Making Cyber Security Interdisciplinary: Recommendations for a Novel Curriculum and Terminology Harmonization

by

Robert B. Ramirez

B.S. Computer Science
Columbia University in the City of New York, 2015

SUBMITTED TO THE INSTITUTE FOR DATA, SYSTEMS, AND SOCIETY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN TECHNOLOGY AND POLICY
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2017

Signature of Author: _____
Technology and Policy Program
May 19, 2017

Certified by: _____
Abel Sanchez
Director, MIT Geospatial Data Center (GDC)
Thesis Supervisor

Accepted by: _____
Munther A. Dahleh
William A. Coolidge Professor of Electrical Engineering and of Computer Science
Director, Institute for Data, Systems, and Society
Acting Director, Technology and Policy Program

Making Cyber Security Interdisciplinary: Recommendations for a Novel Curriculum and Terminology Harmonization

by

Robert B. Ramirez

Submitted to the Institute for Data, Systems, and Society on
May 19, 2017 in Partial Fulfillment of the
requirements for the Degree of
Master of Science in Technology and Policy

ABSTRACT

Cyber security was historically a technical subfield of computer science. However, pervasive computing technology has recently made security a significant concern for management and policy. In this thesis, I review the academic literature of cyber security, and argue that security as a field comprises four different subdisciplines: policy, computer science, management, and social science. Furthermore, collaboration and communication between these fields is lacking, as evidenced by differing terminology between these fields and few interdisciplinary journal publications. The remainder of this thesis is devoted to answering the question "How can cyber security professionals, including academic researchers, better approach cyber security as an interdisciplinary field; and what are the benefits of doing so?" This thesis recommends two steps the cyber security community can take towards becoming more interdisciplinary: undergraduate multi-departmental education; and harmonizing terminology between subdisciplines.

To the first step, I present a novel curriculum design: an interdisciplinary minor in cyber security, which would equip non-security professionals with basic knowledge of security, and equip security professionals with skills for approaching security with an interdisciplinary mindset. I create a balanced curriculum design based on the findings from my literature review regarding the four subdisciplines of security. MIT's entire subject catalog was sourced for classes, to design a model curriculum. While this curriculum proposal was developed for MIT, the design is institution-agnostic, and I discuss how to apply it to other universities.

Second, to facilitate cross-disciplinary communication, I recommend instituting change at the higher, professional level. To achieve this, I recommend authors harmonize their jargon usage. This change would improve idea flow between authors from different disciplines, who work towards potentially mutually beneficial solutions, but who write for separate audiences in their publications. To identify areas in need of harmonization, I first examine the extent of differences in keyword usage in articles from each the four security subdisciplines. I also analyze time-series trends of terminology usage in cyber security journal articles, and I develop a methodology for authors or standards bodies to use when deciding whether a word or phrase is appropriately interdisciplinary, or has been accepted by the general cyber security community.

Thesis Supervisor: Abel Sanchez

Title: Director, MIT Geospatial Data Center (GDC)

Acknowledgements

This work would not have been possible without the collaboration, support, and assistance of a multitude of persons beyond just myself. I would like to thank my advisor, Dr. Abel Sanchez, for all his patience and guidance, for his warm and inviting spirit, and for his enjoyable tangential conversations. I'm forever grateful to him for working with me and my friends when we were in search of a new research lab. I am also indebted to Nazli Choucri for her guidance when writing the work that this thesis is partially based on. I would also like to thank Stuart Madnick for his help supporting my passion for education development, and for welcoming me at his research meetings.

I would like to express my extreme gratitude to Howie Shrobe and his research group for nurturing my interests in cyber security, and for giving me countless opportunities to better engage with the field. Among my distinguished colleagues, I would also like to thank my good friends and fellow lab members, Greg Falco and Carlos Caldera. You have been with me since my first week at MIT, and I could not have been luckier in finding such supportive friends and ambitious colleagues. I could not have been successful without you.

I thank my friends and cohort of the Technology and Policy Program for always being open to me no matter how many times I came and went. I especially thank Barb and Frank for putting up with all my questions and last-minute requests.

I also thank my good friends from home in Jacksonville and from college. I could not have made it to MIT, or through MIT, if I did not have your respect, your help, or your good humor. You are truly the greatest gift in life.

I would like to thank my family for their love, their encouragement, their unwavering belief in me, and their understanding all those times I was too busy to call. They know better than anyone that from the moment I discovered the institution of MIT as a young child, my dream in life has been to participate in the incredible work that goes on here. I attribute my ambition on that front to my brother, George, for first telling me and inspiring me about MIT. I owe my family so much for helping me get here, however tortuous the path might have been. It brings me endless joy to know that I have made them proud.

Finally, I thank God for all the opportunities and all the second chances I have received in life, and for giving me the strength to walk the paths of my dreams. May I always have faith in him.

Table of Contents

List of Figures

List of Tables

1 Introduction

DISCLAIMER
This chapter is partially based on an edited version of prior work.

