes beyond the restrictions of traditional print publishing. Future research can draw an up-to-date picture of the information security specialty by focusing on the regular social media posts of its active scholars and others (e.g., industry, government, individual users). It would be especially useful for the specialty to ascertain the impact that their research efforts are having in the real world.

Finally, the substantial reliance of contemporary society on the flow of information would naturally lead people to ask a very difficult question: are there segments of the information security specialty that are having a positive impact on protecting society's information assets? If so, can these segments be studied in order to identify the secrets of their success? This is the challenge of scientometrics. Researchers are encouraged to use the present study as a starting point along with novel scientometric techniques (e.g., altmetrics) to dig deeper into the information security specialty. The ultimate goal is to explore and provide science managers with what they need to engineer an information security specialty that outpaces information security threats and vulnerabilities.

Bibliography

Abrams, Marshall D., Sushil Jajodia, and Harold J. Podell. 1995. *Information Security: An Integrated Collection of Essays*. Los Alamitos: IEEE Computer Society Press.

Abrizah, A., and Mee-Chin Wee. 2011. "Malaysia's Computer Science Research Productivity Based on Publications in the Web of Science, 2000-2010." *Malaysian Journal of Library and Information Science* 16 (1): 109-124.

Acedo, Francisco Jose, Jose Carlos Casillas. 2005. "Current Paradigms in the International Management Field: An Author Co-Citation Analysis." *International Business Review* 14 (5): 619-639.

Ahmad, Atif, A.B. Ruighaver, W.T. Teo. 2005. "An Information-Centric Approach to Data Security in Organizations." Proceedings at the TENCON 2005-2005 IEEE Region 10 Conference, Melbourne, Qld, November 21-25, 21-24.

Alberti, Leon Battista, Augusto Buonafalce, Charles J. Mendelsohn, and David Kahn. 1997. *ATreatise on Ciphers*. Torino: Galimberti.

Anderson, Richard C., Francis Narin, and Pail Mcallister. 1978. "Publication Ratings Verses Peer Review Ratings of Universities." *Journal of the American Society for Information Science* 29 (2): 91-103.

Anderson, J. P. 1972. *Information Security in a Multi-User Computer Environment*. Advances in Computers. Vol. 12.

Anegon, Felix de Moya, Evaristo Jimenez Contreras, and Mercedes de la Moneda Corrochano. 1998. "Research Fronts in Library and Information Science in Spain (1985-1994)." *Scientometrics* 42 (2): 229-246.

Anegon, Felix de Moya, Victor Herrero-Solana, and Evaristo Jimenez-Contreras. 2006. "A Connectionist and Multivariate Approach to Science Maps: The SOM, Clustering and MDS applied to Library and Information Science Research." *Journal of information Science* 32 (1): 63-77.

Arunachalam, Subbiah, and Udai N. Singh. 1985. "Sophisticated Science in a Small Country: A Scientometric Analysis of Superconductivity Research in Israel." *Journal of Information Science* 10 (4): 165-171.

Astrom, Fredrick., Rickard Danell, Larsen Birger, Jesper Wiborg Schneider, Balazas Schlemmer. "Celebrating Scholarly Communication Studies: A Festschrift for Olle Persson at his 60th Birthday." *International Society for Scientometrics and Informatics,* June 2009, 5.

Astrom, Fredrik. 2010. "The Visibility of Information Science and Library Science Research in Bibliometric mapping of the LIS Field." *The Library Quarterly* 80 (2): 143-159.

Backaus, Klaus, and Kai Lugger, and Mattias Koch. 2011. "The Structure and Evolution of Business-to-Business Marketing: A Citation and Co-Citation Analysis." *Industrial Marketing Management* 40 (6): 940-951.

Baker, Donald R. 1990. Citation Analysis: A Methodological Review." *Social Work Research and Abstracts* 26 (3): 3-10.

Bajwa, R.S., and K. Yaldram, S. Rafique. 2013. "A Scientometric Assessment of Research Output in NanoScience and Nanotechnology: Pakistan Perspective." *Scientometrics* 94 (1): 333-342.

Bala, Adarsh, and B.M. Gupta. 2010. “Research Activities in Biochemistry, Genetics and Molecular Biology During 1998-2007 in India: A Scientometric Analysis.” *DESIDOC Journal of Library and Information Technology* 30 (1): 3-14.

Bassecoulard, Elise, Alain Lelu, and Michel Zitt. 2007. “Mapping Nanosciences By Citation Flows: A A Preliminary Analysis.” *Scientometrics* 70 (3): 859-880.

Bauer, Friedrich L. 2007. “Rotor Machines and Bombes.” In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 382-445. New York: Elsevier.

Bayer, Alan, E., John C. Smart, and Gerland W. McLaughlin. 1990. “Mapping Intellectual Structure of a Scientific Subfield Through Author Cocitations.” *Journal of the American Society for Information Science* 41 (6): 444-52.

Bell, David. 1974. *The Coming of the Post-Industrial Society*. New York: Basic Books.

Bernal, John D. 1967. *The Social Function of Science*. Cambridge: M.I.T Press.

van den Besselaar, Peter, and Loet Leydesdorff. 1996. “Mapping Change in Scientific Specialties: A Scientometric Reconstruction of the Development of Artificial Intelligence.” *Journal of the American Society for Information Science and Technology* 47 (6): 415-436.

Beyhan, Berna, and Dilek Cetindamar. 2011. “No Escape from the Dominant Theories: The Analysis of Intellectual Pillars of Technology Management in Developing Counrties.” *Technological Forecasting and Social Change* 78 (2011): 103-115.

Bhattacharya, Sujit, and Prajit K. Basu. 1998. “Mapping A Research Area at the Micro Level Using Co-Word Analysis.” *Scientometrics* 43 (3): 359-372.

Bisbey, Richard., and Denise Hollingworth. 1978. “Protection Analysis: Final Report.” Technical Report,University of California. http://csrc.nist.gov/publications/history/bisb78.pdf.

Bishop, Matt, and Carrie Gates. 2008. "Defining the Insider Threat." *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*. http://nob.cs.ucdavis.edu/bishop/papers/2008-csiiw/definsider.pdf.

Bjork, Bo-Christer. 2013. “The Publishing Delay in Peer Reviewed Scholarly Journals.” *Journal of Informatics* 7 (4): 914-923.

Bjurstrom, Andreas, and Merritt Polk. 2011. “Climate Change and Interdisciplinarity: A Co-Citation Analysis of IPCC Third Assessment Report.” *Scientometrics* 87 (3): 525-550.

Blyth, Andrew, and Gerald L. Kovacich. 2006. *Information Assurance: Securing the Information Environment*. 2nd Ed. New York: Springer.

Bradford, Samuel C. 1985. “Sources of Information of Specific Subjects.” *Information Science* 10 (4): 173-180.

Botha, Reinhardth A., and Tshepo G. Gaaingwe. 2006. “Reflecting on 20 SEC Conferences.” *Computers and Security* 25 (4): 247-256.

Borner, Katy, Chaomei Chen, and Kevin W. Boyack. 2003. “Visualizing Knowledge Domains.” *Annual Review of the American Society for Information Science and Technology* 37 (1): 179-255.

Boyack, Kevin W., Katy Borner, and Richard Klavans. 2009. “Mapping the Structure and Evolution of Chemistry Research.” *Scientometrics* 79 (1): 45-60.

Boyack, Kevin W., Richard Klavans, and Katy Borner. "Mapping the Backbone of Science." *Scientometrics* 64 (3): 351-374.

Braam, R.R., H.F. Moed, and A.F.J. van Raan. 1991. "Mapping of Science by Combined Co-Citation and Word Analysis. I. Structural Aspects." *Journal of the American Society for Information Science* 42 (4): 233-251.

Braun, T., A. Schubert, W. Glanzel, M.T. Beck. E. Garfield, and M. Orban. 2001. *Scientometrics: An International Journal for All Quantitative Aspects of the Science of Science, Communication in Science and Science Policy*. Vol. 52 (2). Dordrecht: Kluwer Academic Publishers.

Breitenstein, Mikel. "Toward an Understanding of Visual Literacy: Examining of Conference Papers of the International Visual Literacy Association, 1991-2000." Doctoral Dissertation, Long Island University, 2003.

Bruer, John T. 2010. "Can We Talk? How the Cognitive Neuroscience of Attention Emerged from Neurobiology and Psychology, 1980-2005." *Scientometrics* 83 (3): 751-764.

Cabanac, Guillaume. 2012. "Shaping the Landscape of Research in Information Systems From the Perspective of Editorial Boards: A Scientometric Study of 77 Leading Journals." *Journal of the American Society for Information Science and Technology* 65 (3): 977-996.

Callon, M., J.P. Courtial, W.A. Turner, and S. Bauin. 1983. "From Translation to Problematic Networks: An Introduction to Co-Word Analysis." Social Science Information 22 (2): 191-235.

Callon, M., J. Law, and A Rip. 1986. *Mapping the Dynamics of Science and Technology*. London: Sage.

Cambrosio, A., C. Limoges, J.P. Courtial., and F. Laville. 1993. "Historical Scientometrics? Mapping Over 70 Years of Biological Safety Research with Co-Word Analysis." *Scientometrics* 27 (2): 119-143.

Capaccio, Tony. 2013. "Pentagon Five-Year Cybersecurity Plan Seeks #23 Billion." *Bloomberg,* June 10. http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html.

Carpenter, M.P., and Narin F. 1973. "Clustering of Scientific Journals." *Journal of the American Society for Information Science* 24 (6): 425-436.

Carr, Jeffrey. 2010. *Cyber Warfare.* Cambridge: O'Reilly.

Casillas, Jose, and Francisco Acedo. 2007. "Evolution of the Intellectual Structure of family Business Literature: A Bibliometric Study of *FBR*." *Family Business Review* 20 (2): 141-162.

Castells, Manuel. 1996. *The Rise of the Networked Society: The Information Age: Economy, Society and Culture*. Vol 1. Cambridge, MA: Oxford University Press.

Chabinsky, Steven R. 2010. *The Cyber Threat: Who's Doing What to Whom?* Washington, DC: Federal Bureau of Investigations. Retrieved from http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom.

Charvet, Francois F., Martha C. Cooper, and John T. Gardner. 2008. "The Intellectual Structure of Supply Chain Management: A Bibliometric Approach." *Journal of Business Logistics* 29 (1): 47-73.

Chebrolu, S., Abraham, A., Thomas, J.P. 2005. "Feature Deduction and Ensemble Design of Intrusion Detection Systems." *Computers and Security* 24 (4): 295-307.

Chen, Chaomei. 2006. “CiteSpace II: Detecting and Visualizing Emerging Trends and Transient Patterns in Scientific Literature.” *Journal of the American Society for Information Science and Technology* 57 (3): 359-377.

Chen, Chaomei, Katherine McCain, Howard White, and Xia Lin. 2002. Mapping Scientometrics (1981-2001). *Proceedings of the American Society for Information Science and Technology* 31 (1): 25-34.

Chen, Kaihua, and Jiancheng Guan. 2011. “A Bibliometric Investigation of Research Performance in Emerging Nanobiopharmaceuticals.” *Jornal of informetrics* 5 (2): 233-247.

Chen, Liang-Chu, and Yen-Hsuan Lien. 2011. “Using Author Co-Citation Analysis to Examine the Intellectual Structure of e-Learning: A MIS Perspective.” *Scientometrics* 89 (3): 867-886.

Chen, Yunwei, Shu Fang, and Katy Borner. 2011. “Mapping the Development of Scientometrics: 2002-2008.” *Journal of Library Science in China* 3: 131-46.

Chu, Heting. “Communication in Superconductivity Research: A Study of Scientific Discoveries With Particular Reference to a Developing Country.” Doctoral Dissertation, Drexel University, 1991.

—. 2005. “Taxonomy of Linked Web Entities: What Does it Imply for Webometric Research?” *Library and Information Science Research* 27 (1): 8-27.

—. 2010. *Information Representation and Retrieval in the Digital Age*. Medford: Information Today.

Chubin, Daryl E. “The Conceptualization of Scientific Specialties.” *The Sociological Quarterly* 17 (4): 448-476.

Clark, Kennith E. 1957. *America’s Psychologists: A Survey of a Growing Profession*. Washington: American Psychological Association.

Clarke, Richard, and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to do about it.* New York: Harpercollins.

Cobo, M.J., A.G. Lopez-Herrera, E. Herrera-Viedma, and F. Herrera. 2011. “An Approach for Detecting, Quantifying, and Visualizing the Evolution of a Research Filed: A Practical Application to the Fuzzy Sets Theory Field.” *Journal of Informatics* 5 (1): 146-166.

Cole, Jonathan R., and Harriet A. Zuckerman. “The Emergence of a Scientific Specialty: The Self-Exemplifying Case of the Sociology of Science.” In *The Idea of Social Structure: Papers in Honor of Robert K. Merton*, edited by Lewis A. Coser, 139-174. New York: Harcourt-Brace-Jovanovitch, 1975.

Cole, Stephen. 1992. *Making Science: Between nature and Society*. Cambridge: Harvard University Press.

Conway, James M., and Allen I. Huffcutt. 2003. "A Review and Evaluation of Exploratory Factor Analysis Practices in Organizational Research." *Organizational Research Methods* 6 (2): 147-168.

Cooper, Stephen, Christine Nickell, Victor Piotrowski, Bradley Oldfield, Ali Abdallah, Matt Bishop, Bill Caelli, Melissa Dark, E.K. Hawthorne, Lance Hoffman, Lance C. Perez, Charles Pfleeger, Richard Raines, Corey Schou, and Joel Brynielsson. 2010a. “An Exploration of the Current State of Information Assurance Education.” *ACM SIGCSE Bulletin* 41 (4), 109-125.

Cooper, Stephen, Christine Nickell, Lance C. Perez, Brenda Oldfield, Joel Bryniesson, Asim Gencer Gokce, Elizabeth K. Hawthorne, Karl J. Klee, Andrea Lawrence, and Susanne Wetzel. 2010b. "Towards Information Assurance (IA) Curricular Guidelines." Proceedings of the 2010 Annual Conference of the Innovation and Technology in Computer Science Education, Ankara, Turkey, June 28-30.

Copeland, Jack B. 2007. "Tunny and Colossus: Breaking the Lorenz Schlusselzusatz Traffic." In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 447-476. New York: Elsevier.

Corrin, Amber. 2013. "2014 Budget: DOD Budget Includes Boosts for Cyber, Future Priorities." *FCW,* April 10. http://fcw.com/articles/2013/04/10/dod-budget.aspx.

Coulter, N., I. Monarch, and S. Konda. 1998. "Software Engineering as Seen Through its Research Literature: A Study in Co-Word Analysis." *Journal of the American Society for Information Science* 49 (13): 1206-1223.

Courtail, J.P. 1994. "A Coword Analysis of Scientometrics." *Scientometrics* 31 (3): 251-260.

—. 1998. "Comments on Leydesdorff's Article." *Journal of the American Society for Information Science* 49 (1): 98.

Crane Diana. 1972. *Invisible Colleges: Diffusion of Knowledge in Scientific Communities*. Chicago: University of Chicago Press.

Crowley, Ed. 2003. "Information System Security Curricula Development." Proceeding of the 4th Annual Conference on Information Technology Curriculum ACM, New York, New York, 249-255.

Culnan, M.J. 1986. "The Intellectual Development of Management Information Systems, 1972-1982: A Co-citation Analysis." *Management Science* 32 (2): 1956-172.

Cybersecurity Information Assurance Interagency Working Group. 2010. *Cybersecurity Game-Change Research & Development Recommendations.* Washington, D.C: Federal Networking and Information Technology Research and Development Program. http://www.nitrd.gov/pubs/CSIA_IWG_%20Cybersecurity_%20GameChange_RD_%20Recommendations_20100513.pdf.

Dastidar, Prabir. 2004. "Ocean Science and Technology Research Across the Counrties: A Global Scenario. *Scientometrics* 59 (1): 15-27.

Dastidar, Prabir, and S. Ramachandran. 2008. "Intellectual Structure of Antarctic Science: A 25-Years Analysis." *Scientometrics* 77 (3): 389-414.

Davarpanah, Mohammad Reza. 2012. "Scientometric Analysis of Nuclear Science and Technology Research Output in Iran." *Journal of Scholarly Publishing* 43 (4): 421-439.

Davis, M., C.S. Wilson, W.W. Hood. 1999. "Ophthalmology and Optics: An Informetric Study of Australia's Contribution to Fields in the Vision Science Domain, 1991-95." *Scientometrics* 46 (3): 399-416.

De Bellis, Nicola. 2009. *Bibliometrics and Citation Analysis*. Lanham, Maryland: The Scarecrow Press, Inc.

De May, Mark. 1982. *The Cognitive Paradigm*. London: Reidel.

DeNardis, Laura. 2007. "A History of Internet Security." In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 681-702. New York: Elsevier.

Department of Defense. 2010. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Department of Defense. http://ra.defense.gov/documents/rtm/jp1_02.pdf.

—. 2011. *Strategy for Operating in Cyberspace*. Washington, DC: U.S.Department of Defense. Retrieved from http://www.defense.gov/news/d20110714cyber.pdf.