1.1 Motivation

Cyber security is a popular field of study with a growing body of research, though it is still in its nascence relative to other fields [77,78]. It is rooted in traditional computer science, but has recently gained prevalence in other fields. Among these are law and business management, as well as areas of technology that did not originally operate with the Internet, such as smart grids, cars, and other cyber-physical systems. These areas must deal with new and unanticipated security vulnerabilities because of their newfound connections to computer systems and the Internet [112]. As a new field that emerged from many old ones and which serves as a unifying concern among disparate disciplines, cyber security has received little attention in its own independent formalization, outside cryptography. Instead, research goals and terminology are specified by the separate fields that depend on security, even as cyber security has become more complex. The pace of growth of businesses and of cyber security challenges encourages continued ad hoc approaches to security. The urgency of quickly protecting against cyber-crime may outweigh careful consideration of research trajectories or collaboration between disciplines. At the same time, the field is still relatively new, and standardizing certain aspects of it too early could stifle growth.

Outside of cryptography, cyber security as an academic discipline has been left to organically evolve. Research directions are often not determined by an overarching agenda, but by what is being talked about by people in a given subdiscipline, such as policy, even if knowledge of what other subdisciplines are researching would change that agenda. Standardization is commonplace in scientific disciplines, beginning with either systematic nomenclature or otherwise standardized vocabulary [87-89]. Yet there have been very few efforts in cyber security research standardization, and all of them have been government-led, rather than academically or business-led [118,119]. Despite its relevance for multiple disciplines, cyber security itself is not very interdisciplinary. This is largely due to this lack of involvement of the separate fields with each other.

Increased interdisciplinary communication in cyber security would facilitate the flow of ideas between parties, leading to invaluable gains in innovation. Such unification would also lend itself to the community formulating overarching research goals. In this thesis, I facilitate more unified research by the global multi-stakeholder cyber security community, especially by academia, by

facilitating greater communication among the disparate disciplines that concern themselves with this area. I do so by designing a unifying interdisciplinary undergraduate curriculum for cyber security, and through identifying trends in terminology standards for authors to consider when targeting audiences and conducting literature reviews.

1.2 Research Questions

This thesis was motivated by the observed paucity of interdisciplinary research, as well as an apparent lack of communication across disciplines such as business with computer science, when approaching cyber security issues. The broad goal of this research is to remedy these communication barriers that have naturally evolved, or rather, naturally never been broken down. To formalize the scope of this research inquiry, the following three research questions were developed:

1. SUBDISCIPLINES What are the different broad categories of cyber security research, how many are there, to what extent, if any, are they actually segregated, and what specific types of research comprise these areas?
2. EDUCATION What changes to educating cyber security professionals, whether researchers or otherwise, can best enable the workforce to address multi-faceted issues of cyber security now and in the future?
3. TERMINOLOGY If the observations of siloed-off areas of cyber security research and innovation are informed in part by extreme differences in the vocabularies, to what extent does terminology differ between the disciplines, how has it evolved over time, and what guidelines can authors or standards bodies use when deciding how best to communicate with broad, interdisciplinary audiences about cyber security?

1.3 Thesis Overview and Organization

Some work on crafting ontologies of cyber security research has been done in the past using both manual and automated techniques [2, 30, 35, 58, 59, 62, 65, 74, 75]. However, such efforts usually used relatively few inputs, such as starting with a basic phrase of "cyber security" and performing automated searches for papers with this term; and therefore, these studies may not have covered the entire scope of the field of cyber security. This thesis, extends this research to create an accurate general segmentation of the entire field of cyber security.

The approach taken to assess the subjects covered by cyber security work was to perform a large system-wide literature review of the field of cyber security. This literature review was designed to encompass many other literature reviews and scholarly summary articles, and focused on the current directions the field is evolving towards, thus focusing on many of security's newer, less traditional aspects

Next, from this review, the current state of cyber security as a discipline was determined to comprise four loosely-defined fields that can be described as policy, business, infrastructure, and general research. Support for this categorization is also given by similar prior research. Inconsistent terminology usage between the fields, statements from authors and researchers, and the areas of research covered by these separate fields are used as evidence that these fields, while allegedly working towards the same goals, are not unified and lack interdisciplinary communication and idea flow.

Benefits of increasing interdisciplinary communication within cyber security are described herein. The broader hypothesis underlying this thesis is that not allowing disciplines to grow together (by not participating in this growth by utilizing concepts from different disciplines), is a regression towards the mean of one's own discipline, if one believes that innovation is at the edge (of disciplines). While there are numerous edges to innovate on that research constantly takes advantage of, one particular edge – interdisciplinarity – is often overlooked. Interdisciplinarity and harmonized communication create a new innovation edge for cyber security. To improve interdisciplinary communication in cyber security, two systemic changes to cyber security idea exchange methods are proposed and described.

The first such recommendation for improving idea flow is a novel design for an interdisciplinary Minor in Cyber Security that incorporates the four fields that comprise cyber security. The curriculum design is described along with details of the ongoing effort to practically implement such a program at MIT. Additional benefits of such a program beyond giving undergraduate students and faculty an interdisciplinary perspective of security include combatting the widely-cited talent shortage in cyber security. Guidelines for applying this curriculum design to other institutions are also given.

The second recommendation this thesis makes for improving the quality of idea exchange between policymakers, management, and academia is to harmonize the terminology used when communicating cyber security concepts. In this thesis, the extent of inconsistencies in terminology use between the four subdisciplines of cyber security was identified. The benefits of harmonizing terminology, such as policymaking, literature review efficiency, and search engine optimization, are then discussed.

This terminology study is intended to serve as a guide for governance bodies or the academic community when developing standard jargon for cyber security, or to be taken as guidelines for selecting keywords, titles, and proper technical terms in future cyber security literature searches or publications. This thesis was written to adhere to these terminology recommendations except in the use of citations from other articles, which, if conflicting, are indicated with [sic].

Herein I do not attempt to create new standards; rather, my goal is to infer standards based on inclinations of published works, in order to facilitate research and discourse in the field. I hope to

clarify emergent standards and avoid overburdening the research field with unintelligible phraseology.

The specific contributions of this work are sixfold: 1. I identify a large proportion of the emerging trends in cyber security research; 2. I identify the general silos cyber security research falls into, and their associated terminology. 3. I point out a long overdue need for greater collaboration between these isolated silos; and suggest avenues for further research based on my classification. 4. I develop a practical proposal for an undergraduate cross-departmental cyber security minor for MIT and a design that is applicable to other universities. 5. I propose guidelines to consider when selecting cyber security words and phrases when communicating or for standards bodies creating dictionaries. 6. I make specific terminology usage recommendations for communicating across subdisciplines of cyber security, to optimize idea exchange.

This thesis is organized to follow the logic of assessing the state of interdisciplinarity of cyber security, and to describe how to bring closer together the multiple fields of cyber security that are addressing the same problems. The organization of this thesis is as follows.

Chapter 2: Literature Review and The Cyber Security Subdisciplines

In chapter 2, the literature review for classifying cyber security is discussed. Articles were selected for review manually, from results of searches conducted with the MIT libraries Mega-Search. Given the limitations of human ability, this manual portion of the study was not intended to construct any detailed ontology of cyber security, but it was designed to cover a broad area, and was targeted to include other literature reviews, ontologies, and broad articles, as well as standalone articles from emergent sectors of security. Inferences were drawn to identify many current trends, and papers were grouped by broad fields. These broad fields are loosely defined, and are posited to also encompass all research areas that were not explicitly identified. Additional support for this categorization is given by comparing the results to similar prior research.

Chapter 3: Interdisciplinary Cyber Security Education

Chapter 3 identifies the deficiencies in cyber security education at the interdisciplinary level. The following observations were made from this research:

1. There exist no interdisciplinary cyber security education programs in the United States
2. There are no top 20 universities with formal undergraduate cyber security programs
3. There are no minors in cyber security at U.S. universities
4. MIT has sufficient, or nearly sufficient existing coursework and infrastructure in place to create a minor in cyber security that covers the four categories of security

The benefits of a cyber security program that is specifically interdisciplinary are then described. Such benefits are different from the benefits of existing single-department cyber security education programs. Namely, the problem of the human factor can be better solved by instilling general practical knowledge of security in more people. Simple human error is to blame for most security

breaches [See Chapter 3, references 36-37]. Early, widely available education can circumvent the problem of computer vulnerabilities slowly spreading to affect previously unaffected disciplines, like medicine and mechanical engineering, which is inevitable with the progression of the Internet of Things. By allowing cyber security to be an accessible field of study to anyone, organizations' overall security posture will proactively be improved, and workers can anticipate and avoid vulnerabilities more effectively than if they were trained on an as-needed basis in the workforce.

Based on these observations, the ideal interdisciplinary education program was determined to be a multi-departmental minor for undergraduates. A proposal was developed for creating an Interdisciplinary Minor in Cyber Security at MIT. Progress of the proposal is discussed.

Chapter 4: Harmonizing Terminology Across Disciplines

Chapter 4 provides guidelines, metrics, and suggestions for unifying the cross-disciplinary terminology of cyber security research. To achieve this, the myriad keywords taken from the initial literature review are used as inputs to automated journal database queries, to identify trends in terminology use. Linguistic origins and time series trends of usage in publications were then analyzed.

Next, a methodology for researchers to use in the future to identify words and phrases that are emerging as commonly accepted by the academic security community is proposed and justified. Suggestions are made for using cyber security words and phrases to optimize author-side search engine indexing and researcher-side literature review searches. Some general inconsistencies in cyber security terminology usage are also resolved. Lastly, some areas of security research that are lagging or emerging are identified based on low numbers of publications in keyword search results.

Chapter 5: Conclusion

Chapter 5 reviews the three thesis questions posed in Section 1.2 and summarizes the findings of the research. The limitations of the research conducted are presented and future work is discussed.

2 Literature Review of The Cyber Security Subdisciplines

DISCLAIMER
This chapter is heavily based on an edited version of prior work.

The object of this study was to manually identify significant areas of focus in current academic cyber security research, in order to verify the extent of segmentation of the field into different disciplines. Articles were selected for review manually from certain searches using the MIT libraries Mega-Search. Given the limitations of human ability, this manual portion of the study was not intended to construct any detailed ontology of cyber security, but it was targeted to include other literature reviews, ontologies, and broad articles, in addition to standalone articles from emergent sectors of security. Inferences were drawn to identify many current trends, and papers were grouped by broad fields. These broad fields are loosely defined, and are posited to also encompass all research areas that were not explicitly identified. Additional support for this categorization is given by similar prior research.

2.1 Literature Review Method

The intention of this literature review was to assess the state of emerging cyber security research and explore avenues of cyber security that have not received as much traditional attention as standard topics of network security, cryptography, and basic system security that a typical university curriculum in focuses on [105-107]. The manual literature review was performed via a number of particular searches throughout September 2015 with the MIT libraries revolving around journal papers containing the word or prefix "cyber" and selected based on breadth of coverage as candidates for further reading. Selection criteria included priority given to other literature reviews and papers whose intention was broad characterization of issues, with a slight preference away from technical papers.