—. 2012. *Joint Publication 3-13: Information Operations*. Washington, DC: Department of Defense.

Department of Homeland Security. 2009. *A Roadmap for Cybersecurity Research*. Ft. Belvoir: Defense Technical Information Center. http://handle.dtic.mil/100.2/ADA529806.

Dlamini, Moses, Mariki Eloff, and Jan Eloff. 2009. "Information Security: The Moving target." *Computers & Security* 28 (3-4): 189-198.

Dhillon, Mapreet. 2006. "Towards Changes in Information Security Education." *Journal of Information Security Education* 5, 221-233. http://jite.informingscience.org/documents/Vol5/v5p221-233Hentea148.pdf.

Diffie, Whitfield, and Martin Hellman. 1976. "New Directions in Cryptology." *IEEE Transactions on Information Theory* 22 (6): 644-54.

Ding, Y. G. Chowdhury, and S. Foo. 2001. "Bibliometric Cartography of Information Retrieval Research by Using Co_word Analysis." *Information Processing and Management* 37 (6): 817-842.

—. 2000. "Journals as Markers of Intellectual Space: Journal Co-Citation Analysis of Information Retrieval Area." *Scientometrics* 47 (1): 55-73.

Diodato, Virgil. 1994. *Dictionary of Bibliometrics*. New York: The Haworth Press, Inc.

Dolfsma, and Loet Leydesdorff. 2010. "The Citation Field of Evolutionary Economics." *Journal of Evolutionary Economics* (20) 5: 645-664.

Durisin, Boris, and Fulvio Puzone. 2009. "Maturation of Corporate Governance Research, 1993-2007: An Assessment." *Corporate Governance: An International Review* 17 (3): 266-291.

Easley, David, and Jon Kleinberg. 2010. *Networks, Crowds, and Markets: Reasoning About a Highly Connected World*. New York: Cambridge University Press.

Edge, D. 1977. "Why am I not a Co-citationist?" *Society for Social Studies of Science Newsletter* 3: 13-19. http://www.garfield.library.upenn.edu/essays/v3p240y1977-78.pdf.

Egghe, Leo. 2010. "The Hirsch Index and Related Impact Measures." *Annual Review of the Journal of the American Society for Information Science and Technology* 44 (1): 65-114.

Ellis, David, David Allen, and Tom Wilson. 1999. "Information Science and Information Systems: Conjunct Subjects Disjunct Disciplines." *Journal of the American Society for Information Science and Technology* 50 (12): 1095-1107.

Eom, Sean B. 1996. "Mapping the Intellectual Structure of Research in Decision Support Systems Through Author Cocitation Analysis (1971-1993)." *Decision Support Systems* 16 (4): 315-38.

—. 2003. *Author Co-citation Analysis using Custom Bibliographic Databases: An Introduction to the SAS Approach*. Lewiston: Edwin Mellen Press.

—. 2009. *Author Co-Citation Analysis: Quantitative Methods for Mapping the Intellectual Structure of an Academic Discipline*. Hershey: Information Science Reference.

Erfanmanesh, Mohammadamin, Vala Ali Rohani, and A. Abrizah. 2012. “Co-Authorship Network of Scientometrics Research Collaboration.” *Malaysian Journal of Library and Information Science* 17 (3): 73-93.

Executive Office of the President of the United States. 2009. *Cyberspace Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, DC: Executive Office of the President of the United States. http://purl.access.gpo.gov/GPO/LPS118258.

—. 2010. *The Comprehensive National Cybersecurity Initiative*. Washington, D.C.: Executive Office of the President of the United States. http://purl.fdlp.gov/GPO/gpo6112.

Everitt, B.S. 1980. *Cluster Analysis*. London: Heinemann Educational Books Ltd.

Falagas, M.E., E.L. Pitsouni, G.A. Malietzis, and G. Pappas. 2008. “Comparison of PubMed, Scopus, Web of Science, and Google Scholar: Strengths and Weaknesses.” *FASEB Journal* 22 (2): 338-342.

Feistel, Horst. 1973. “Cryptography and Computer Privacy.” *Scientific America* 228 (5): 15-23.

Fortnow, Lance. 2009. "Viewpoint: Time for Computer Science to Grow Up." *Communications of the ACM* 52 (8): 33-35.

Franceschet, Massimo. 2010. "The Role of Conference Publications in Computer Science: A Bibliometric View." *Communications of the ACM* 53 (12): 129-132.

Fernandez-Alles, Mariluz, Antonio Ramos-Rodriguez. 2009. “Intellectual Structure of Human Resources Management Research: A Biblometric Analysis of the Journal Human Resource Management, 1985-2005.” *Journal of the American Society for Information Science and Technology* 60 (1): 161-175.

Field, Andy. 2005. *Discovering Statistics Using SPSS*. London: Sage Publications.

Fredericks, Brian E. 1997. “Information Warfare: At the Crossroads.” *Joint Force Quarterly* Summer, 97-103.

Fuchs, Ludwig, Gunther Pernul, and Ravi Sandhu. 2011. "Roles in Information Security–A Survey and Classification of the Research Area." *Computers & Security* 30 (8): 748-769.

Garfield, Eugene. 1955. “Citation Indexes for Science: A New Dimension in Documentation Through Association of Ideas.” *Science* 122 (3159): 108-11.

—. 1979a. “Scientometrics Comes of Age.” *Current Contents* 46: 5-10.

—. 1979b. *Citation Indexing: Its Theory and Application in Science, Technology, and Humanities*. John Wiley & Sons: New York.

—. 2001. "From Bibliographic Coupling to Co-Citation Analysis Via Algorithmic Historio-Bibliography: A Citationist's Tribute to Belver C. Griffith." Retrieved from http://garfield.library.upenn.edu/papers/drexelbelvergriffith92001.pdf.

—. 2009. "From the Science of Science to Scientometrics. Visualizing the History of Science with HistCite Software". *Journal of Informetrics*. 3 (3): 173-179.

Geer, Dan. 2013. “Resolved: The Internet is No Place for Critical Infrastructure.” *Magazine Communications of the ACM* 56 (6): 48-53.

Georgi, Christoph, Inga-Lena Darkow, and Herbert Kotzab. 2010. “The Intellectual Foundation of the Journal of Business Logistics and its Evolution Between 1978 and 2007.” *Journal of Business Logistics* 31 (2): 63-109.

Gleick, James. 2011. *The Information: A History, A Theory, A flood*. New York: Pantheon Books.

Glenisson, Patrick, Wolfgang Glanzel, Frizo Jassens, and bart De Moor. 2005. "Combining Full Text and Bibliometric Information in Mapping Scientific Disciplines." *Information Processing and Management* 41 (6): 1548-1572.

Glenny, Misha. 2011. *Dark Market: How Hackers Become Mafia*. New York: Vantage Books.

Goldstein, Jeffrey. 1999. "Emergence as a Construct: History and Issues." *Emergence* 1 (1): 49-72.

Gollmann, Dieter. 2007. "Security Models." In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 623-635. New York: Elsevier.

Garvey, William D., and Belver C. Griffith. 1967. "Scientific Communication as a Social System." *Science* 157 (3792): 1011-1016.

Griffith, Belver C., Henry G. Small, Judith A. Stonehill, and Sandra Dey. 1974. "The Structure of Scientific Literatures II: Toward a Macro- and Microstructure for Science." *Science Studies* 4 (4): 339-365.

Griffith, Belver C., Carl M. Drott, and Henry G. Small. 1977. "On the Use of Citations in Studying Scientific Achievements and Communication." *Current Contents* 9 (39): 234-239.

Gu, Yinian. 2004. "Global Knowledge Management Research: A Bibliometric Analysis." *Scientometrics* 61 (2): 171-190.

Gupta, B.M., and Dhawan, S.M. 2005. "Computer Science Research in India: A Scientometric Analysis of research Output During the Period 1994-2001." *DESIDOC Bulletin of Information Technology* 25 (1): 3-11.

Gupta, B.M., Har Kaur, and Adarsh Bala. 2011. "Mapping of Indian Diabetes Research During 1999-2008: A Scientometric Analysis of Publications Output." *DESIDOC Journal of Library and Information Technology* 31 (2): 143-152.

Hammarfelt, Bjorn. 2011. "Interdisciplinary and the Intellectual Base of Literature Studies: Citation Analysis of Highly Cited Monographs." *Scientometrics* 86 (3): 705-725.

Hammonds, Grace L. 1993. "Confidentiality, Integrity, Assured Service: Tying Security All Together." Proceedings on the 1991-1993 Workshop on New Security Paradigms, New York, New York, 48-52.

Harter, Stephen P. 1992. "Psychological Relevance and Information Science." *Journal of the American Society for Information Science and Technology* 43 (9): 602-615.

Hoffman, Donna L., and Morris B. Holbrook. 1993. "The Intellectual Structure of Consumer Research: A Bibliometric Study of Author Cocitations in the First 15 Years of the *Journal of Consumer Research*." *Journal of Consumer Research* 19 (4): 505-17.

Hoffstetter, Dorothy H. "Bibliographical Approach to the History of Idea Development in Bibliometrics." Doctoral Dissertation, Case Western Reserve University, 1985.

Holmes, Boyd Patterson. "The Domain of Information Science, with an Emphasis on Contributing Disciplines: 1973 to 1998." Doctoral Dissertation, The University of Western Ontario, 2002.

Homeland Security Presidential Directive 23/National Security Presidential Directive 54 (January 2008)

Hu, Chang-Ping, Ji-Ming Hu, Sheng-Li Deng, and Yong Liu. 2013. "A Co-Word Analysis of Library and Information Science in China." *Scientometrics* 97 (2): 369-382.

Hu, Chang-Ping, Ji-Ming Hu, Yan Gao, Yao-Kun Zhang. 2011. "A Journal Co-Citation Analysis of Library and Information Science in China." *Scientometrics* 86 (3): 657-670.

Hu, Jie, Yuwei Ma, Liang Zhang, Fuxing Gan, and Yuh-Shan Ho. 2010. "A Historical Review and Bibliometric Analysis of research on lead in Drinking Water Field From 1991 to 2007." *Science of the Total Environment* 408 (7): 1738-1744.

Institute for the Electronical and Electronic Engineers (IEEE). 2013. *IEEE Taxonomy Version 1.0*. IEEE Advancing Technology for Humanity. http://www.ieee.org/documents/taxonomy_v101.pdf.

Institute for the Electronical and Electronic Engineers (IEEE). 2013. *IEEE Thesauri Version 1.0*. IEEE Advancing Technology for Humanity. http://www.ieee.org/ucm/groups/public/@ieee/@web/@org/@pubs/documents/file/2004 2208.pdf.

Ismail, Sharif, Edward Nason, Sonja Marjanovic and Jonathan Grant. 2009. *Bibliometrics as a Tool for Supporting Prospective R&D Decision-Making in the Health Sciences: Strengths, Weaknesses and Options for Future Development*. Santa Monica, CA: RAND Corporation. http://www.rand.org/pubs/technical_reports/TR685.

Jackson, Melody. "A Bibliometric Analysis of Green Building Literature." Doctoral Dissertation, Northcentral University, 2012.

Jain, Anil K., Arun Ross, and Sharath Pankanti. 2006. "Biometrics: A Tool for Information Security." *IEEE Transactions on Information Forensics and Security* 1 (2): 125-143.

Jamali, Hamid R. 2013. "Citation Relations of Theories of human Information Behavior." Webology 10 (1). (eJournal) Article 106. http://www.webology.org/2013/v10n1/a106.html.

Janssens, Frizo, Jacqueline Leta, Wolfgang Glanzel, and Bart De Moor. 2006. "Towards Mapping Library and Information Science." *Information Processing and Management* 42 (6): 1614-1642.

Janssens, Frizo, Wolfgang Glanzel, and bart De Moor. 2008. "A Hybrid Mapping of Information Science." *Scientometrics* 75 (3): 607-631.

Jeong, Senator, and Hong-Gee Kim. 2010. "Intellectual Structure of Biomedical Informatics Reflected in Scholarly Events." *Scientometrics* 85 (2): 541-551.

Kahn, David. 1996. *The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet*. New York, NY: Scribner.

Kajikawa, Yuya, and Yoshiyuki Takeda. 2009. "Citation Network Analysis of organic LEDs." *Technological Forecasting & Change* 76 (8): 1115-1123.

Karpagam, R., S. Gopalakrishnan, M. Natarajan, and B. Ramesh Babu. 2011. "Mapping of Nanoscience Research in India: A Scientometric Analysis, 1990-2009. *Scientometrics* 89 (2): 501-522.

Keenan, Andrew. "The Discourse of the Information Age." Master's thesis, University of Alberta, 2010.

Kent, Karen. 2009. *Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD: National Institute of Standards and Technology.

Kessler, M. M.1963a. "Bibliographic Coupling Between Scientific Papers." *American Documentation* 14 (1): 10-25.

—. 1963b. “Bibliographic Coupling Extended in Time: Ten Case Histories.” *Information Storage & Retrieval* 1 (4): 169-187.

Khan, Gohar Feroz, Junghoon Moon, and Han Woo Park. 2011. “Network of the Core: Mapping and Visualizing the Core of Scientific Domains.” *Scientometrics* 89 (3): 759-779.

Kim, Amy Chan Hyung. “Knowledge Structure in Sports Management: Bibliometric and Social Network Analysis.” Doctoral Dissertation, Ohio State University, 2012.

Kim, Heejung, Jae Yun Lee. 2009. “Archiving Research Trends in LIS Domain Using Profiling Analysis.” *Scientometrics* 80 (1): 75-90.

Kim, Hyunjung. “Examining the Knowledge Structure in the Communication Field: Author Cocitation Analysis for the Editorial Board of the Journal of Communication, 2008 and 2011.” Doctoral Dissertation, University of Buffalo, State University of New York, 2012.

Klir, G. J. 1991. *Facets of systems science*. New York: Plenum Press.

Kraay, Aart., and Jaume Ventura. "The Dot-Com Bubble, the Bush Deficits, and the U.S. Current Account." In *G7 Current Account Imbalances: Sustainability and Adjustment,* edited by Richard H. Clarida, 457-496. The National Bureau of Economic Research: University Chicago Press, 2007.

Kreuzman, Henry. 2001. “A Co-Citation Analysis of Representative Authors in Phiosophy: Examining the Relationship Between Epidemiologists and Philosophers of Science. *Scientometrics* 51 (3): 525-539.

Kuehl, Dan. 2007. “The Information Revolution and the Transformation of Warfare.” In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 821-831. New York: Elsevier.

Kuhn, Thomas S. 1962. *The Structure of Scientific Revolutions*. Chicago, IL: The University of Chicago Press.

Kulkarni, Abhaya V., Brittany Aziz, Iffat Shams, and Jason W. Busse. 2009. “Comparison of Citations in the Web of Science, Scopus, and Google Scholar for Articles Published in General Medical Journals.” *JAMA* 302 (10): 1092-1096.

Kumar, A. and D. Zhang. 2006. "Personal Recognition using Hand Shape and Texture." *IEEE Transactions on Image Processing* 15 (8): 2454-2461.

Kumar, Sameer, and Jariah Mohd. 2013. “Mapping Research Collaborations in the Business and Management Field in Malaysia, 1980-2010.” *Scientometrics* (January): 1-27.

LaMacchia, B., K. Lauter, and A. Mityagin. 2007. *Stronger Security of Authenticated Key Exchange*. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Vol. 4784 LNCS.

Langevin, James R., Michael T. McCaul, Scott Charney, Harry Raduege, and James A. Lewis. *Securing Cyberspace for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, 2008. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Lariviere, Vincent, Cassidy R. Sugimoto, and Blaise Cronin. 2012. “A Bibliometric Chronicling of Library and Information Science’s First Hundred Years.” *Journal of the American Society for Information Science and Technology* 63 (5): 997-1016.

Larsen, Katherine. 2008. “Knowledge Network Hubs and Measures of Research Impact, Science Structure, and Publications Output in Nanostructured Solar Cell Research.” *Scientometrics* 74 (1): 123-142.

Law, J., and J. Whittaker. 1992. “Mapping Acidification Research: A Test of the Co-Word Method.” *Scientometrics* 23 (3): 417-461.

Lee, Woo Hyoung. 2008. How to Identify Emerging Research Fields Using Scientometrics: An Example in the Field of Information Security. *Scientometrics* 76 (3): 503-525.

Leeuw, Karl de., and Jan Bergstra. 2007. *The History of Information Security: A Comprehensive Handbook*. New York: Elsevier.

Levitt, Jonathan M., and Mike Thelwall. 2009. “The Most Highly Cited Library and Information Science Articles: Interdisciplinarity, First Authors and Citation Patterns.” *Scientometrics* 78 (1): 45-67.

Lewis, Ted. G. 2006. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Monterey, CA: Wiley-Interscience.

Leydesdorff, Leot. 1987. “The Use of Scientometric Methods for Evaluating National Research Programs.” *Science and Technology Studies* 5 (1): 22-31.

—. 1997. “Why Words and Co-Words Cannot Map the Development of the Sciences.” *Journal of the American Society for Information Science* 48 (5): 418-427.

—. 2001. *The Challenge of Scientometrics: The Development, Measurement, and Self-Organization of Scientific Communication.* New York: Universal Publishing.

—. 2004. The Evaluation of Research and the Scientometric Research Program: Historical Evolution and Redefinitions of the Relationships.” Studies in Science of Science 22 (3): 225-232.

—. 2006. "Can Scientific Journals Be Classified in Terms of Aggregated Journal-Journal Citation Relations Using the Journal Citation Reports?" *Journal of the American Society for Information Science and Technology* 57 (5): 601-613.

Leydesdorff, Leot, and Ismael Rafols. 2008. “A Global Map of Science Based on ISI Subject Categories.” *Journal for the American Society for Information Science and Technology* 60 (2): 348-362.

Leydesdorff, Leot, and Ping Zhou. 2007. “Nanotechnology as a Field of Science: Its Delineation in Terms of Journals and Patents.” *Scientometrics* 70 (3): 693-713.

Leydesdorff, Leot, and Robert L. Goldstone. 2014. “Interdisciplinarity at the Journal and Specialty Level: The Changing Knowledge Bases of the *Journal Cognitive Science*.” Journal of the *American Society for Information Science and Technology* 65 (1): 164-177.

Leydesdorff, Leot, and Liwen Vaughan. (2006). “Co-occurrence Matrices and their Applications in Information Science: Extending ACA to the Web Environment.” *Journal of the American Society for Information Science and Technology*, 57(12), 1616-1628.

Li, Ling-Li, Guohua Ding, Nan Feng, Ming-Huang Wang, Yuh-Shan Ho. 2009. “Global Stem Cell Research Trend: Bibliometric Analysis as a Tool for Mapping of Trends from 1991-2006.” *Scientometrics* 80 (1): 39-58.

Lin, Yang. “The Intellectual Structure of Political Communication Research: An Author Co-Citation Analysis.” Doctoral Dissertation, University of Oklahoma, 1997.

Lin, Yang, and Lynda L. Kaid. 2000. “Fragmentation of the Intellectual Structure of Political Communication Study: Some Empirical Evidence.” *Scientometrics* 47 (1): 143-164.

Liu, Gao-Yong, Ji-Ming Hu, and Hui-Ling Wang. 2012. “A Co-Word Analysis of Digital Library Field in China.” *Scientometrics* 91 (): 203-217.

Liu, Zao. 2005. “Visualizing the Intellectual Structure in Urban Studies: A Journal Co-Citation Analysis (1992-2002).” *Scientometrics* 62 (3): 385-402.

Liu, Zao, and Chengzhi Wang. 2005. “Mapping Interdisciplinarity in Demography: A Journal Network Analysis.” *Journal of Information Science* 31 (4): 308-316.

Locke, Joanne, and Hector Perera. 2001. “The Intellectual Structure of International Accounting in the Early 1990s.” *The International Journal of Accounting* 36 (2): 223-249.

Lord, Kristine M., and Travis Sharp. (2011). *America’s Cyber Future: Security and Prosperity in the Information Age.*Vol. I. Washington, DC: Center for a New American Security.

Lunin, Lois F., and Howard D. White. 1990. “Perspectives on Author Co-citation analysis.” Journal of the American Society for Information Science and Technology 41 (6): 429-432.

Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, September 2010. Retrieved from http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

Ma, Rumin. 2012. “Discovering and Analysing the Intellectual Structure and Its Evolution of LIS in China, 1998-2007.” *Scientometrics* 93 (3): 645-659.

Ma, Rumin, Qiangbin Dai, Chaoqun Ni, and Xuelu Li. 2009. “An Author Co-Citation Analysis of Information Science in China with Chinese Google Scholar Search Engine, 2004-2006.” *Scientometrics* 81 (1): 33-46.

Maconachy, Victor W., Corey D. Schou, Daniel Ragsdale, and Don Welch. 2001. “A Model for Information Assurance: An Integrated Approach.” Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West point, New York, June 5-6, 306-310.

MacRoberts, M.H., and Barbra R. MacRoberts. 1986. “Quantitative Measures of Communication in Science: A Study of the Formal Level .” *Social Studies of Science* 16 (1): 151-172.

—. 1989. “Problems of Citation Analysis: A Critical Review.” Journal of the American Society for Information Science 40 (5): 342-349.

—. 1996. “Problems of Citation Analysis.” *Scientometrics* 36 (3): 435-444.

Massey, James L. 1988. “An Introduction to Contemporary Cryptology.” *Proceeding of the IEEE* 76 (5): 533-49.

May, K.O. 1966. “Quantitative Growth of the Mathematical Literature.” *Science* 154 (3757): 1672-1673.

Mcallister, Paul R., and Francis Narin. 1983. “Characterization of the Research Papers of U.S. Medical Schools.” *Journal of the American Society for Information Science* 34 (2): 123-131.

McCain, Katherine W. 1983. “The Author Cocitation Structure of Macroeconomics.” *Scientometrics* 5 (5): 277-289.

—. 1984. "Longitudinal Author Cocitation Mapping: The Challenging Structure of Macroeconomics." *Journal of the American Society for Information Science* 35 (6): 351-359.

—. 1986. “Mapping Authors in Intellectual Space: A Technical Overview.” *Journal of the American Society for Information Science* 41 (6): 433-443.

—.1995. “The Structure of Biotechnology R&D.” *Scientometrics* 32 (2): 153-175.

—.1990a. “Cocited Author Mapping as a Valid Representation of Intellectual Structure.” *Journal of the American Society for Information Science* 37 (3): 111-122.

—.1990b. “Mapping Authors in Intellectual Space: A Technical Overview.” *Journal of the American Society for Information Science* 41 (6): 433-443.

—.1991. “Mapping Economics Through the Journal Literature: An Experiment in Journal Cocitation Analysis.” *Journal of the American Society for Information Science* 42 (4): 290-296.

—. 1998. “Neural Networks Research in Context: A Longitudinal Journal Cocitation Analysis of an Emerging Interdisciplinary Field.” *Scientometrics* 41 (3): 389-410.

—.2010. “Core Journal Literatures and Persistent Research Themes in an Emerging Interdisciplinary Field: Exploring the Literature of Evolutionary Developmental Biology.” *Journal of Informetrics* 4 (2): 157-165.

McCain, Katherine W., June M. Verner, Gregory W. Hislop, William Evanco, and Vera Cole. 2005. “The Use of Bibliometric and Knowledge Elicitation Techniques to Map a Knowledge Domain: Software Engineering in the 1990s.” *Scientometrics* 65 (1): 131-144.

McCumber, John R. 1991. “Information Systems Security: A Comprehensive Model.” Proceedings at the 14th National Computer Security Conference, Washington D.C., October 1-4.

Melhart, Bonnie, and Stephanie White. "Issues in Defining, Analyzing, Refining, and Specifying System Dependability Requirements." Proceedings of the Seventh IEEE International Conference and Workshop on Engineering of Computer Based Systems, 2000.

Menard, Henry W. 1971. *Science: Growth and Change*. Cambridge, MA: Harvard University Press.

Merton, Robert K. “Paradigm for the Sociology of Knowledge.” In *The Sociology of Science*. Chicago: University of Chicago Press, 1973.

Metcalfe, Robert M. "Packet communication." Doctoral Dissertation, Massachusetts Institute of Technology, 1973. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=AD0771430.

Meushaw, Robert. 2012. Developing a Blueprint for a Science of Cyber Security. Guest Editor’s Column. *The Next Wave* 19 (2): 1.

Mikhailov, Ivanovich Aleksandr, Arkadii Ivonovich Chernyi, and Rudzhero Sergeevich Giliarevskii. 1984. *Scientific Communications and Informatics*. Arlington, VA: Information Resources Press.

Milgram, Stanley. 1967. “The Small-World problem.” *Psychology Today* 1 (1): 61-67.

Milojevic, Stasa. 2009. “Bog Science, Nano Science?: Mapping the Evolution and Socio-Cognitive Structure of Nanoscience/Nanotechnology Using Mixed Methods.” Doctoral Dissertation, University of California.

Milojevic, Stasa, and Loet Leydesdorff. 2013. “Information Metrics *(iMetrics)*: A Research Specialty with a Socio-Cognitive Identity?” *Scientometrics* 95 (1): 141-157.

Mitre Corporation. 2010. *Science of Cyber-Security*. McLean, VA: Mitre Corporation. Retrieved from http://www.fas.org/irp/agency/dod/jason/cyber.pdf.

Moed, Henk F. 2005. *Citation Analysis in Research Evaluation*. Dordrecht, Nevetherlands: Springer.

Mohammadi, Ehsan. 2012. “Knowledge Mapping of the Iranian Nanoscience and Technology: A Text Mining Approach.” *Scientometrics* 92 (3): 593-608.

Mohrman, Kathryn. 2008. “The Emerging Global Model with Chinese Characteristics.” *Higher Education Policy* 21 (1): 29-48. http://www.international.ac.uk/media/4355/the%20emerging%20global%20model%20with%20chinese.pdf.

Moravcsik, Michael J. 1977. “A Progress Report on the Quantification of Science.” *Journal of Scientific and Industrial Research* 36 (5): 195-203.

Moravcsik, Micheal J., and Poovanalingam Murugesan. 1979. “Citation Patterns in Scientific Revolutions.” Scientometrics 1 (2): 161-169.

Morris, Steven A. 2005. “Manifestation of Emerging Specialties in Journal Literature: A Growth Model of Papers, References, Exemplars, Bibliographic Coupling, Cocitation, and Clustering Coefficient Distribution.” *Journal of the American Society for Information Science and Technology* 56 (12): 1250-1273.

Morris, Steven A., and Betsy Van der Veer Martens. 2008. “Mapping Research Specialties.” Annual *Review of the American Society for Information Science and Technology* 42 (1): 213-295.

Moya-Anegon, Felix, Zaida Chinchilla-Rodriquez, Benjamin Vargas-Quesada, Elena Corera-Alvarez, Francisco Jose Munoz-Fernandez, Antonio Gonalez-Molina, Victor Herrero-Solana. 2007. “Coverage Analysis of Scopus: A Metric Approach.” *Scientometrics* 73 (1): 57-58.

Mrayati, Mohammed, Yahya Meer Alam, and M. Hassan at-Tayyan. 2003. *al-Kindi's Treatise on Cryptanalysis.* trans. Said M. al-Asaad. Vol. 1 of the *Arabic Origins of Cryptology. Riyadh: King Faisal Center for Research and Islamic Studies.*

Mulla, K.R. 2012. “Identifying and mapping the Information Science and Scientometrics Analysis Studies in India (2005-2009): A Bibliometric Study.” *Library Philosophy and Practice* (eJournal). Paper 772. http://digitalcommons.unl.edu/libphilprac/772/.

Murugan, C., and R. Balasubramani. 2012. “Scientometric Mapping of Remote Sensing Research Output: A Global Perspective.” *Library Philosophy and Practice*. (eJournal). Paper 801. http://digitalcommons.unl.edu/libphilprac/801/.

Nalimov, V. V., and Z. M. Mulchenko. 1971. *Measurement of Science. Study of the Development of Science as an Information Process*. Ft. Belvoir: Defense Technical Information Center.

Natale, Fabrizio, Gianluca Fiore, and Johann Hofherr. 2012. “Mapping the Research on Aquaculture. A Bibliometric Analysis of Aquaculture Literature.” *Scientometrics* 90 (3): 983-999.

National Science Board. 1973. *Science Indicators 1973.* Washington, DC: Government Printing Office.

National Science and Technology Council. 2011. *Trustworthy cyberspace strategic plan for the Federal Cyberspace Research and Development Program*. Washington, D.C.: Executive Office of the President of the United States. http://www.nitrd.gov/subcommittee/csia/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf.

Neff, Mark William, and Elizabeth A. Corley. 2009. “35 years and 160,000 Articles: A Bibliometric Exploration of the Evolution of Ecology.” *Scientometrics* 80 (3): 657-682.

Nerur, Sridhar P., Abdul A. Rasheed, and Vivek Natarajan. 2008. “The Intellectual Structure of the Strategic Management Field: An Author Co-Citation Analysis.” *Strategic Management Journal* 29 (3): 319-336.

Nicolaisen, Jeppe. 2007. “Citation Analysis.” *Annual Review of Information Science and Technology* 41 (1): 609-641.

Noyons, E.C.M, and A.F.J. van Raan. 1994. Bibliometric Cartography of Scientific and Technological Development of an R&D Field.” *Scientometrics* 30 (1): 157-173.

—. 1998. Monitering Scientific Developments from a Dynamic Perspetive: Self-Organized Structuring to Map Neural Network Research." *Journal of the American Society for Information Science* 49 (1): 68-81.

Office of Management and Budget. 2013. *Fiscal year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*. Washington, DC: Office of Management and Budget.

Otte, Evelien., and Ronald Rousseau. 2002. "Social Network Analysis: A Powerful Strategy, Also for the Information Sciences". *Journal of Information Science.* 28 (6): 441-453.

Oree, William L. "Analysis of the Unites States Computer Emergency Readiness Team's (U.S. CERT) Einstein III Intrusion Detection System, and its Impact on Privacy." Master's thesis, Naval Postgraduate School, 2013.

Osareh, Farideh, and Katherine W. McCain. 2008. "The Structure of Iranian Chemistry Research, 1990-2006: An Author Cocitation Analysis." *Journal of the American Society for Information Science and Technology* 59 (13): 2146-2155.

Park, Han Woo, and Loet Leydesdorff. 2008. "Korean Journals in the Science Citation Index: What Do They Reveal About the Intellectual Structure of S&T in Korea?." *Scientometrics* 75 (3): 439-462.

—. 2009. "Knowledge Linkage Structures in Communication Studies Using Citation Analysis Among Communication Journals." *Scientometrics* 81 (1): 157-175.

Patra, Swapan Kumar, Partha Bhattacharya, and Neera Verma. 2006. "Bibliometric Study of Literature on Bibliometrics." *DESIDOC Bulletin of Information Technology* 26 (1): 27-32.

Perez, Lance C., Stephen Cooper, Elizabeth K. Hawthorne, Susanne Wetzel, Brynieisson, Asim Gencer Gokce, John Impagliazzo, Youry Khmelevsky, Karl Klee, Margaret Leary, Amelia Philips, Norbert Pohlmann, Blair Taylor, and Shambhu Upadhyaya. 2011. "Information Assurance in Two- and Four-Year Institutions." Proceedings of the 16th Annual Conference on Innovation and Technology in Computer Science Education - Working group Reports, New York, New York, June 27-29, 39-53.

Peritz, Bluma C. 1980-81. "The Methods of Library Science Research: Some Results from a Bibliometric Survey." *Library Research* 2 (3): 251-678.

—. 1981. "Citation Characteristics in Library Science: Some Further Results from a Bibliometric Survey." *Library Research* 3 (1): 47-65.

Persson, Olle. 1994. "The Intellectual base and Research Fronts of *JASIS* 1986-1990." *Journal of the American Society for Information Science and Technology* 45 (1): 31-38.

—. 2000. "A Bibliometric View of Scientometrics (1978-1999)." [WWW]. Retrieved August 14, 2013, from the World Wide Web: http://www8.umu.se/inforsk/scientometrics/.

—. 2010. "Identifying Research Themes with Weighted Direct Citation Links." *Journal of Informatics* 4 (3): 415-422.

Pilkington, Alan, and Jack Meredith. 2009. "The Evolution of the Intellectual Structure of Operations Management-1980-2006: A Citation/Co-Citation Analysis." *Journal of Operations Management* 27 (3): 185-202.

Ponzi, Leonard J. 2002a. "The Evolution and Intellectual Development of Knowledge Management." Doctoral Dissertation, Long Island University.

—. 2002b. “The Intellectual Structure and Interdisciplinary Breadth of Knowledge Management: A Bibliometric Study of its Early Stage of Development.” *Scientometrics* 55 (2): 259-272.

Porche, Isaac R., Jerry M. Sollinger, Shawn McKay. 2011. *A Cyberworm that Knows No Boundaries*. Santa Monica, CA: RAND Corporation.http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.sum.pdf.

Porter, A.L., A.T. Roper T.W. Mason, F.A. Rossini, and J. Banks. 1991. *Forecasting and Management of Technology*. New York: Wiley.

Porter, Alan L., and Ismael Rafols. 2009. “Is Science Becoming More Interdisciplinary? Measuring and Mapping Six Research Fields Over Time.” *Scientometrics* 81 (3): 719-745.

Pouris, Anastassios. 2007. “Nanoscale Research in South Africa: A Mapping Exercise Based on Scientometrics.” *Scientometrics* 70 (3): 541-533.

Pratt, Jean A., Karina Hauser, and Cassidy R. Sugimoto. 2012. “Defining the Intellectual Structure of Information Systems and Related College of Business Disciplines: A Bibliometric Analysis.” *Scientometrics* 93 (2): 279-304.

Preneel, Bart. 2007. “An Introduction to Modern Cryptology.” In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 565-590. New York: Elsevier.

President Barack Obama. 2009. “Remarks by the President on Securing Our Nation's Cyber Infrastructure.” Washington, DC: Office of the President of the United States. Retrieved from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

President George W. Bush. *Comprehensive National Cybersecurity Initiative.* Washington, DC: White House, 2009. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

Price, Derek J. De Solla. 1961. *Science Since Babylon*. New Haven: Yale University Press.