When technical papers were selected for review they were more often cyber-physical security papers, such as ones on SCADA and PLC security. In addition, some papers from the Columbia University/Global Commission on Internet Governance (GCIG) 2015 Conference on Internet Governance and Cybersecurity [sic] were selected independently for review. In addition, the selection process evolved slightly over time, becoming more restrictive, as is typical with literature reviews. The selection process for papers that I identified using the MIT libraries online database is illustrated by the following search parameters, which were chosen to narrow down the articles selected for the literature review. Successive terms in each search (e.g. "review" followed by "overview") were added sequentially in time as the search was revised during the initial article selection process in September 2015:

1. (cyber) AND (review OR overview OR meta-analysis OR survey OR primer OR literature OR outline OR governance OR international OR global OR sustainable) NOT (bullying OR psychology OR psychosocial)
2. cyberspace AND ((review OR overview OR meta OR survey OR primer OR literature OR outline or sustainable)) NOT ((bullying OR psychology OR psychosocial))
3. (cyber) AND (ontology)

All searches were restricted to academic journal articles or conference papers from the years 2012-2015. From these searches and the GCIG Conference, 134 candidate papers were selected. Further manual inspection for breadth of coverage was performed, with preference to topics less commonly covered in undergraduate cyber security education. Time constraints for reading the papers also played a somewhat restrictive role in paper selection. 77 papers in total were selected from this group and were read or skimmed for content [1-74, 121-123]. The number of citations per paper was not known when selecting papers.

2.2 Literature Review Findings

After reading the selected articles, they were analyzed for commonalities. For the initial stage of the analysis, the selected papers were grouped into categories corresponding to their general area of research. The proposed categories are outlined in Table 1 below with summaries detailing all the encompassed research subjects. These categories are qualitatively described in Section 2.3.

Researchers can consider these categories in the future when creating more formal categorizations or ontologies of cyber security. The goal of this thesis is not to delineate the formal boundaries of cyber security, but rather to model the current topics of the field. However, developing a full machine learning topic model of cyber security was beyond the scope of this thesis, and is left to future research. The articles selected in this literature review were also few enough in number that manual review was preferable over topic modeling, to fully understand the nature of the articles' subjects.

Identifying different areas of cyber security research is an important step in formalizing the research methodology of cyber security, as it points to which fields security might benefit from drawing frameworks from in the future. Understanding the scope of research being done also helps frame research agendas, whether large publicly funded agendas or small, private agendas.

It became evident from this literature review and from the identification of cyber security categories that there is a communication gap in cyber security which divides traditional technological research from the public and private sectors' nontechnical dealings with cyber security. This communication gap is a large problem impeding progress in this space, because it results in avenues for cross-disciplinary innovation being overlooked. The remainder of this chapter describes the identified categories and these overlooked innovation edges, as well as the causes and consequences of this communication gap.

Table 1	Categories of cyber security publications from the literature review			
Label	General Descriptor*	General topics included**	Extended High-Level Summary***	References
A	Public Sector Policy	Global Internet law, politics, and governance	Arguably the most diverse category in this literature review. Contains papers on cyberspace geography and jurisdiction, papers on issues surrounding concepts of cyber war, Internet standards and governance, or various other legal issues, including crime problems that have a very legalistic or political angle. Papers containing broad questions of national security and strategy, the global multistakeholder community, and many other broad policy or international relations questions are included in this category.	3, 7, 9, 12, 13, 14, 15, 20, 21, 23, 25, 26, 34, 36, 39, 41, 43, 45, 46, 49, 51, 52, 53, 54, 56, 64, 67, 69, 71, 121, 122, 123
B	Cyberspace Infrastructure	Technical computer science cyber security research, hardware, software, networks, CPS, cryptography	Most of the technological publications. While this literature review focused on the new trend in cyber security of critical infrastructure, and thus that dominates this category, this category could theoretically include anything mathematical, or related to software for, the infrastructure of cyberspace. In this review, this includes SCADA vulnerabilities and security of cyber-physical (e.g. critical infrastructure) systems, as long as they maintain some degree of technical rigor such as modeling. It could also have included encryption schemes, Internet protocol articles, and more. This category would not include software or models designed for policy analysis, business management, criminological or sociological papers, or broad descriptions of cyber security.	5, 8, 16, 17, 18, 19, 24, 29, 38, 48, 55, 63, 66, 70
C	Business and Operations	Business management, frameworks, best practices	Articles aiming to call attention to: poor business practices and other kinds of risks for businesses; culture and awareness; and ways to improve these practices (many of which are simply negative statements: e.g. "stop leaving CISOs/CIOs out of the loop"). In addition, this category encompasses papers that include more in-depth *positive* frameworks for maintaining cyber security in a business through education, access control, supply-chain management, etc. That is, these frameworks specify what *to* do as opposed to what *not to* do. Many of these papers include not only suggestions for management but also propose research agendas for cyber security management.	1, 27, 28, 31, 37, 40, 42, 44, 50, 57, 61, 68
D	General Research	General cyber-crime, threats, Ontologies, social science studies	Publications about what cyber-crimes or vulnerabilities exist. Includes social science research. This research is more technical than categories A or C, but is much higher-level than in B. Other inclusions in this category are such "system-wide" topics as "A systematic literature review of computer ethics issues"	2, 4, 6, 10, 11, 22, 28, 30, 32, 33, 35, 47, 58, 59, 60, 62, 65, 73, 74

Table 1. Descriptions and summaries of proposed categories of cyber security research. Based on the literature review. [132]

***Not meant to completely encapsulate the category out of context; simply meant as a means of easily referring to the general categories of journal articles' research. Categories may have some overlap; they are intended primarily for organizing the topics found in the literature review, and for sensitivity rather than specificity. **In this review. *** See section 4 for illustrative summaries of select papers.**

2.3 Article Summaries by Category

This section describes the articles assigned to each category in more detail to illustrate the different emergent categories and subcategories of cyber security. Section 2.5 analyzes the general shortcomings of the state of research in the field. Precisely defining each category is beyond the scope of this thesis, as I do not wish to circumscribe research with specific definitions.

2.3.1 Public

The "Public" category includes issues of concern to governments. It includes work regarding laws, international norms, and national security. Global technical standards produced by bodies like as ICANN and W3C, while often specifying norms, are instead placed in the Infrastructure category. Also not in this category are topics like business operations and supply chain management, even if government services benefit from these topics. I discuss those topics in Section 2.3.3, the *Business* category.

Harrop et al. (2013) give a short summary of cyber security efforts in the UK and the US. They attempt to assess their protection measures, some of which address information sharing between entities on such topics as vulnerabilities and "cyber" incidents [25]. This includes a list of recommendations used by the UK Center for Protection of National Infrastructure (CPNI) to ensure security, and describes a number of UK efforts to help businesses and the nation address cyber security. They go on to describe the state of US cyber security such as the NIST cybersecurity [sic] framework [83]. They also list the critical national infrastructure sectors of the two countries.

Pawlak et al. (2013) analyze and compare advances in threat evolution and government security, concluding that governments need to do more to defend themselves and their states, starting with basic capacity building [49]. The authors say that nations are in danger of severely lagging behind trends in cyberspace. They also note, based on another study, eight innovations that will shape the future cyber security-risk landscape: the cloud, big data, the internet of things, mobile internet, the neuronal interface, contactless payments, mobile robots, quantum computing, and the militarization of cyberspace. Lastly, they call for researchers to create a model of how exactly public and private spheres will collaborate in the future.

Grant et al. (2014) apply the concept of cyber-geography to military operations and come up with cartographic terms for cyberspace. They also suggest that researchers might be able to use their ontology to shed light on the attribution problem of being unable to expediently identify malicious actors through cyberspace [23].

Chertoff et al. (2015) describe the state of Internet jurisdiction law, i.e. the problem of assigning legal authority to a particular forum when a suit traverses multiple states. They propose four potential formulations that might clearly and fairly define the controlling jurisdiction in cases [9].

These formulations are choice-of-law rules that states might adopt based on either: the citizenship of the subject of the offending information, data, or system; the location where the harm has taken place; the citizenship of the data creator; or the citizenship of the data holder or custodian.

Lin (2015) compares nuclear and cyber technology and regulation, listing a host of differences, and a few similarities, between potential problems these two technologies create, which he places into categories of strategy, operations, acquisition, and arms control [26].

Common to all these articles, including the ones not mentioned here, is a notion of a system of governments that is lagging behind technology and that may not even be equipped to manage it well at all. The articles in this category serve as a call to researchers and the global multistakeholder Internet community alike to unite in search of solutions. They also point out a looming threat to governments and nations, not only in the form of cyber-attacks, but also in the form of non-governmental entities taking over management of traditionally government-regulated matters, such as international communication, national security, and even control over borders and international law. These problems foreshadow many other problems to come for national governments, all of which are exacerbated by the existence of the Internet and widespread computing.

2.3.2 Infrastructure

This category includes most of the articles that address technological problems of cyber security; specifically, those problems related to the actual infrastructure of cyberspace. This does not necessarily include solutions to every problem that businesses or academic researchers might address – for example, a software tool for managing finances is a category C, Business, topic. The Infrastructure category includes papers that discuss various aspects of cyber security of critical infrastructure, as well as security issues concerning the operation of cyberspace, such as cryptography. It also encompasses papers describing methods for intrusion detection, reverse engineering, and computer forensics, among other issues.

Franke et al. (2014) systematically review 102 papers, drawn from IEEE Xplore, Scopus, Springer link, and Web of Science, in an effort to create a research agenda in the area of cyber situational awareness. Topics they cover include game theory, cognition, vulnerability detection, attack detection, other network analysis, broad primers; a great variety of articles on securing industrial control systems (ICSs)/SCADA (such as power grids); some concepts of emergency management; various tools, architectures, and algorithms on a host of topics, including attribution; and many papers on "visualization," for cyber situational awareness. They note deficits of articles on teamwork (in various senses of the word), information exchange, military strategy, and in nation-wide or other high-level cyber situational awareness, despite cyber situational awareness being extremely popular with policy-makers [16]. Franke et al. recommend more attention be paid to these areas; to efforts to deceive attackers; and to confidentiality and integrity. The authors suggest

that researchers perform experiments to measure how particular solutions contribute to the overall understanding of a situation; and they enumerate further directions for game-theoretic research; for data fusion algorithms for low-level and high-level information, like sensors and NLP; and for empirical work and exercises. Among efforts for cyber situational awareness, ICSs research is well-endowed with articles.