—. 1963. *Little Science, Big Science*. New York, New York: Columbia University press.

—. 1965. “Networks of Scientific Papers.” *Science* 149 (3683). 510-15.

—. 1969. “Measuring the Size of Science.” *Proceedings of the Israel Academy of Sciences and Humanities* 4 (6): 98-111.

—. 1978. “Toward a Model for Scientific Indicators.” In *Toward a Metric of Science: The Advent of Scientific Indicators,* edited by Elkana, Yehuda, Joshua Lederberg, Robert K. Merton, Arnold Thackray, Harriet Zuckerman, 69-96. New York: John Wiley & Sons.

Ramos-Rodriguez, Rafael-António, and José Ruiz-Navarro. 2004. “Changes in the Intellectual Structure of Strategic Management Research: A Bibliometric Study of the Strategic Management Journal, 1980-2000.” *Strategic Management Journal* 25 (10): 981-1004.

van Raan, Anthony F.J., and R.J.W Tijssen. 1993. “The Neural Net of Neural Network Research: An Exercise in Bibliometric Mapping.” *Scientometrics* 26 (1): 169-192.

van Raan, Anthony F.J. 2001. “Bibliometrics and Internet: Some Observations and Expectations.” *Scientometrics* 50 (1): 59-63.

—. 2004. “Measuring Science.” In *Handbook of Quantitative Science and Technology Research: The Use of Publication and Patent Statistics in Studies of S&T Systems,* edited

by Moed, Henry F., Wolfgang Glanzel, and Ulrich Schmoch, 19-50. North-Holland: Kluwer Academic Publishers.

Reid, Edna F., and Hsinchun Chen. 2007. “Mapping the Contemporary Terrorism Research Domain.” *International Journal of Human-Computer Studies* 65 (1): 42-56.

Rice, R.E., Christine L. Borgam, Diane Bednarski, and P.J. Hart. 1989. “Journal-to-Journal Citation Data: Issues of Validity and Reliability.” *Scientometrics* 15 (3-4): 257-282.

Rip, A., and J.P. Courtial. 1984. “A Co-Word Maps of Biotechnology: An Example of Cognitive Scientometrics.” *Scientometrics* 6 (6): 381-400.

Rip, A. 1988. “Mapping of Science: Possibilities and Limitations.” In *Handbook of Quantitative Science and Technology,* edited by A.F.J van Raan, 253-273. North-Holland: Elsevier Science Publishers.

Rivest, Ronald L., Adi Shamir, and Len Adleman. 1978. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM* 21 (2): 120-126.

Larry Roberts. "The Arpanet and Computer Networks." In *Proceedings of the ACM Conference on The history of Personal Workstations* (HPW '86), edited by John R White and Kathi Anderson, 51-58. New York, NY: ACM, 1986.

Rohrabacher, Dana. 2013. *Cyber Attacks: An Unprecedented Threat to U.S. National Security: Hearing Before the Subcommittee on Europe, Eurasia, and Emerging Threats of the Committee on Foreign Affairs House of Representatives.* 113th Cong. 2013. Retrieved from http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg80123/pdf/CHRG-113hhrg80123.pdf.

Rorissa, Abebe, and Xiaojun Yuan. 2012. “Visualizing and mapping the Intellectual Structure of Information Retrieval.” *Information Processing and Management* 48 (1): 120-135.

Rosengren, K.E. “Sociological Aspects of the Literary System.” Doctoral Dissertation, Natur Och kultur, 1968.

Rowlands, I. 1999. “Patterns of Author Cocitation in Information Policy: Evidence of a Social, Collaborative and Cognitive Structure.” *Scientometrics* 44 (3): 533-546.

Sagar, Anil, B.S. Kademani, R.G. Garg, and Vijai Kumar. 2010. “Scientometric Mapping of Tsunami Publications: A Citation Based Study.” *Malaysian Journal of Library and Information Science* 15 (1): 23-40.

Saghafi, Saman, Maryam Asadi and Farideh Osareh. 2013. “Historiographical Map of Iranian Engineering Scientific Publications During 1939-2011.” *International Journal of Information Science and Management* 3 (2): 1-24.

Salamon, Lester M., Stephanie L. Geller, and Kasey L. Spence. 2009. "Impact of the 2007-2009 Economic Recession on Nonprofit Organizations." *The John Hopkins Listening Post Project* 14. http://www.thewritechoicenetwork.com/images/resources/Economic_Recession_on_Nonprofit_Organizations_John_Hopkins_University.pdf.

Sanz-Casado, Elias, J. Carlos Garcia-Zorita, Antonio Eleazar Serrano-Lopez, Birger Larsen, and Peter Ingwersen. 2013. “Renewable Energy Research 1995-2009: A case Study of Wind Power Research in EU, Spain, and Germany and Denmark.” Scientometrics 95 (1): 197-224.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M. 2009. "The Security of Practical Quantum Key Distribution." *Reviews of Modern Physics*, 81 (3): 1301-1350.

Schiffman, Susan, M. Lance Reynolds, and Forrest W. Young. 1981. *Introduction to Multidimensional Scaling: Theories, Methods, and Applications*. New York: Academic Press.

Schneier, Bruce. 2000. *Secrets and lies: Digital security in a networked world*. New York: Wiley.

—."The Psychology of Security." Last Modifed January 18, 2008. https://www.schneier.com/essay-155.html.

—. 2014. *Carry On: Sound Advice from Schneier on Security*. Indianapolis: Wiley.

Schubert, Andras, and Hajnalka Maczelka. 1993. "Cognitive Changes in Scientometrics During the 1980s, as Reflected by the Reference Patterns of its Core Journal." *Social Studies of Science* 23 (3): 571-581.

Schummer, Joachim. 2004. "Multidisciplinary, Interdisciplinary, and Patterns of Research Collaboration in Nanoscience and Nanotechnology." *Scientometrics* 59 (3): 425-465.

Schwechheimer, Holger, Mathias Winterhager. 2001. "Mapping Interdisciplinary Research Fronts in Neuroscience: A Bibliometric View to Retrograde Amnesia." *Scientometrics* 51 (1) 311-318.

"Scopus Facts and Figures." *Elsevier.com*. Last modified August 2013. http://cdn.elsevier.com/assets/pdf_file/0007/148714/scopus_facts_and_figures.pdf

Seglen, Per O. 1998. "Citation Rates and Journal Impact Factors are Not Suitble for Evaluation of Research." *Acta Orthop Scand* 69 (3): 224-229.

Shafique, Muhammad. 2013. "Thinking Inside the Box? Intellectual Structure of the Knowledge Base of Innovation Research (1988-2008)." *Strategic Management Journal* 34 (1): 62-93.

Shalini, R., and Janaki, A. 1985. "Facets of Information Science: A Study into its Composition Through Citation Analysis." *Library Science* 22 (2): 120-128.

Shannon, Claude E. 1945. *A Mathematical Theory of Cryptography.* Memorandum MM 45-110-02, September 1, 1945. Bell Laboratories.

—. 1949. "Communication Theory of Secrecy Systems." *Bell System Technical Journal.* 28 (4): 656-715.

Shao, Jufang, and Huiyun Shen. 2011. "The Outflow of Academic Papers from China: Why is it Happening and Can It Be Stemmed." *Learned Publishing* 24: 95-7.

Shea, Dana A. 2003. *Critical Infrastructure Control Systems and the Terrorist Threat*. Washington, D.C.: Congressional Research Service. http://fpc.state.gov/documents/organization/39559.pdf.

Simon, H. A. 1962. "The Architecture of Complexity." *Proceedings of the American Philosophical Society* 106 (6): 467-482.

—. 1896. *Problem Solving and Decision Making*.

Singh, Munindar P. "Toward a Science of Security." IEEE Computing and Society, Computing Now January, 2013. http://www.computer.org/portal/web/computingnow/archive/january2013.

Siponen, Mikko T., and Harri Oinas-Kukkonen. 2007. "A Review of Information Security Issues and Respective Research Contributions." *SIGMIS Database* 38 (1): 60-80.

Small, Henry, and Belver C. Griffith. 1974. “The Structure of Scientific Literature's I: Identifying and Graphing Specialties.” *Science Studies* 4 (1): 17-40.

—. 1973. “Cocitation in the Scientific Literature: A New Measure of the Relationship Between Two Documents.” *Journal of the American Society for Information Science* 24 (4): 265-269.

Small, Henry G. 1978. “Cited Documents as Concept symbols.” *Social Studies of Science* 8 (3): 327-340.

Smith, David. 2006. “New Information-Centric Approach to data Security: Increasing Threat Level Calls for a New Defense Strategy.” *Homeland Defense Journal* 4 (7): 48-50.

Smith, A. D. and W. T. Rupp. 2002. "Issues in Cybersecurity: Understanding the Potential Risks Associated with Hackers/Crackers." *Information Management and Computer Security* 10 (4): 178-183.

Smith, Linda. 1981. “Citation Analysis.” *Library Tends* 30 (1): 83-106.

Solms, Basie. 2001. “Information Security-A Multidimensional Discipline.” *Computers & Security* 20 (6): 504-08.

Solms, Rossouw von, and Johan van Niekerk. 2013. “From Information Security to Cyber Security.” *Computers and Security* 38 (October): 97-102.

Spasser, M.A. 1997. “Mapping the Terrain of Pharmacy: Co-Classification Analysis of the International Pharmaceutical Abstracts Database.” *Scientometrics* 39 (1): 77-97.

Stamp, Mark. 2011. *Information Security: Principles and Practice*. Hoboken, NJ: Wiley.

Stud, Pardeep, and Mike Thelwall. 2014. "Evaluating Altmetrics." *Scientometrics* 98 (2): 1131-1143.

Sun, Y. L., W. Yu, and Z. Han. 2006. "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks." *IEEE Journal on Selected Areas in Communications* 24 (2): 305-315.

Tabah, Albert N. 1999. “Literature Dynamics: Studies on Growth, Diffusion, and Epidemics.” *Annual Review of Information Science and Technology* 34: 249-286.

Templeton, T. Clay, and Kenneth R. Fleischmann. 2013. “Research Specialties as Emergent Phenomena: Connecting Emergence Theory and Scientometrics.” *iConference 2013 Proceedings*. https://www.ideals.illinois.edu/bitstream/handle/2142/42107/403.pdf?sequence=2.

Teixera, Aurora A.C. 2011. “Mapping the Invisible College(s) in the Field of Entrepreneurship.” *Scientometrics* 89 (1): 1-36.

Thewall, Mike, Stefanie Haustein, Vincent Lariviere, Cassidy R. Sugimoto. 2013. "Do Altmetrics Work? Twitter and Ten Other Social Web Services." *PLoS ONE* 8 (5): e64841. doi:10.1371/journal.pone.0064841.

Tsay, Ming-Yueh, Hong Xu, and Chia-Wen Wu. 2003. “Author Co-Citation Analysis of Semiconductor Literature.” *Scienometrics* 58 (3): 529-545.

Tsay, Ming-Yueh, and Yi-Jen Lin. 2009. “Scientometric Analysis of Transport Phenomenon Literature, 1900-2007.” *Malaysian Journal of Library and Information Science* 14 (3): 35-58.

United States. “The Comprehensive National Cybersecurity Initiative.” Executive Office of the President. Accessed on January 4, 2013. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

Vaughn, Rayford B., David A. Dampier, and Merill B. Warkentin. 2004. “Building an Information Education Program.” Proceedings of the First Annual Conference on Information Security Curriculum Development, New York , New York, 41-45.

Walke, Rajpal, and S.M. Dhawan. 2007. “Materials Science Research in India: Scientometric Analysis.” *DESIDOC Bulletin of Information Technology* 27 (1): 69-76.

Wallace, Danny P., and Susan Bonzi. 1985. “The Relationship Between Journal Productivity and Quality.” In ASIS 1985; Proceedings of the 48th ASIS Annual Meeting; Las Vegas, Nevada, October 20-24, 1985, vol. 22, edited by Carol A. Parkhurst, 193-196. White Plains, NY: Knowledge Industry Publications, Inc for the American Society for Information Science, 1985, 393.

Ware, Willis H. 1979. *Security Controls for Computer Systems: Report of Defense Science Board, Task Force on Computer Security*. Santa Monica, CA: RAND Corporation. http://www.rand.org/pubs/reports/R609-1/index2.html.

Weaver, Warren. 1948. Science and complexity. *American Scientist* 36: 536-544.

West. James A. 2003. “An Analysis of the Evolution of Instructional Technology as a Discipline.” Doctoral Dissertation, Northern Illinois University.

West, Ryan. 2008. “The Psychology of Security: Why Do Good Users Make Bad Decisions.” *Communications of the AMC* 51 (4): 34-40.

White, Howard D. 1981. “Cocited Author Retrieval Online: An Experiment with the Social Indicators Literature.” *Journal for the American Society for Information Science* 32 (1): 16-21.

—. 1983. “A Cocitation Map of the Social Indicators Movement.” *Journal for the American Society for Information Science* 34 (5): 307-312.

—. “Author Co-Citation Analysis: Overview and Defense.” In *Bibliometrics and Scholarly Communication*, Christine Borgman, 84-106. Newbury Park: Sage, 1990.

—. 2003. Author Cocitation Analysis and Pearson's *r*." *Journal of the American Society for Information Science and Technology* 54 (13): 1250-1259.

White, Howard D., and Belver C. Griffith. 1981. “Author Cocitation: A Literature Measure of Intellectual Structure.” *Journal of the American Society for Information Science and Technology* 32 (3): 163-171.

—. 1982. “Authors as Makers of Intellectual Space: Co-Citation in Studies of Science, Technology and Science.” *Journal of Documentation* 38 (4): 255-272.

White, Howard D., and Katherine W. McCain. 1998. “Visualizing a Discipline: An Author Co-Citation Analysis of Information Science, 1972-1995.” *Journal of the American Society for Information Science* 49 (4): 327-55.

Whiteman, Michael E., and Herbert J. Mattord. 2009. *Principles of Information Security* (3th ed.). Boston, Mass: Thomson Course Technology.

Whiteman, Michael E., and Herbert J. Mattord. 2011. *Roadmap to Information Security: For IT and Infosec Managers*. Boston, Mass: Thomson Course Technology.

Whiteman, Michael E., and Herbert J. Mattord. 2012. *Principles of Information Security* (4th ed.). Boston, Mass: Thomson Course Technology.

Wilson, Patrick. 1996. “The Future of Research in our Field.” In *Information science: From the development of the discipline to social interaction,* Johan Olaisen, Erland Munch-Petersen, and Patrick Wilson, 319-323. Oslo: Scandinavian University Press.

Wuegrer, Gerhard A., and Angela Elisabeth Smejkal. 2013. "The Knowledge Domain of the Academy of International Business Studies (AIB) Conferences: A Longitudinal Scienometric Perspective for the Years 2006-2011." *Scientometrics* (95) 2: 541-561.

Yan, Erlia, Ying Ding, and Qinghua Zhu. 2010. "Mapping Library and Information Science in China: A Coauthorship Network Analysis." *Scientometircs* 83 (1): 115-131.

Yerkey, Neil, and Maryruth Giogowski, 1989. "Bibliographic Scatter of Library and Information Science Literature." *Journal of Education for Library and Information Science* 30 (2): 90-101.

Yoo, Jun Yeong, Jae Yun Lee, and Sanghee Choi. 2013. "Intellectual Structure of Korean Theology 2000-2008: Presbyterian Theology Journals." *Journal of Information Science* 39 (3): 307-318.

Yoshihara, Toshi. 2001. *Chinese Information Warfare a Phantom Menace or Emerging Threat?* Carlisle, PA: Strategic Studies Institute, U.S. Army War College. http://carlisle-www.army.mil/usassi/ssipubs/pubs2001/chininfo/chininfo.htm.

Yost, Jeffrey R. 2007. "A History of Computer Security Standards." In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 595-620. New York: Elsevier.

Zhao, Dangzhi. 2009. "Mapping Library and Information Science: Does Field Delineation Matter?" *Journal of the American Society for Information Science and Technology* 46 (1): 1-11.

Zhao, Dangzhi, and Andreas Strotmann. 2008. "Comparing All-Author and First-Author Co-Citation Analyses of Information Science." *Jornal of Informetrics* 2 (3): 229-239.

—. 2008. "Evolution of Research Activities and Intellectual Influences in Information Science 1996-2005: Introducing Author Bibliographic-Coupling Analysis." *Journal of the American Society for Information Science and Technology* 59 (13): 2070-2086.

—. 2011. "Intellectual Structure of Stem Cell Research: A Comprehensive Author Co-Citation Analysis of a Highly Collaborative and Multidisciplinary Field." *Scientometrics* 87 (1): 115-131.

Zhao, Limei, and Qingpu Zhang. 2011. "Mapping Knowledge Domains of Chinese Digital Library Research Output, 1994-2010." *Scientometrics* 89 (1): 51-87.

Zhu, Wenjia, and Jiancheng Guan. 2013. "A Bibliometric Study of Service Innovation Research: Based on Complex Network Analysis." *Scientometrics* 94 (3): 195-216.