Genge et al. (2015) provide a detailed description of their "cyber attack impact assessment methodology," which has the potential to be a general-purpose tool for assessing attack impacts on cyber-physical systems [18]. This carries implications for securing cities and countries, although these applications were not detailed in the paper.

Huang et al. (2015) detail an in-depth cyber-physical network architecture that prevents cascading failures by=resisting collapse from errors on either the cyber or the physical side both in simulations and mathematically provably [29].

Gao et al. (2014) review a literature on SCADA implementation and security, providing a comprehensive reference. They describe two main categories of security issues in SCADA systems: direct threats (terrorist attacks, etc.) and indirect security threats (e.g. viruses, bugs). Gao et al. reiterate a common notion that SCADA security cannot be approached like traditional IT security, as availability and safety are paramount in SCADA systems, and SCADA infrastructure is less dynamic and less globally networked than traditional IT systems are [17].

Cheminod et al. (2013) provide a literature review about the conceptual state of security for critical infrastructure and cyber-physical systems. They focus on both the component level and the system level, including the state of policy enforcement. They also provide a host of resources for industrial networks, and mention future areas of research in detail [8].

It is clear from these papers that there is no shortage of work being done on cyber-physical systems security. However, research of the connections and interactions of critical infrastructure with the rest of cyberspace and society is somewhat behind, as is research of the interaction of cyber-physical systems security and traditional cyber security. Not integrating cyber-physical security with concepts concerning other areas of cyber security is a common ailment among these papers. It is equally important for other STEM fields besides cyber-physical systems, who are now researching cyber security, to also integrate with traditional "computer science" cyber security researchers in this manner.

2.3.3 Business

The third proposed category of cyber security focus concerns business practices and other organizational and human factors affecting cyber security. The following descriptions of articles give an illustrative overview of the types of articles that fall into this category.

Messmer (2013) calls attention to the lack of coordination within businesses, many of which are also lagging behind technologically [42]. She points to the fact that insurance decisions concerning cyber security are not discussed with C-level information officers as often as they should be. This problem is easily remedied, but it is a reflection of other organizational shortcomings in the workforce. CIOs and CISOs might be described as *Business* actors whose worldviews differ from the *General* worldviews of insurance companies.

Khan et al. (2015) notes that the weak links in supply chains are often subject to attack. By analyzing the literature to identify if supply chain models can incorporate "cyber-resilience," the authors provide recommendations for practice. In addition, Khan et al. give a number of research directions for identifying cyber-risk in supply chains and securing against it [37].

"Cyber-resilience", and used by Khan et al., is a popular buzzword that contrasts with cyber security by emphasizing the inevitability of cyber-attacks and the importance of being able to rebound as a business from such hiccups. However, proper cyber security education among employees and management is a better solution than implementing buzzwords, and would eliminate the confusing notion that cyber security does not imply resilience.

Andel et al. (2013) surveyed various cyber programs at universities and retroactively document how a particular program developed at the University of South Alabama was created. They detail the goals and objectives and how they created a curriculum that attempts to be comprehensive. They comment briefly on the problem of naming courses, which reflects this author's views on the necessity of a defined vocabulary: they give the example of Cybersecurity vs Cyber Engineering and the ambiguity of the differences between these two topics [1]. Readers will note, however, that the former is a much more widely accepted term than the latter; authors should strive away from using the latter.

Sitnikova et al. (2014) write about "broader Internet security management and governance of the Internet and the cyberspace." They take a risk management approach to formulate a methodological framework for managing cyber security. They base their conclusions on a review of cases and previous studies, and highlight solutions at various levels of business operations, considering classic business elements of technology, people, and "processes," emphasizing that technology cannot solve all problems [57].

Jaitner et al. (2015) identify domains of science that contribute to the "cyber" field of study. They also identify points of necessary collaboration (presently implemented or not) across fields regarding a nation's cyber readiness. The goal of their paper is to identify areas not fully explored in academia, and for generating curricula recommendations. They aim to be comprehensive, drawing knowledge from Russia, and covering math, finance, linguistics, and natural sciences [31].

All the articles in this category point out that the organizational principles of businesses, and even of academic fields of study, are not synchronized. There are vulnerabilities in supply chains, in employee trust relationships, and from social engineering. These papers also illustrate the point to be covered later about a lack of well-defined terminology and the prevalence of ad hoc phrases to describe certain, even redundant, aspects of cyber security. Moreover, papers in this category make clear that technological solutions alone cannot ensure cyber security.

2.3.4 General

The "General" category contains all papers with issues which pervade the entire realm of cyber security, as well as descriptions of the field in general, and characterizations of cyberspace and humans' interactions with it – including most articles from social sciences.

Zhang et al. (2012) give a primer on, empirically, what actual crimes exist in cyber space. They categorize the crimes and call for action on existing problems such as cyber terrorism, phishing, and others [72].

Busse et al. (2015) give a helpful introduction to Ontology; specifically, contrasting the various meanings the word takes on in information science with social sciences. They conclude by stating

> *"Different disciplines need to grow together more and more. The major challenges of our time – scientific and social – can only be solved interdisciplinarily. To be successful, it is vital that we manage to find results of various teams in various disciplines worldwide and to integrate them reasonably. Ontologies are of vital importance for this: by the power of standardizing terms, their meanings, and relations; furthermore, by the possibility of integrating different domain-ontologies; and, last but not least, by supporting the semantic web in search, reasoning and integration with computer applications. This is why we expect the importance of ontologies to grow significantly in future*" [6].

In short, Busse et al. provide a strong argument for cross-discipline communication and standardization of vocabulary terms.

Ju An et al. (2010) put forth a cyber security vulnerability ontology for comprehensive use, giving examples and references [35]. They are among many authors who propose information science-type ontologies, but do not necessarily scope the use of the ontologies, demonstrate their use, or make their ontologies publicly accessible.

Jardine (2015) gives an interesting perspective on the state of cyber-crime. He finds that most vulnerabilities are decreasing (when normalized against the growth of IT), and most attacks are increasing (whether normalized or not), but are increasing more slowly over time and may soon be seen to be decreasing (predicting a concave-down trend in attacks). In short, the picture of cyber-crime is not as bleak as the absolute numbers make it seem when compared to the growth

of cyberspace [33]. However, Jardine note that the data he used may be imperfect; and trends were only analyzed from 2008 – 2014. Jardine's recommendations for the community include: focus on the user rather than the system (i.e. put more effort into educating and empowering the user, and continue putting the same effort into the technology of the system); use open-source code, like SSL, where possible, to find vulnerabilities more quickly (e.g. Heartbleed); create stricter rules for reasonable disclosure timeframes of zero-day knowledge held by governments; develop international agreements on norms for web-based attacks; create more cyber-crime insurance or other ways of spreading costs out; and he recommends that small-to-medium-sized companies need to invest in IT security and training as much as large companies do; and that cyber security companies start to collect and represent their data in normalized terms with respect to the size of their networks, the way Jardine does in his article.

In Chertoff et al. (2015), Michael Chertoff, former Secretary of Homeland Security, gives a primer on the dark web, the intentionally hidden part of the deep web, unindexed by search engines and impossible to reach with normal browsers. A traditional search engine sees about 0.03 percent of the web – the other 99.97% is the deep web. The authors assert that the global community needs to consider the deep web's impact when discussing Internet governance. A huge amount of crime (and a huge diversity of it) is supported in the deep web, and new ways to map and monitor it are needed. They nevertheless emphasize that the deep web's existence is good, in some ways, for everybody [10].

Common shortcomings of papers in this category are a lack of ontological understanding and scoping of the problems of cyber security, as well as indicators of a lack of a defined cyber security vocabulary across disciplines. These papers all conclude that the field needs more interdisciplinary cooperation, and that better characterization of cyber-crime and novel approaches to combating it, not necessarily technically, are imperative. Lack of consistent vocabulary is not in itself problematic – Busse et al. go into detail about the differences in the meaning of the word "ontology" between computer science, philosophy, and psychology – but the importance of such a paper is not to be understated [6]. To solve this problem in communication, the solution is itself communication. Standardizing vocabulary offers one outlet for such communication. Explaining differences in terms is another. Still another is creating businesses out of university research.

2.3.5 Summary of the Four Cyber Security Categories

To summarize all four categories, it is evident from this literature review that there is a long-standing disconnect between traditional technological research in cyber security and the public and private sectors' nontechnical dealings with cyber security. This problem is likely a combined issue resulting from neither technical researchers nor management in business or government reaching out to communicate to the other parties. However, there is also a communication problem between researchers in the same category. Fundamentally, communication among researchers and between

research fields and other sectors of society stands out as a stymieing problem for cyber security when the field is broadly analyzed.

It might appear that this thesis takes the supposed benefits of interdisciplinary research and communication for granted. Indeed, it may worry some readers that authors like Busse et al. propose such heavy collaboration between disciplines; perhaps it might cause a kind of regression towards the mean if all disciplines standardized communication. However, that is not what is proposed in this thesis. I propose only that cyber security workers take additional steps to work across the identified subdisciplines. Not allowing disciplines to grow together (by not participating in this growth by utilizing concepts from different disciplines), is itself a regression towards the mean of one's own discipline, if one believes that innovation is at the edge (of disciplines). While there are numerous edges to innovate on that research constantly takes advantage of, one particular edge – interdisciplinarity – is often overlooked. Interdisciplinarity and harmonized communication create a new innovation edge for cyber security. This assumption is used as the justification for the improvements to interdisciplinary cyber security communication presented in this thesis.

2.4 Comparison with Prior Research

After creating this classification of the field of cyber security, I came across some similar prior work. Delineation of the field of cyber security into four categories has recently been done by other initiatives as well. In 2015, the European CAMINO Project created the THOR acronym approach of "(T)echnical", "(H)uman", "(O) rganizational", and "(R)egulatory." The CAMINO Project asserts that cyber security can be comprehensively perceived as a combination of these four dimensions [82]. The THOR approach was put forth with the goal of creating an operational suggestion for a cyber security roadmap for Europe, and assumes integration of the four categories they proposed. This contrasts with my methodology of classifying the current state of research, which (empirically) highlights the lack of cooperation between the different categories, and more comprehensively describes the categories. In addition, the THOR model does not classify general research.