Zong, Qian-Jin, Hong-Zhou Shen, Qin-Jian Yuan, Xiao-Wei Hu, Zhi-Ping Hou, and Shun-Gu Deng. 2013. "Doctoral Dissertations of Library and Information Science in China: A Co-Word Analysis." *Scientometrics* 94 (2): 781-799.

Appendix A Historical Perspective of Information Security Research

1. Information Security Research: Before the Electronic Computer

Aside from a short history focusing on computer security in Whiteman and Mattord (2009), and a compilation of articles published in a handbook edited by Leeuw and Bergstra (2007), few histories have been written on information security. There have been some thorough histories, however, written about subdomains that fall within the information security specialty. For instance, Kahn (1996) covered a comprehensive history of cryptology and communications security, with a strong emphasis on their role in WWI, WWII, and the Cold War. With his focus on cryptology, Kahn (1996) was able to develop a history that goes back over 3000 years to such civilizations as Ancient Egypt. Whiteman and Mattord (2009) limited their historical coverage of information security to after the development of the electronic computer, while Leeuw and Bergstra (2007) begin at the Renaissance primarily focusing on cryptology, communications security, and computer security. Briefly addressed in this section is some background on information security concepts and a perspective on the history of information security with regard to some of its landmark events, publications, and researchers.

Cryptology, according to Kahn (1996), is the oldest and, as pointed out by Schneier (2000), still most vital information-centric technique for information security. As discussed in Smith (2006) and Ahmad, Ruighaver, and Teo (2005), an information-centric approach holds as its main focus the protection of information within an information system, as opposed to an infrastructure-centric approach which has as its main objective the protection of the medium carrying the information, be it, a scroll, file cabinet, computer system, or network. Cryptology seeks to make information recognizable to those authorized to know it, and unrecognizable to those who are not. This is accomplished, according to Stamp (2011), by using a cipher to encrypt

plaintext, and in turn, make it ciphertext. A cipher can also be known as a cryptosystem, and is a form of algorithm. An algorithm, in its most basic sense, is a set of instructions. Therefore, a cryptosystem is a set of instructions that indicates how to rearrange plaintext in such a way as to make it unrecognizable to adversaries. Plaintext is understandable text; it is the information that is to be hidden. Ciphertext is the result, text that has undergone encryption and is now unrecognizable to adversaries. The cipher key sets the cipher and gives the particular details of how the cipher can be used to reveal (i.e., decrypt) or secure (i.e., encrypt) information. Before moving on, it should be noted that cryptanalysis refers to the science of decrypting information in hidden messages, while cryptography is the science of encrypting messages to hide information.

Kahn (1996) dated the earliest attempts at cryptology back to ancient Egypt. Ancient Egyptians applied cryptography techniques to the hieroglyphic writings on the tombs of rulers and kings as a means to exalt power and prestige. Likewise, cryptography was used in ancient China, which went hand-in-hand with the ancient Chinese ideographic language, to conceal the meaning of words. Similar uses of cryptology were found in other ancient societies such as Mesopotamia, Assyria, Babylon, Greece, and Rome. Being that the majority of people in the ancient world were illiterate, cryptological techniques were not of much use and stood stagnant for thousands of years. Little is known about the ancient use of cryptology other than it was limited to simple substitution ciphers and served to support information confidentiality (i.e., keeping information secret).

It was not until Al-Kindi (801-873 AD), a ninth century Arab philosopher, published his *Treatise on Cryptanalysis* that cryptology became the focus of scientific inquiry (Mrayati, Alam, and at-Tayyan 2003). Al-Kindi introduced, for the first time, the use of statistical measures,

specifically frequency analysis, to decipher hidden text. Al-Kindi argued that besides the obvious semantic meaning behind linguistic symbolic characters, there was the grammatical structure and positioning of the linguistic characters, the interconnected relationship of which would still be present even if the characters were changed. Al-Kindi discovered, according to Mrayati, Alam, and at-Tayyan (2003) that if analyzed quantitatively, this underlying quantitative substrate of communication could be used to reveal enough meaning to decipher encrypted text. Unfortunately, Arab scholarship eventually waned and scientific coverage of cryptology did not see resurgence until the Italian Renaissance.

The Italian Renaissance (14th-16th century), with its combination of constant feuding and diplomatic maneuvering taking place between the Italian nation-states and the reemergence of scientific inquiry, was a perfect place for a scientific focus on cryptology to once again come to light. Secret communications, often using carriers on horseback delivering encrypted messages, were a key instrument for coordinating activities amongst the warring nation-states. The Renaissance set the stage for humanists to approach scientific inquiry on a much greater scale than the previous centuries. One particular Northern Italian polymath, Leon Battista Alberti, produced the publication, *Treatise on Ciphers* (1466), focusing on frequency analysis (Alberti, Buonafalce, Mendelsohn, and Kahn 1997). Alberti is credited, as noted by Kahn (1996), with the invention of the cipher disk, which led to highly complex polyalphabetic ciphers. A cyber disk was composed of two rotating disks on a single axis. On the circumference of those disks were alphabets; one disk's alphabet was plaintext while the other was ciphertext. Simply turning the cipher disk mechanized the process of transposing plaintext into ciphertext. This system led to polyalphabetic ciphers, that is, simultaneously using multiple ciphertext alphabets

in encryption. Polyalphabetic ciphers would stay relatively unbreakable for around 400 years (Kahn 1996).

The use of polyalphabetic ciphers and the introduction of electronic rotor machines led to highly complex encryption. At this point in history, cryptographers had an easier time than cryptanalysts. In fact, Auguste Kerckhoffs, a 19th century Dutch military and cryptology scholar, suggested, as part of his famous cryptography maxim, to let the enemy know the design of the cryptographic system, because if it is of any worth, it will not matter (Massey 1988). In other words, since encryption algorithms were thought to be undecipherable, the cipher key was the real important part of keeping a message secret. Later, a prominent early contemporary cryptologist, Claude Shannon (1949), would indeed prove that there was a mathematically unbreakable cryptographic algorithm called a one-time pad (to be discussed in later paragraphs).

Since monoalphabetic systems, (i.e., using a single alphabetic character for ciphertext substitution) was considered insecure, the only option was polyalphabetic systems. However, using multiple ciphertext alphabet characters in substitutions was very cumbersome. Bauer (2007) suggested that fruitful development and use of mechanical encryption devices did not happen until the discovery and wide use of electrical relay circuits. Technology permitted around the 1910s, and the most popular type of mechanical encryption device became the rotor. At first, rotors, according to Bauer (2007, 382), used simple substitution, that is, the "pairwise juxtaposition of plaintext symbols and ciphertext symbols". Soon, WWI pushed development and the electrically driven rotor was produced. The rotor machine used an array of wheels with electrical contact points all representing either plaintext or ciphertext maneuvered in such a way as to produce a substitution scheme that could exponentially increase in complexity as more

ciphertext wheels were added. The rotor made creating complex polyalphabetic codes less cumbersome.

Wireless radio communication, as discussed in Gleick (2011), was invented by Guglielmo Marconi just prior to 1900 and its widespread use during WWI made communication security a major concern. Radio facilitated easy long distance communication, nevertheless radio waves were not protected by any security mechanisms. Radio waves permeated the air and allowed anyone with a radio device to intercept messages. This realization prompted wide-scale government investment in cryptology, in particular, the use of electromechanical rotor cipher machines. The ENIGMA was one such machine developed by the German engineer Arthur Scherbius that was heavily used during WWI (Bauer 2007). The ENIGMA used electromechanically driven rotor cipher disks compressed into a small, portable machine that resembled a typewriter.

As indicated in Kahn (1996), cryptology's prominent role in WWI, is underscored in the deciphering of the Zimmerman Telegram which caused the U.S. to enter the war, shifting the tide of the war towards the Allies advantage. The Zimmerman Telegram was an encoded message sent to Mexico from Germany using wireless radio signals asking Mexico to invade the U.S. (at that time a neutral nation) as part of a German war strategy. The British were able to decipher the Zimmerman Telegram using stolen German military cipher key documents. The British warned the U.S., eventually causing the U.S. to enter the war on the side of the Allies. Breaking an ENIGMA code, such as in the Zimmerman Telegram, would not likely have been possible if not for the British getting hold of German military documents containing cipher keys.

It was not until 1938 that electromechanical cryptanalysis machines were built; for example, Marian Rejewski's Polish Cryptologic Bomb was used to assist mathematicians in

countering the advantage of electromechanical cryptographic devices. The Cryptologic Bomb drastically reduced the complexity of a secret code, as noted by Bauer (2007), by mechanically using brute force, (i.e. using a large number of possible keys until one combination worked). Alan Turing, a British mathematician working with British signals intelligence at Bletchley Park, created a similar device called the Bombe to counter the ENIGMA. Besides ENIGMA, Copeland (2007, 447) pointed out that the Nazis had developed a more technologically advanced cryptographic system using the Lorenz SZ40 cipher machine, referred to as "Tunny" by the British intelligence services at Bletchley Park. Tunny was carefully guarded by the Nazis and only used for encrypting communications between the highest echelon in the Nazi command. The Tunny system, a teleprinting machine, would send and receive messages via radio waves, and automatically encrypt outgoing messages and decrypt incoming messages before printing (Copeland 2007). British signals intelligence put a lot of resources into breaking Tunny and in the early 1940s. Thomas Flowers, a British engineer working at Bletchley Park, created Colossus, the first electronic programmable digital computer system. Colossus successfully assisted the British in decrypting Tunny messages.

In 1945, Claude Shannon, an American engineer working at Bell labs on behalf of U.S. intelligence services, published a classified paper titled, "A Mathematical Theory of Cryptography;" it was later republished in 1949 in a declassified version titled, "Communication Theory of Secrecy Systems". Shannon (1949) proved that one-time pads are theoretically completely secure if the key used is statistically random, uses the same number of characters as in the plaintext, is used only once, and stays secret. The one-time pad is immune from frequency analysis, since its randomness gives it a uniform frequency distribution. The key should only be used once before being discarded, thus establishing no pattern for cryptanalysts to reveal.

However, one-time pads required the distribution of an identical key to a receiver and a sender. This led to difficulty in coordinating the distribution of these one-time keys to geographically disbursed senders and receivers. The one-time pad moved the research problem of encryption from developing secure algorithms to focusing on secure key distribution. This problem caused the one-time pad to be used sparingly, only when the message was vital and there was no need for large-scale access to it.

2. Information Security Research: After the Electronic Computer

Whitman and Mattord (2009, 3) suggested, "the history of information security begins with the history of computer security." The development of electronic computers marked a shift in information security from focusing on securing information to primarily focusing on securing computer infrastructure. Computers were created to assist in the management and processing of large amounts of information produced during World War II. In the early to mid 1940s, according to Yost (2007, 597), the first digital computer named the Electronic Numerical Integrator and Computer (ENIAC) was built in the U.S. ENIAC was used for military ballistic missile calculations.

WWII drove initiatives for increased physical security measures to protect computers from physical threats such as sabotage and espionage. One particular fear that computer security researchers had was compromising emanations; that is, the heavy radiation emitted from early computers was thought to be detectable by enemies from a distance and able to be deciphered to reveal information. This fear became a reality in the 1950s, as pointed out by Yost (2007), when British intelligence was able to frequently eavesdrop on and decipher the electromechanical radiation emanating from computers at French embassies. Radiation eavesdropping was not always practical for the reason that one had to be in close physical proximity to detect the proper

amount of radiation. Yet, fear of this security problem drove the U.S. National Security Agency (NSA) to develop the first compromising emanations security standard, called TEMPEST. TEMPEST required steps to reduce and contain compromising emanations with computers that handled classified information. The TEMPEST standard was mostly maintained by building radiation shields around computers or placing the computers in secured facilities, termed Secure Compartmented Information Facilities (SCIF) (Yost 2007).

Aside from its data processing functions, electronic computers, were also developed to act as electronic file cabinets by functioning to store and make accessible a multitude of documents in the form of digital files. The physical security of information, often secret government and proprietary information, involved keeping documents in locked physical file cabinets, safes, and vaults. Similarly, the physical security of information, as it relates to computers, also required limiting physical access to these electronic files by physically isolating the computers, sometimes with armed guards, and placing them in SCIF (Whitman and Mattord 2009). The physical security of information held in computers has also included preventing access to a computer by creating a password-protected interface. These methods were not directly focused on securing the information in the computer as much as they were focused on securing access to the computer system itself. Physical security became more difficult as computer technology improved and more computers that are compact were built and widely distributed.

Physical security became less of an issue as new computer threats and vulnerabilities were realized with the development of digital computer network technology. Digital computer network technology largely began development in the U.S. during the 1950s when IBM and MIT were contracted by the U.S. Department of Defense to develop computer systems for a Semi-

Automatic Ground Environment (SAGE) system. Yost (2007, 600) described SAGE as "a complex system of radar and networked computers designed to provide early detection against enemy air attack". Around the same time, in the early 1960s, MIT's related project, Multiple Access Computer (MAC), introduced computer time-sharing technology. The modern day Internet is a product of computer time-sharing initiatives, which at first, sought to connect multiple distributed users to a single computer using telephone lines. The purpose of time-sharing, according to Yost (2007, 600), was to "more effectively utilize expensive processing and memory resources of computers". Soon after, the Department of Defense's Advanced Research Project Agency, led by researcher Larry Roberts, started to develop an extended network of computers for information sharing and management. The network was called the Advanced Research Project Agency Network (ARPANET) (DeNardis 2007).

The creation of large-scale networks influenced a change in the focus of information security back to an information-centric approach. DeNardis (2007) suggested that in the early later half of the twentieth century, the Cold War, marked by threats of widespread nuclear destruction in the U.S. homeland, impelled U.S. defense strategists to call for a more resilient information system to share and manage vital defense related information. The previous method of delivering magnetic computer tapes via postal mail was not efficient with regard to speed and not sufficient in the face of nuclear destruction. This led to the rise of wide area networks (WAN), for example, ARPANET. Between the 1970s and 1980s, according to Whitman and Mattord (2009), the use of ARPANET steadily grew, leading to the potential for misuse. Research conducted by Robert Metcalfe (1973), one of the inventors of the Ethernet, in his dissertation, titled *Packet Communication*, highlighted fundamental security issues with ARPANET. For instance, Metcalfe (1973) pointed to the potential for unauthorized access. The

extent of the concern surrounding ARPANET at this time, as outlined in Whitman and Mattord (2009, 5), included:

- Vulnerability of password structure and formats
- Lack of safety procedures for dial-up connections
- Nonexistent user identification and authorization to the system

Soon after, a landmark publication was produced by Bisbey and Hollingworth (1978) at the University of California for the Defense Advanced Research Projects Agency (DARPA), titled *Protection Analysis: Final Report*. Bisbey and Hollingworth (1978) investigated the vulnerabilities of operating systems and automatable techniques to detect such vulnerabilities.

It was not until the following year, 1979, which one of the most substantial changes would occur in information security. Confronted with culminating concerns about information security, due to quick advancements with digital computer network technology, the Department of Defense commissioned the RAND Corporation to perform research on the state of computer security. The RAND research group was headed by Willis Ware, a prominent researcher in computer science and information security. The RAND report, edited by Ware (1979) and, titled *Security Control for Computer Systems: Report of Defense Science Board Task Force on Computer Security*, would turn out to be, in Yost's (2007, 602) opinion, "by far the most important and thorough study on technical and operational issues regarding secure computing systems of its time period". Ware's (1979) conclusions focused on the change from closed computing environments to open computing environments. Distributed networks, especially WANs, are inherently less secure than isolated computer systems. Ware (1979, 1) pessimistically cautioned, "the expanded problems of security provoked by resource-sharing systems might be viewed as the price one pays for the advantages these systems have to offer". He also goes on to argue that these security challenges are "fundamentally a problem of protecting information" and

can be addressed with a shift from focusing on the computer and network infrastructure, which are intrinsically vulnerable, to focusing on the information within these systems (Ware 1979, 1).

Yet, the convenience and efficiency of WANs for managing and interacting with information began persuading organizations to allow remote access to sensitive information. This marked a turn from closed information systems, highlighted by isolated computers and private networks, to open information systems, often utilizing WANs to allow easy remote access to more users. The move towards system openness relieved some of the security focus on access to information systems and placed it back on accessing information instead. As an information-centric technique, Gollman (2007) discussed multilevel security being developed during the 1970s and 1980s for military purposes to delineate access to information within an open information system. Document security levels, the designation of the level of sensitivity regarding information (e.g. unclassified, confidential, secret, top secret), along with security clearance, (i.e., the level of access to sensitive information a user is allowed) all facilitated an open system where users could freely access the information system itself, but only have access to information within it for which they are authorized. Prominent information security models such as the Bell-LaPadula model were designed to support these multilevel systems.

Information-centric approaches (e.g., cryptography) steadily advanced alongside these other information security techniques. For example, Horst Feistel, a researcher at IBM, led a team of researchers in developing a data encryption system called the Demon, that later became known as Lucifer. Feistel (1973) published some of his work on Lucifer in an article titled, “Cryptography and Computer Privacy”. In 1976, Lucifer would become the Data Encryption Standard (DES) adopted by the National Bureau of Standards. Around the same time, Whitfield Diffie and Martin Hellman (1976) published a landmark paper titled, “New Directions in

Cryptology". Diffie and Hellman (1976) developed a theoretical solution to the long held problem facing the one-time pad, namely secret key distribution. Their solution, called public-key cryptography, involved splitting the standard symmetric key into an asymmetric, mathematically linked set of keys, one public and one private. Public-key encryption used a trapdoor, one way function, one that can only simply be solved in one direction but exceedingly difficult, if not impossible, to solve in the other. Public-key algorithms would go on to play a vital role in many other widely used cryptosystems, applications, and protocols, including many trusted Internet standards. Building off Diffie and Hellman's (1976) theoretical work, Rivest, Shamir, and Adleman (1978) created a more robust, testable algorithm, labeled RSA. RSA made public-key encryption workable and it sprouted into RSA Data Security, a successful business venture for Rivest, Shamir, and Adleman.

Up until the late 1980s and early 1990s, information security was focused on government and business initiatives, since most information assets were held by these institutions. Major networking between institutions and between institutions and individual people would not take hold until the 1990s with the rise of the Internet and personal computers. The Internet's insecurity is largely a product of security being a low priority during the rush to its widespread deployment. Whitman and Mattord (2009, 7-8) articulate the reason for the contemporary Internet security dilemma:

> Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats.

3. Information Security Research: In the Networked Society

Computers and the Internet have been around for decades, but the dramatic extent to which they have become integrated into the very fabric of society has only taken place over the last decade. This social integration has made information security a problem at the very heart of society. The term ‘cyberspace’ has come to be used to refer to this complex integration of information technology and society. The Department of Defense (2012, II-9) defines cyberspace as follows:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

One milestone, which serves to distinguish the current historical period from earlier ones is the designation of cyberspace, by the Department of Defense (2011), as a new domain of war. Cyberspace's designation as a new domain of war underscores the dramatic extent to which society’s most vital social infrastructures and functions have become dependent on information technology. Such dependence, as addressed by President Obama (2009), has led to information security being of top strategic national importance, as well as being important in the everyday lives of individuals.

Research by Kuel (2007) discussed the increased integration of computer systems, networks, and critical infrastructure into complex cyber systems that support society’s most critical functions. These cyber systems process information for large scale industrial and critical infrastructure tasks, for example, energy creation and distribution, water treatment facilities, transportation, telecommunications, and military logistics. Shea (2003) explained that the nation’s critical infrastructure is managed by certain cyber systems called Supervisory Control

and Data Acquisition Systems (SCADA) and Distributed Control Systems (DCS). SCADA and DCS, to a great degree, now function independent of human interaction and are networked globally for remote control. SCADA systems and DCS have taken center stage in information security research for national defense and homeland security. Damage to these systems, as pointed out by Shea (2003), could cause severe harm to society. In one example, Porche, Sollinger, and McKay (2011) report that Stuxnet, a cyber worm, intentionally caused physical damage and crippled a nuclear facility in Natanz, Iran in 2010. The integrity of information that regulated the Natanz nuclear reactor's centrifuges was intentionally compromised (i.e., sabotage) leading to severe damage.

Realizing that information security is of strategic national importance, President George W. Bush, in 2008, issued *Homeland Security Presidential Directive 23/National Security Presidential Directive 54* (HSPD 23/NSPD 54), which outlined U.S. cyber security goals and delegated responsibilities for meeting those goals to the Department of Homeland Security (DHS), the Office of Management and Budget, and the NSA. HSPD 23/NSPD 54 is mostly classified except for the portions that were included in the Executive Office of the President of the United States's (2010) *Comprehensive National Cybersecurity Initiative* (CNCI). In 2009, the Executive Office of the President of the United States published, *Cyberspace Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure,* which led the Cybersecurity Information Assurance Interagency Working Group (CIAIWG) (2010), working through the National Science and Technology Council (NSTC), to investigate conducting and sponsoring R&D in cybersecurity. NSTC (2011) argued that up until this point, cybersecurity was being dealt with by a piecemeal strategy; that is, patching problems after they occur and not taking a systemic approach.

The overall national research strategy induced by the NSTC (2011) was to build a *Trustworthy Cyberspace*. NSTC (2011) aimed to accomplish this through a four part strategic agenda to guide the scientific communities in industry and academia. The NSTC (2011) agenda included:

1. Inducing Change: Using game-changing R&D themes focused at figuring out the fundamental causes of threats and developing radically different techniques to assure the security of critical cyber systems and infrastructure (3).
2. Accelerating Transition to Practice: Developing efforts to promote quick and efficient adoption and measurement of efficacy of the new approaches resulting from these research themes (14).
3. Developing Scientific Foundations: Promote the move of cybersecurity to a scientific field highlighted by "the discovery of scientific laws, hypothesis testing, repeatable experimental design, standardized data-gathering methods, metrics, common terminology, and critical analysis that engenders reproducible results and rationally based conclusions." (3, 10).
4. Maximizing Research Impact: Supporting integration between game-changing R&D themes, including cooperation between industries, government and private sector, national priorities, and international partners (12).

At a more granular level, CIAIWG (2010) had developed three specific research themes that are to be approached by the scientific community. These themes were:

1. Moving Target: Developing technologies that are diverse, shift and change over time increasing complexity and cost for attackers, limit exposure of vulnerabilities to attack, and increase resilience (3).
2. Tailored Trustworthy Spaces: Create flexible, adaptive, customizable, negotiated, distributed trust environments, supporting functional and policy requirements that are produced from a wide spectrum of activities in the face of evolving threats, while recognizing and evolving based on feedback from the user and the user's context (7).
3. Cyber Economic Incentives: Recognize that existing cybersecurity solutions are not being used, because they do not align with objectives, and resources are not being properly allocated. Develop a scientific framework that will enable sound metrics for cost/risk analysis in order to incentivize cybersecurity practices by building a strong business case for improved cybersecurity mechanisms and processes (12).

In addition to the above R&D strategies and themes promoted by NSTC (2011) and CIAIWG (2010), the NSA and DHS had created a joint initiative, called the National Center of Academic Excellence in IA Education and Research. The goal of their initiative is to promote

higher education and research into information security by developing partnerships and promoting research agendas that align to national information security needs. Collaborative government efforts, led by DHS, have outlined detailed public and private cybersecurity R&D agendas based on a list of 11 hard research problems that DHS (2009) had determined will have the greatest impact on information security. According to DHS (2009), research aimed at these hard problems will be the focus of federal and private funding. These 11 hard problems were as follows:

1. Scalable Trustworthy Systems (including systems architecture and requisite development technology)
2. Enterprise-Level Metrics (including measures of overall system trustworthiness)
3. System Evaluation Life Cycle (including approaches for sufficient assurance)
4. Combating Insider Threats
5. Combating Malware and Botnets
6. Global-Scale Identity Management
7. Survivability of Time-Critical Systems
8. Situational Understanding and Attack Attribution
9. Provenance (relating to information, systems, and hardware)
10. Privacy-Aware Security
11. Usability Security (DHS 2009, vii)

In the current information age, information is the lifeblood of society. It is no wonder why government has taken the initiative to frame and promote the information security research agenda. Information security research in this decade, as in previous decades, will continue to be shaped by social needs as expressed by industry and government.

References

Ahmad, Atif, A.B. Ruighaver, W.T. Teo. 2005. "An Information-Centric Approach to Data Security in Organizations." Proceedings at the TENCON 2005-2005 IEEE Region 10 Conference, Melbourne, Qld, November 21-25, 21-24.

Alberti, Leon Battista, Augusto Buonafalce, Charles J. Mendelsohn, and David Kahn. 1997. *ATreatise on Ciphers*. Torino: Galimberti.

Bauer, Friedrich L. 2007. "Rotor Machines and Bombes." In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 382-445. New York: Elsevier.

Bisbey, Richard., and Denise Hollingworth. 1978. "Protection Analysis: Final Report." Technical Report, University of California. http://csrc.nist.gov/publications/history/bisb78.pdf.

Copeland, Jack B. 2007. "Tunny and Colossus: Breaking the Lorenz Schlusselzusatz Traffic." In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 447-476. New York: Elsevier.

Cybersecurity Information Assurance Interagency Working Group. 2010. *Cybersecurity Game-Change Research & Development Recommendations.* Washington, D.C: Federal Networking and Information Technology Research and Development Program. http://www.nitrd.gov/pubs/CSIA_IWG_%20Cybersecurity_%20GameChange_RD_%20Recommendations_20100513.pdf.

DeNardis, Laura. 2007. "A History of Internet Security." In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 681-702. New York: Elsevier.

Department of Defense. 2011. *Strategy for Operating in Cyberspace*. Washington, DC: U.S.Department of Defense. Retrieved from http://www.defense.gov/news/d20110714cyber.pdf.

—. 2012. *Joint Publication 3-13: Information Operations*. Washington, DC: Department of Defense.

Department of Homeland Security. 2009. *A Roadmap for Cybersecurity Research*. Ft. Belvoir: Defense Technical Information Center. http://handle.dtic.mil/100.2/ADA529806.

Diffie, Whitfield, and Martin Hellman. 1976. "New Directions in Cryptology." *IEEE Transactions on Information Theory* 22 (6): 644-54.

Executive Office of the President of the United States. 2009. *Cyberspace Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, DC: Executive Office of the President of the United States. http://purl.access.gpo.gov/GPO/LPS118258.

—. 2010. *The Comprehensive National Cybersecurity Initiative*. Washington, D.C.: Executive Office of the President of the United States. http://purl.fdlp.gov/GPO/gpo6112.

Feistel, Horst. 1973. "Cryptography and Computer Privacy." *Scientific America* 228 (5): 15-23.

Gleick, James. 2011. *The Information: A History, A Theory, A flood*. New York: Pantheon Books.

Gollmann, Dieter. 2007. "Security Models." In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 623-635. New York: Elsevier.

Homeland Security Presidential Directive 23/National Security Presidential Directive 54 (January 2008)

Kahn, David. 1996. *The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet*. New York, NY: Scribner.

Kuehl, Dan. 2007. "The Information Revolution and the Transformation of Warfare." In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 821-831. New York: Elsevier.

Leeuw, Karl de., and Jan Bergstra. 2007. *The History of Information Security: A Comprehensive Handbook*. New York: Elsevier.

Massey, James L. 1988. "An Introduction to Contemporary Cryptology." *Proceeding of the IEEE* 76 (5): 533-49.

Metcalfe, Robert M. "Packet communication." Doctoral Dissertation, Massachusetts Institute of Technology, 1973. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=AD0771430.

Mrayati, Mohammed, Yahya Meer Alam, and M. Hassan at-Tayyan. 2003. *al-Kindi's Treatise on Cryptanalysis.* trans. Said M. al-Asaad. Vol. 1 of the *Arabic Origins of Cryptology. Riyadh: King Faisal Center for Research and Islamic Studies.*

National Science and Technology Council. 2011. *Trustworthy cyberspace strategic plan for the Federal Cyberspace Research and Development Program*. Washington, D.C.: Executive Office of the President of the United States. http://www.nitrd.gov/subcommittee/csia/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf.

Porche, Isaac R., Jerry M. Sollinger, Shawn McKay. 2011. *A Cyberworm that Knows No Boundaries*. Santa Monica, CA: RAND Corporation.http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.sum.pdf.

President Barack Obama. 2009. "Remarks by the President on Securing Our Nation's Cyber Infrastructure." Washington, DC: Office of the President of the United States. Retrieved from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

Rivest, Ronald L., Adi Shamir, and Len Adleman. 1978. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM* 21 (2): 120-126.

Schneier, Bruce. 2000. *Secrets and lies: Digital security in a networked world*. New York: Wiley.

Shannon, Claude E. 1945. *A Mathematical Theory of Cryptography.* Memorandum MM 45-110-02, September 1, 1945. Bell Laboratories.

—. 1949. "Communication Theory of Secrecy Systems." *Bell System Technical Journal.* 28 (4): 656-715.

Shea, Dana A. 2003. *Critical Infrastructure Control Systems and the Terrorist Threat*. Washington, D.C.: Congressional Research Service. http://fpc.state.gov/documents/organization/39559.pdf.

Stamp, Mark. 2011. *Information Security: Principles and Practice*. Hoboken, NJ: Wiley.

Ware, Willis H. 1979. *Security Controls for Computer Systems: Report of Defense Science Board, Task Force on Computer Security*. Santa Monica, CA: RAND Corporation. http://www.rand.org/pubs/reports/R609-1/index2.html.

Whiteman, Michael E., and Herbert J. Mattord. 2009. *Principles of information security* (3th ed.). Boston, Mass: Thomson Course Technology.

Yost, Jeffrey R. 2007. "A History of Computer Security Standards." In *The History of Information Security: A Comprehensive Handbook,* edited by Karl de Leeuw and Jan Bergstra, 595-620. New York: Elsevier.

Appendix B Top 100 Highest Cited Documents

Document	f	Document	f	Document	f
Shamir 1979	374	Campbell	55	Boneh 2008	38
Diffie	272	D'Arcy	54	Lowe	38
Rivest	236	Bulgurcu	53	Paulson	38
Boneh 2004	218	Burrows	53	Rackoff	38
Menezes	143	Fiat	53	Stone-Gross	38
Bellare 1993	134	Messerges	53	Zhou	38
Dolev	130	Straub 1990	53	Blanchet	37
Zhu 2003	123	Cramer	51	Dodis	37
Eschenauer	121	Paxson	51	Foster	37
Koblitz	118	Perrig	51	Meadows	37
Goldwasser 1984	103	Ferraiolo	50	Chan	36
Waters	102	Akyildiz 2002a	48	Chaum 1991	36
Pointcheval	96	Chaum 1985	48	Cox	36
Goldwasser 1988	90	Elgamal	48	Enck	36
Straub 1998	84	Raya	48	Halderman	36
Mchugh	83	Avizienis	47	Herath	36
Liu	82	Josang	47	Hwang	36
Akyildiz 2002b	81	Dhillon	46	Jung	36
Lamport	79	Armando	45	Klein	36
Du	76	Xiong	45	Paillier	36
Bellare 2003a	71	Boneh 2003	44	Abadi 1993	35
Boneh 2001	69	Ammann	43	Abadi 2002	35
Stoica	69	Lee	43	Denning	35
Newsome	68	Gu	42	Lippmann	35
Chaum 1981	60	Lie	42	Steiner	35
Chen	60	Ateniese 2000	41	Valdes	35
Cavusoglu	59	Boneh 2005	41	Barham	34
Goldreich	59	Dunlap	41	Bellare 2003b	34
Gordon	58	Lin	40	Reiter	34
Sandhu	58	Sheyner	40	Rosenberg	34
Ristenpart	57	Eskin	39	Yu	34
Shamir 1985	57	Jonsson	39	Zhu 2004	34
Goyal	56	Needham	39		
Groth	56	Ateniese 2006	38		

Appendix C Top 100 Highest Frequency Keywords

Keyword	f	Keyword	f	Keyword	f
Computer Network Security	27279	Architecture	2866	Enterprise	1578
Wireless	12027	Wireless TeleCommunications Systems	2619	Topology	1535
Internet Protocols	11038	Cyber	2444	Media	1526
Internet	9286	Platform	2300	Malware	1524
Cryptography	8800	Smart	2255	Bandwidth	1501
Authentication	7708	Computer Simulation	2248	Signature	1486
Access Control	7664	Public Key Cryptography	2222	Intelligent	1482
Applications	6662	Encryption	2190	Requirement	1467
Mobile	6485	Intrusion	2118	Training	1441
Privacy	6128	Classification	2077	Identity-Based	1388
Communications	5819	Learning	2057	Hash	1383
Computer Security	5493	Trust	2026	Servers	1377
Image	5377	IP	2003	Attackers	1353
Environment	5313	Grid	1990	Education	1332
Technology	5309	Information Systems	1947	Students	1328
Security Systems	5296	Distributed Computer Systems	1886	Integrity	1311
Detection	5255	Cloud	1852	Industry	1305
Methodology	5184	Embedded	1846	Vector	1294
Computer Crime	5023	Integration	1825	Scalable	1284
Humans	4786	Information Management	1800	Denial	1275
Attack	4698	Monitoring	1785	Surveillance	1248
Rights	4409	Watermarking	1774	Automation	1245
Intrusion Detection System	4349	Electronic Commerce	1749	Protection	1242
Malicious	4239	United States	1741	Reliability	1239
Information Technology	4209	Mining	1722	Semantics	1238
Software	4181	Strategies	1674	P2P	1221
Infrastructure	3842	RFID	1668	Healthcare	1220
Web	3813	Speed	1661	Vulnerabilities	1213
Management	3757	Standards	1641	Cyber Security	1206
Information Security	3686	Availability	1637	Firewall	1187
Confidentiality	3550	Biometrics	1618		
Design	3428	Anonymity	1604		
Computer Science	3073	Mathematical Models	1596		
Medical Records Systems	3000	Costs	1594		
Key	2908	Optimization	1590		

Appendix D List of Top 100 Highest Cited Document

Abadi, Martın, and Phillip Rogaway. 2002. "Reconciling Two Views of Cryptography."*Journal of Cryptology* 15 (2): 103-127.

Abadi, Martin, Michael Burrows, Butler Lampson, and Gordon Plotkin. 1993. "A Calculus for Access Control in Distributed Systems." *ACM Transactions on Programming Languages and Systems (TOPLAS)* 15 (4): 706-734.

Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. 2002a. "A Survey on Sensor Networks." *Communications magazine, IEEE* 40 (8): 102-114.

Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. 2002b. "Wireless Sensor Networks: A Survey." *Computer Networks* 38 (4): 393-422.

Ammann, Paul, Duminda Wijesekera, and Saket Kaushik. "Scalable, Graph-Based Network Vulnerability Analysis." In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 217-224. ACM, 2002.

Armando, Alessandro, David Basin, YOhan Boichut, Yannick Chevalier, Luca Compagna, Jorge Cuellar, Pierre C. Hankes Drielsma, Pierre C. Heám, Olga Kouchnarenko, Jacapo Mantovani, Sebastian Mödersheim, David von Oheimb, M. Rusinowitch, Judson Santiago, Mathieu Turuani, Luca Viganò, and Laurent Vigneron. "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications." In *Proceedings of the 17th International Conference on Computer Aided Verification* (CAV'05), Kousha Etessami and Sriram K. Rajamani (Eds.). Springer-Verlag, Berlin, Heidelberg, 281-285, 2005.

Ateniese, Giuseppe, Kevin Fu, Matthew Green, and Susan Hohenberger. 2006. "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage." *ACM Transactions on Information and System Security (TISSEC)* 9 (1): 1-30.

Ateniese, Giuseppe, Jan Camenisch, Marc Joye, and Gene Tsudik. "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme." In *Advances in Cryptology—CRYPTO 2000*, 255-270. Springer Berlin Heidelberg, 2000.

Avizienis, Algirdas, J-C. Laprie, Brian Randell, and Carl Landwehr. 2004. "Basic Concepts and Taxonomy of Dependable and Secure Computing." *IEEE Transactions on Dependable and Secure Computing* 1 (1): 11-33.

Barham, Paul, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, and Andrew Warfield. 2003. "Xen and the Art of Virtualization." *ACM SIGOPS Operating Systems Review* 37 (5): 164-177.

Bellare, Mihir, Daniele Micciancio, and Bogdan Warinschi. "Foundations of group signatures: Formal definitions, Simplified Requirements, and a Construction Based on General Assumptions." In *Advances in Cryptology—Eurocrypt 2003*, 614-629. Springer Berlin Heidelberg, 2003a.

Bellare, Mihir, Chanathip Namprempre, David Pointcheval, and Michael Semanko. 2003b. "The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme." *Journal of Cryptology* 16 (3): 185-215.

Bellare, Mihir, and Phillip Rogaway. 1993. *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*. Yorktown Heights, N.Y.: IBM T.J. Watson Research Center.

Blanchet, Bruno, Martín Abadi, and Cédric Fournet. 2008. "Automated Verification of Selected Equivalences for Security Protocols." *The Journal of Logic and Algebraic Programming* 75 (1): 3-51.

Boneh, Dan, and M. Franklin. "Identity-Based Encryption from the Weil Pairing." In *Advances in Cryptology—CRYPTO 2001*, pp. 213-229. Springer Berlin Heidelberg, 2001.

Boneh, Dan, Craig Gentry, Ben Lynn, and Hovav Shacham. "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps." In *Advances in cryptology—EUROCRYPT 2003*, 416-432. Springer Berlin Heidelberg, 2003.

Boneh, Dan, Xavier Boyen, and Hovav Shacham. "Short Group Signatures." In *Advances in Cryptology–CRYPTO 2004*, 41-55. Springer Berlin Heidelberg, 2004.

Boneh, Dan, Xavier Boyen, and Eu-Jin Goh. "Hierarchical Identity Based Encryption with Constant Size Ciphertext." In *Advances in Cryptology–EUROCRYPT 2005*, 440-456. Springer Berlin Heidelberg, 2005.

Boneh, Dan, and Xavier Boyen. 2008. "Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups." *Journal of Cryptology* 21 (2): 149-177.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS quarterly* 34 (3): 523-548.

Burrows, Michael, Martin Abadi, and Roger M. Needham. 1989. "A Logic of Authentication." *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 426 (1871): 233-271.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market." *Journal of Computer Security* 11 (3): 431-448.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. 2004. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers." *International Journal of Electronic Commerce* 9 (1): 70-104.

Chan, Haowen, Adrian Perrig, and Dawn Song. "Random Key Predistribution Schemes for Sensor Networks." In *Proceedings of 2003 Symposium on Security and Privacy*, 197-213. IEEE, 2003.

Chaum, David L. 1981. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms." *Communications of the ACM* 24 (2): 84-90.

Chaum, David L. 1985. "Security Without Identification: Transaction Systems to Make Big Brother Obsolete." *Communications of the ACM* 28 (10): 1030-1044.

Chaum, David, and Eugène Van Heyst. "Group signatures." In *Advances in Cryptology—EUROCRYPT'91*, 257-265. Springer Berlin Heidelberg, 1991.

Chen, Brian, and Gregory W. Wornell. 2001. "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding." *IEEE Transactions on Information Theory* 47 (1): 1423-1443.

Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, and Talal Shamoon. 1997. "Secure Spread Spectrum Watermarking for Multimedia." *IEEE Transactions on Image Processing* 6 (12): 1673-1687

Cramer, Ronald, and Victor Shoup. 2003. "Design and Analysis of Practical Public-Key Encryption Schemes Secure Against Adaptive Chosen Ciphertext Attack." *SIAM Journal on Computing* 33 (1): 167-226.

D'Arcy, John, Anat Hovav, and Dennis Galletta. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach." *Information Systems Research* 20 (1): 79-98.

Denning, Dorothy E. 1976. "A Lattice Model of Secure Information Flow."*Communications of the ACM* (19) 5: 236-243.

Dhillon, Gurpreet, and James Backhouse. 2001. "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives." *Information Systems Journal* 11 (2): 127-153.

Diffie, Whitfield, and Martin E. Hellman. 1976. "New Directions in Cryptography."*Information Theory, IEEE Transactions on* 22 (6): 644-654.

Dodis, Yevgeniy, Leonid Reyzin, and Adam Smith. "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and other Noisy Data." In *Advances in cryptology-Eurocrypt 2004*, 523-540. Springer Berlin Heidelberg, 2004.

Dolev, Danny, and Andrew C. Yao. 1983. "On the Security of Public Key Protocols". *IEEE Transactions on Information Theory* 29 (2): 198-208.

Du, Wenliang, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, Jonathan Katz, and Aram Khalili. 2005. "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks." *ACM Transactions on Information and System Security (TISSEC)* 8 (2): 228-258.

Dunlap, George W., Samuel T. King, Sukru Cinar, Murtaza A. Basrai, and Peter M. Chen. 2002. "ReVirt: Enabling Intrusion Analysis Through Virtual-Machine Logging and Replay." *ACM SIGOPS Operating Systems Review* 36 (SI): 211-224.

ElGamal, Taher. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." In *Advances in Cryptology*, 10-18. Springer Berlin Heidelberg, 1985.

Enck, William, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol Sheth. 2010. "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones." *OSDI*, 10: 1-6.

Eschenauer, Laurent, and Virgil D. Gligor. "A Key-Management Scheme for Distributed Sensor Networks." In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 41-47. ACM, 2002.

Eskin, Eleazar, Andrew Arnold, Michael Prerau, Leonid Portnoy, and Sal Stolfo. 2002. "A Geometric Framework for Unsupervised Anomaly Detection." In *Applications of Data Mining in Computer Security*, 77-101. Springer US, 2002.

Ferraiolo, David F., Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. 2001. "Proposed NIST Standard for Role-Based Access Control." *ACM Transactions on Information and System Security (TISSEC)* 4 (3): 224-274.

Fiat, Amos, and Adi Shamir. "How to prove yourself: Practical Solutions to Identification and Signature Problems." In *Advances in Cryptology—CRYPTO'86*, 186-194. Springer Berlin Heidelberg, 1987.

Foster, Ian, Carl Kesselman, and Steven Tuecke. 2001. "The Anatomy of the Grid: Enabling Scalable Virtual Organizations." *International Journal of High Performance Computing Applications* 15 (3): 200-222.

Goldreich, Oded, Silvio Micali, and Avi Wigderson. 1991. "Proofs That Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems."*Journal of the ACM (JACM)* 38 (3): 690-728.

Goldwasser, Shafi, and Silvio Micali. 1984. "Probabilistic Encryption." *Journal of Computer and System Sciences* 28 (2): 270-299.

Goldwasser, Shafi, Silvio Micali, and Ronald L. Rivest. 1988. "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks." *SIAM Journal on Computing* 17 (2): 281-308.

Gordon, Lawrence A., and Martin P. Loeb. "The Economics of Information Security Investment." *ACM Transactions on Information and System Security (TISSEC)* 5 (4): 438-457.

Goyal, Vipul, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data." In *Proceedings of the 13th ACM Conference on Computer and communications security*, 89-98. ACM, 2006.

Groth, Jens, and Amit Sahai. "Efficient Non-Interactive Proof Systems for Bilinear Groups." In *Advances in Cryptology–EUROCRYPT 2008*, 415-432. Springer Berlin Heidelberg, 2008.

Gu, Guofei, Roberto Perdisci, Junjie Zhang, and Wenke Lee. 2008. "BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection." In *USENIX Security Symposium*, 139-154.

Halderman, J. Alex, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. 2009. "Lest We Remember: Cold-Boot Attacks on Encryption Keys."*Communications of the ACM* (52) 5: 91-98.

Herath, Tejaswini, and H. Raghav Rao. 2009. "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organizations." *European Journal of Information Systems* 18 (2): 106-125.

Hwang, Min-Shiang, and Li-Hua Li. 2000. "A New Remote User Authentication Scheme Using Smart Cards." *IEEE Transactions on Consumer Electronics* 46 (1): 28-30.

Jonsson, Erland, and Tomas Olovsson. 1997. "A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior." *IEEE Transactions on Software Engineering* 23 (4): 235-245.

Jøsang, Audun, Roslan Ismail, and Colin Boyd. 2007. "A Survey of Trust and Reputation Systems for Online Service Provision." *Decision Support Systems* 43 (2): 618-644.

Jung, Jaeyeon, Balachander Krishnamurthy, and Michael Rabinovich. "Flash crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites." In *Proceedings of the 11th International Conference on World Wide Web*, 293-304. ACM, 2002.

Klein, Gerwin, Kevin Elphinstone, Gernot Heiser, June Andronick, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood. "SeL4: Formal Verification of an OS Kernel." In *Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles*, 207-220. ACM, 2009.

Koblitz, Neal. 1987. "Elliptic Curve Cryptosystems." *Mathematics of computation* 48 (177): 203-209.

Lamport, Leslie. 1981. "Password Authentication with Insecure Communication."*Communications of the ACM* 24 (11): 770-772.

Lee, Wenke, and Salvatore J. Stolfo. 2000."A Framework for Constructing Features and Models for Intrusion Detection Systems." *ACM transactions on Information and system security (TISSEC)* 3 (4): 227-261.

Lie, David, Chandramohan Thekkath, Mark Mitchell, Patrick Lincoln, Dan Boneh, John Mitchell, and Mark Horowitz. 2000. "Architectural Support for Copy and Tamper Resistant Software." *ACM SIGPLAN Notices* 35 (11): 168-177.

Lin, Xiaodong, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen. 2007. "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications." *IEEE Transactions on Vehicular Technology* 56 (6): 3442-3456.

Lippmann, Richard P., David J. Fried, Isaac Graf, Joshua W. Haines, Kristopher R. Kendall, David McClung, R.K. Cunningham, S.E. Webster, D. Wyschogrod, M.A. Zissman, and Dan Weber. 2000. "Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection Evaluation." In *DARPA Information Survivability Conference and Exposition, 2000. DISCEX'00. Proceedings*, 2, 12-26. IEEE, 2000.

Liu, Donggang, Peng Ning, and Rongfang Li. 2005. "Establishing Pairwise Keys in Distributed Sensor Networks." *ACM Transactions on Information and System Security (TISSEC)* 8 (1): 41-77.

Lowe, Gavin. "Breaking and Fixing the Needham-Schroeder Public-Key Protocol Using FDR." In *Tools and Algorithms for the Construction and Analysis of Systems*, 147-166. Springer Berlin Heidelberg, 1996.

McHugh, John. 2000. "Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory." *ACM Transactions on Information and System Security (TISSEC)* 3 (4): 262-294.

Meadows, Catherine. 1996. "The NRL Protocol Analyzer: An overview." *The Journal of Logic Programming* 26 (2): 113-131.

Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone.1997. *Handbook of applied Cryptography*. Boca Raton: CRC Press.

Messerges, Thomas S., Ezzat A. Dabbish, and Robert H. Sloan. 2002. "Examining Smart-Card Security Under the Threat of Power Analysis Attacks." *IEEE Transactions on Computers* 51 (5): 541-552.

Needham, Roger M., and Michael D. Schroeder. 1978. "Using Encryption for Authentication in Large Networks of Computers." *Communications of the ACM* 21 (12): 993-999.

Newsome, James, and Dawn Song. 2005. "Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software." Carnegie Mellon University, Department of Electrical and Computer Engineering paper 5. http://repository.cmu.edu/ece/3/.

Paillier, Pascal. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes." In *Advances in cryptology—EUROCRYPT'99*, 223-238. Springer Berlin Heidelberg, 1999.

Paulson, Lawrence C. 1998. "The Inductive Approach to Verifying Cryptographic Protocols." *Journal of Computer Security* 6 (1): 85-128.

Paxson, Vern. 1999. "Bro: A System for Detecting Network Intruders in Real-Time." *Computer Networks* 31 (23): 2435-2463.

Perrig, Adrian, Robert Szewczyk, J. D. Tygar, Victor Wen, and David E. Culler. 2002. "SPINS: Security Protocols for Sensor Networks." *Wireless Networks* 8 (5): 521-534.

Pointcheval, David, and Jacques Stern. 2000. "Security Arguments for Digital Signatures and Blind Signatures." *Journal of Cryptology* 13 (3): 361-396.

Rackoff, Charles, and Daniel R. Simon. "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack." In *Advances in Cryptology—CRYPTO'91*, 433-444. Springer Berlin Heidelberg, 1992.

Raya, Maxim, and Jean-Pierre Hubaux. 2007. "Securing Vehicular Ad Hoc Networks."*Journal of Computer Security* 15 (1): 39-68.

Reiter, Michael K., and Aviel D. Rubin. 1998. "Crowds: Anonymity for Web Transactions." *ACM Transactions on Information and System Security (TISSEC)* 1 (1): 66-92.

Ristenpart, Thomas, Eran Tromer, Hovav Shacham, and Stefan Savage. "Hey, You, Get Off of my Cloud: Exploring Information Leakage in Third-Party Compute Clouds." In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 199-212. ACM, 2009.

Rivest, Ronald L., Adi Shamir, and Len Adleman. 1978. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM* 21 (2): 120-126.

Rosenberg, Jonathan, Henning Schulzrinne, Gonzalo Camarillo, Alan Johnston, Jon Peterson, Robert Sparks, Mark Handley, and Eve Schooler. *SIP: session initiation protocol*. Vol. 23. RFC 3261, Internet Engineering Task Force, 2002.

Sandhu, Ravi S., Edward J. Coynek, Hal L. Feinsteink, and Charles E. Youmank. 1996. "Role-Based Access Control Models yz." *IEEE computer* (29) 2: 38-47.

Shamir, Adi. 1979. *How to Share a Secret*. Cambridge: Massachusetts Institute of Technology, Laboratory for Computer Science.

Shamir, Adi. "Identity-Based Cryptosystems and Signature Schemes." In *Advances in Cryptology*, 47-53. Springer Berlin Heidelberg, 1985.

Sheyner, Oleg, Joshua Haines, Somesh Jha, Richard Lippmann, and Jeannette M. Wing. "Automated Generation and Analysis of Attack Graphs." In *Proceedings of 2002 IEEE Symposium on Security and Privacy,* 273-284. IEEE, 2002.

Steiner, Michael, Gene Tsudik, and Michael Waidner. 2000. "Key Agreement in Dynamic Peer Groups." *IEEE Transactions on Parallel and Distributed Systems* 11 (8): 769-780.

Stoica, Ion, Robert Morris, David Karger, M. Frans Kaashoek, and Hari Balakrishnan. 2001. "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications." In *ACM SIGCOMM Computer Communication Review* 31 (4): 149-160.

Stone-Gross, Brett, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. "Your Botnet is my Botnet: analysis of a botnet takeover." In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 635-647. ACM, 2009.

Straub, Detmar W. 1990. "Effective IS security: An Empirical Study." *Information Systems Research* 1 (3): 255-276.

Straub, Detmar W., and Richard J. Welke. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making." *MIS Quarterly* 22 (4): 441-469.

Valdes, Alfonso, and Keith Skinner. "Probabilistic Alert Correlation." In *Recent Advances in Intrusion Detection*, 54-68. Springer Berlin Heidelberg, 2001.

Waters, Brent. "Efficient Identity-Based Encryption Without Random Oracles." In *Advances in Cryptology–EUROCRYPT 2005*, 114-127. Springer Berlin Heidelberg, 2005.

Xiong, Li, and Ling Liu. 2004. "Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities." *IEEE Transactions on Knowledge and Data Engineering* 16 (7): 843-857.

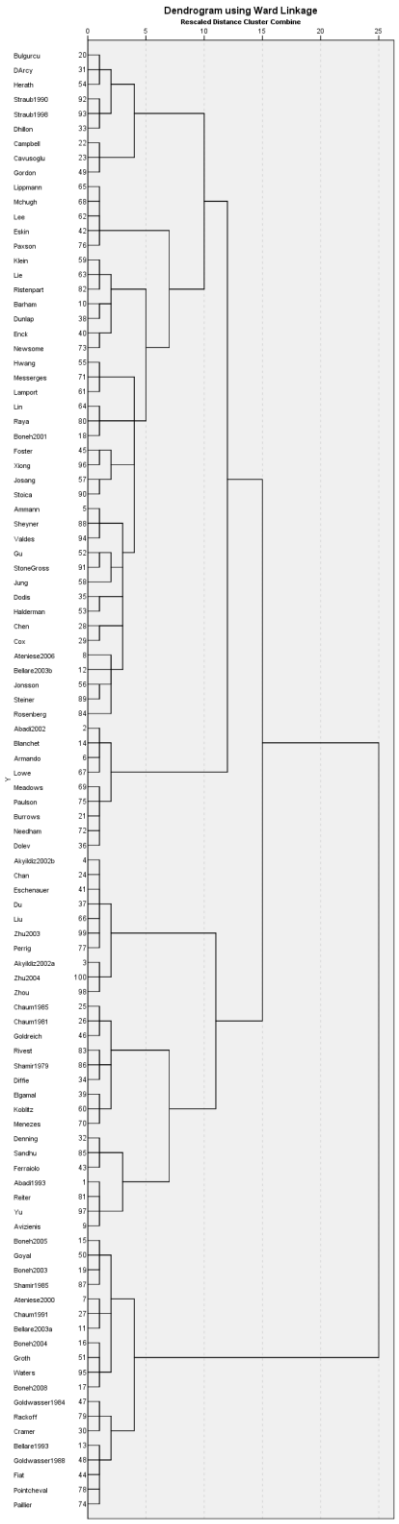
Yu, Ting, Marianne Winslett, and Kent E. Seamons. 2003. "Supporting Structured Credentials and Sensitive Policies Through Interoperable Strategies for Automated Trust Negotiation." *ACM Transactions on Information and System Security (TISSEC)* 6 (1): 1-42.

Zhou, Lidong, and Zygmunt J. Haas. 1999. "Securing Ad hoc Networks." *Network, IEEE* 13 (6): 24-30.

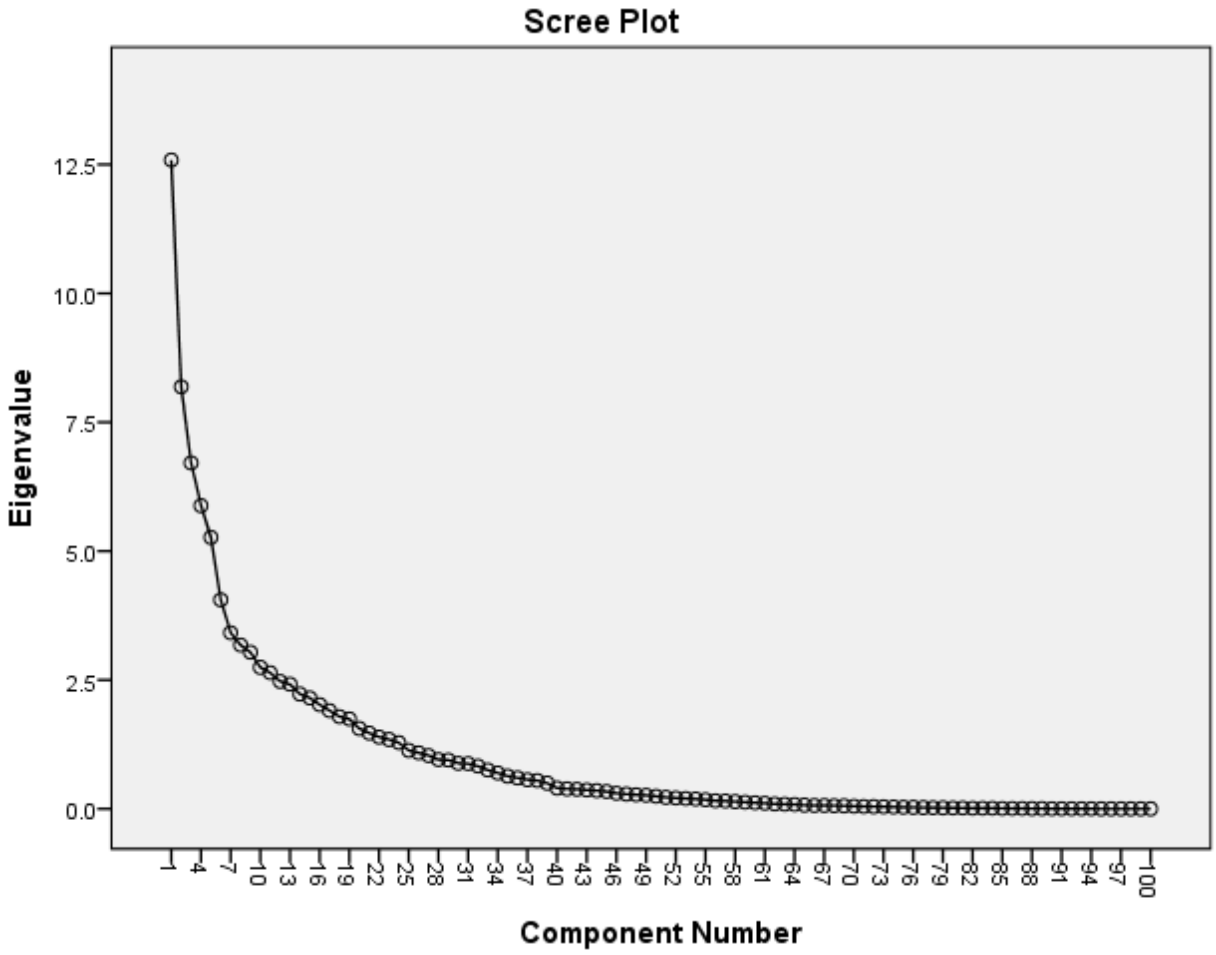
Zhu, Sencun, Sanjeev Setia, and Sushil Jajodia. 2003. "LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks." *Proceedings of the ACM Conference on Computers and Communications Security:* 62-72. http://thor.cs.ucsb.edu/~ravenben/papers/sensors/LEAP-ccs03.pdf.

Zhu, Sencun, Sanjeev Setia, Sushil Jajodia, and Peng Ning. 2004."Interleaved Hop-By-Hop Authentication Against False Data Injection Attacks in Sensor Networks." In 2004 *Proceedings of IEEE Symposium on Security and Privacy:* 259-271. http://edge.cs.drexel.edu/regli/Classes/CS680/Papers/Sensor%20Nets/ilhap.pdf.

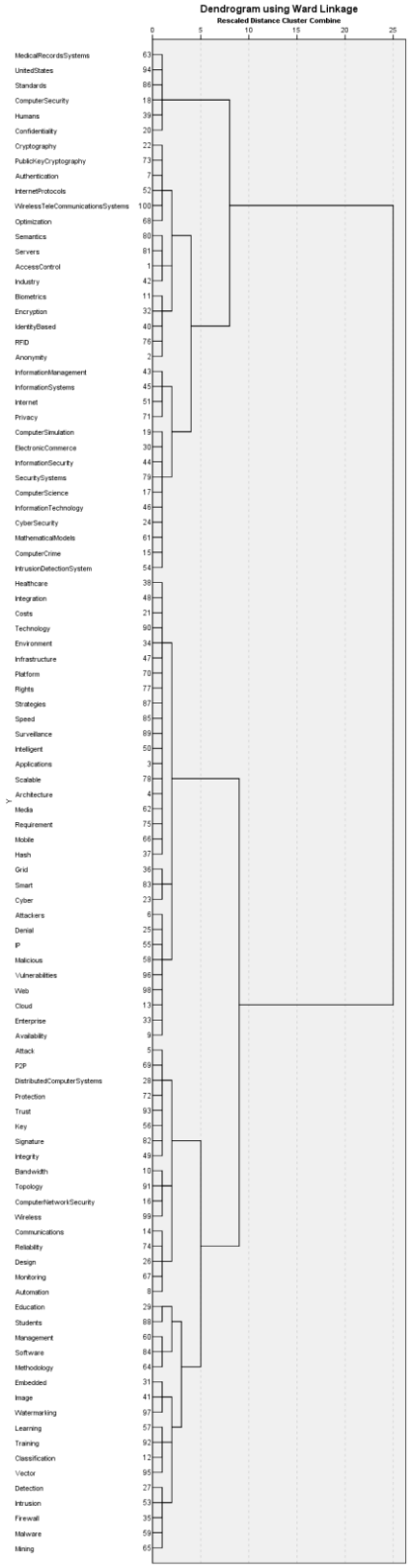
Appendix E Co-Citation Dendrogram



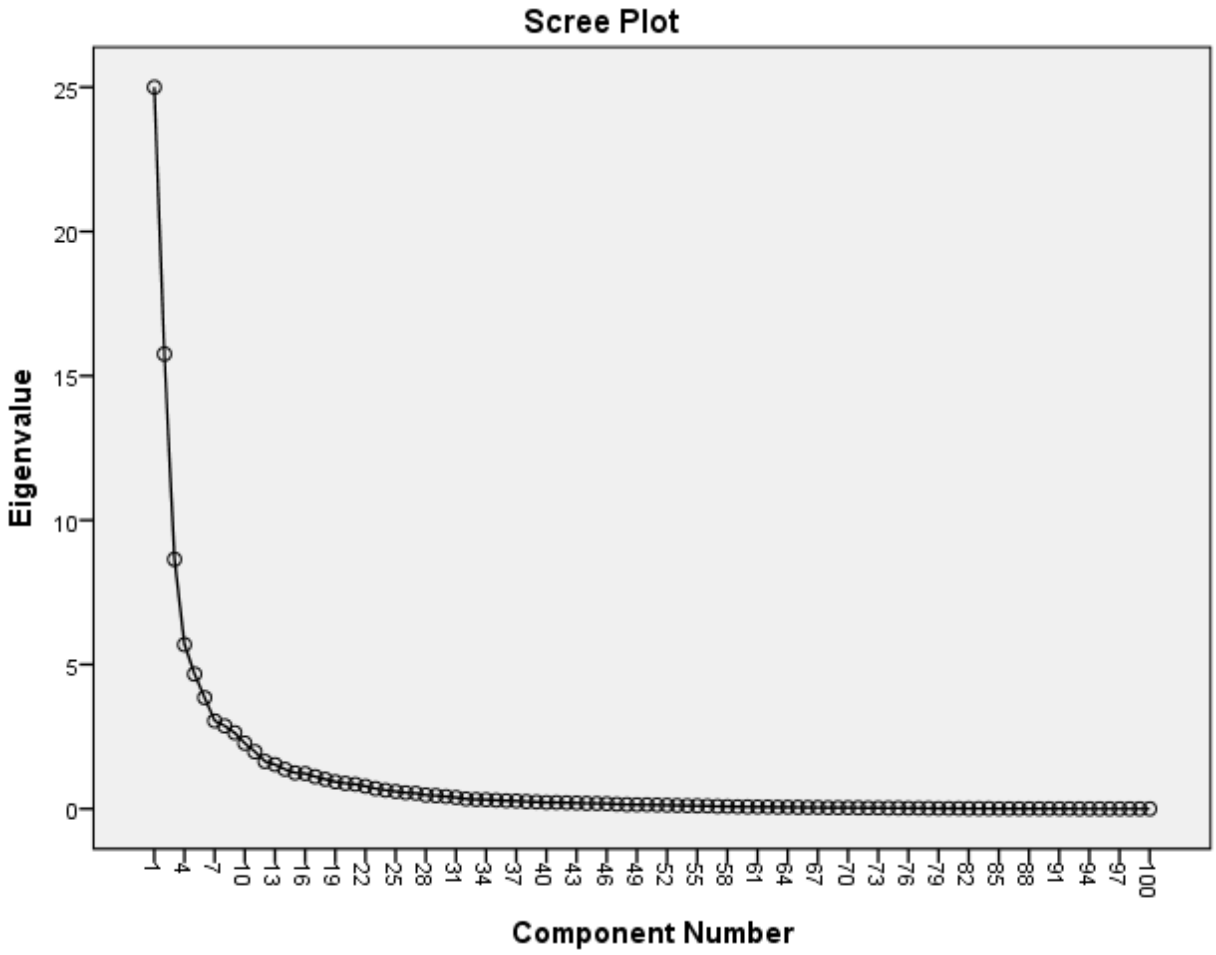
Appendix F Co-Citation Scree Plot



Appendix G Co-Word Dendrogram



Appendix H Co-Word Scree Plot



Appendix I Multivariate and Network Analyses Procedures

The co-occurrence matrices were converted to correlation and proximity matrices using SPSS before running the multivariate analyses (McCain 1990). Accordingly, correlation (*r*) is a measurement of the relationship between variables, namely two documents/keywords. The value of the association between the two variables ranges from -1.0 to 1.0. The positive or negative indicates the direction of the correlation while the *r* value illustrates the relative strength of the correlation (Field 2005). In other words, a greater value suggests that there is a higher correlation between two variables. A correlation matrix, described by McCain (1990), produces a one-dimensional view of inter-document/keyword proximities. This correlation matrix can be expanded and improved via multivariate statistical analyses techniques (factor analysis, cluster analysis, MDS). The factor analysis process in SPSS produced the correlation matrix, which was used as the raw data for the cluster analysis. The cluster analysis process in SPSS formed the proximity matrix that was subsequently used for the multidimensional scaling. The following are some general procedures and configurations for running the multivariate analyses in SPSS.

Factor Analysis Procedures:

- Upload co-occurrence matrices and adjust measure to scale
- Select: Analyze > Data Reduction > Factor
- Extraction Dialogue Box: Choose Principle Component Analysis as method, correlation matrix for analyze, both unrotated factor solution and scree plot for display, and eigen value over 1 for extract
- Descriptives Box: For statistics select Univariate descriptives and Initial solution and Correlations Matrix select Coefficients, Significance levels, and Determinant

Cluster Analysis Procedures:

- Upload correlation matrices
- Select: Analyze > Correlate > Hierarchical Cluster
- Check Variables, as opposed to Cases for Cluster
- Method dialogue box: select Ward's Method
- Check Statistics and Plots
- Input range of solutions from minimum 2 to maximum 99
- Check agglomeration schedule and proximity matrix

Multidimensional Scaling Procedures:

- Upload proximity matrices
- Select: Analyze > Scale > Multidimensional Scaling
- Choose Data are Distances
- Open Model dialogue box: select level of measurement ratio, matrix under conditionality, Dimensions minimum 2 maximum 3, Euclidean distance for Scaling Model
- Open Options dialogue box: select all of the options under Display and leave the critera options set to default

The Network Graph was constructed using the files created from Bibexcel in Pajek. The basic steps will be presented here. However, for a more detailed review of the procedures, see Astrom et al. (2009).

- After the matrices are produced in Bibexcel, highlight the .COC file
- Select Mapping > Create net-file for Pejak > undirected graph
- Highlight the .CIT file > Mapping > Create vec-file
- Select .COC > Analyze > Co-Occurrences > Cluster pairs
- Select the PE2-file > Mapping > Create clu-file
- Open Pejak application > upload .net, .vec, and .clu files
- Select Draw > Network - First Partition - First Vector
- Within the drawing select > Layout > Energy > Kamada-Kawai > Separate Components
- Go back to Pajek main interface, select Network > Create New Network > Transform > Remove > Lines with value (adjust according for visual acuity e.g., remove lines under 30 for co-citation data and lines under 100 for co-word data)

References

Field, Andy. 2005. *Discovering Statistics Using SPSS*. London: Sage Publications.

McCain, Katherine W. 1990. “Mapping Authors in Intellectual Space: A Technical Overview.” *Journal of the American Society for Information Science* 41 (6): 433-443.

Persson, O., R. Danell, J. Wiborg Schneider. 2009. How to use Bibexcel for various types of bibliometric analysis. In Celebrating scholarly communication studies: A Festschrift for Olle Persson at his 60th Birthday, ed. F. Åström, R. Danell, B. Larsen, J. Schneider, p 9–24. Leuven, Belgium: International Society for Scientometrics and Informetrics.

Persson, Olle. "Bibexcel." Accessed January 2, 2014. http://www8.umu.se/inforsk/Bibexcel/.