2.5 Literature Review Conclusions

The broad literature review I conducted reveals that cyber security is still a nascent and poorly defined academic field with little educational basis, and few formalized research methods that it can claim as its own, especially outside of cryptography. Cyber security is currently a primarily system-level discipline. Furthermore, most of its immediate implications lie outside of academia or the industry it caters to; it is a global and ubiquitous problem, with misaligned incentives between academia, industry, and governments.

However, there are some operational measures that can be taken to improve the pace and quality of security research; among them, is facilitating communication between scholars by standardizing terminology. It became apparent during the literature review that there is little to no standard

terminology, especially outside technical cyber security, of which, cryptography is by far the most formalized; however even the robustness of some practical implementations for private key encryption, such as AES, are supported not by rigorous mathematical proofs, but by popular vetting and the test of time [80]. Standardizing terminology when scientific and engineering practices have not been standardized may prove difficult. Alternatively, it might be a prerequisite for formalizing the engineering aspects of the field. Chapter 4 explores this more.

Another measure that could better align incentives between stakeholders is to create more university-level cyber security education. Formalizing the educational requirements for an academic "cyber security" discipline would help to improve collaboration and communication between researchers from the four areas of cyber security I identified. If many undergraduate institutions adopted a comprehensive concept of what "cyber security" as a field is, then future researchers, policymakers, and businesses can better tackle the ubiquitous system-level problems described in the articles and literature reviews I summarized in the previous sections (as can advisory faculty). In Chapter 3, I describe even more benefits (and perhaps more tangible ones) that creating broad cyber security curricula at universities will give the industry, and I outline the ongoing effort I am leading to create such an undergraduate program at MIT.

Chapter 4 also follows from this literature review, focusing on the lack of consistency in cyber security nomenclature, such as, as Choucri, et al. wrote, whether to use "cyber" as a prefix, as in "cybersecurity" or as an adjectival modifier (i.e. a separate word, as in "cyber security" or "cyber-security") [75]. Sometimes even within the same article there is no displayed agreement on this convention, and authors may vacillate between the two [84].

3 Interdisciplinary Cyber Security Education

3.1 Proposing a New Interdisciplinary Minor at MIT

This chapter follows directly from the conclusion of Chapter 2 that cyber security is a multidisciplinary yet fractured academic field. This chapter considers MIT as a case study for creating a minor in cyber security in order to improve communication across the boundaries of the four subdisciplines of cyber security identified in Chapter 2. As of this writing, an interdisciplinary minor in cyber security is an extremely novel construct at universities, there is no interdisciplinary cyber security education program in the United States. There are also no top 20 universities with formal undergraduate cyber security programs of any kind. Most importantly for the novelty of this chapter, there are currently no minors in cyber security in place at U.S. educational institutions. Despite its novelty, the idea of teaching cyber security as an interdisciplinary field has received support from both academia and governments, as described in Chapter 2.

Because this research is derived from my effort to create a new program at MIT – the Minor in Cyber Security – in this chapter, I describe the design of the minor specifically through the lens of MIT. Understanding MIT's subjects will help the reader to better follow the material in this chapter. For a better understanding of MIT's subjects and their numbering, please consult the MIT subject listing [176]. In the concluding section of this chapter, I describe how other institutions can adapt my model of cyber security to their own educational initiatives (Section 3.6.5). In this introduction I first explain how the interdisciplinary nature of cyber security lends itself well to developing an undergraduate minor program.

The structure of this chapter closely follows that for the official proposal form for an interdisciplinary (cross-departmental) undergraduate minor in cyber security to MIT's Committees on Curricula (CoC) and the Undergraduate Program (CUP). This chapter is hence structured in a Question and Answer format, following the structure MIT's Minor Proposal form. I drafted the rationale for this program on such a form on the CoC website, and it is available for faculty to modify in the future. At the end of this chapter, I discuss the details of the effort to put this proposal into action at MIT, and I outline how the ideas in the proposal can be applied at other institutions. The structure of this chapter is designed to mirror that of the official MIT proposal form (which is much briefer) in order to aid faculty who would like to develop this program at MIT or elsewhere in the future. There are many details involved in proposing the rationale of a new minor to MIT's bureaucracy, and they cannot be summarized independently from explaining the proposed curriculum as well. Because of this, I develop the rationale behind the design and necessity for a Minor in Cyber Security alongside the presentation of the actual curriculum of the minor.

Creating a new minor at MIT requires the support of a body of faculty who agree to maintain the program. Creating a minor is typically a grassroots effort that requires a mixture of approval from course instructors and some commitment to faculty to advise students. A minor also requires a

department to support administrative costs, which are usually small, and it needs the support of the deans in the schools that the subjects constituting the curriculum of the minor are based in. The primary hurdle to overcome when creating a new minor at MIT is getting a few faculty to commit some of their time to push for its creation. As part of creating this proposal, I have done much work communicating with faculty and getting them to sign on to the idea, but that crucial aspect of creating the minor is still a work in progress. However, this proposal assumes that it is a body of faculty collectively proposing the new program to a committee. As long as the faculty are committed, there is usually not problem creating such a program at MIT.

3.2 Rationale for an Interdisciplinary Program

Question: Describe the interdisciplinary construct of the program and the rationale for designing it as such.

Cyber security is quickly being recognized as a concern for business management, end-user safety, computer science, national and international politics, sociology, law enforcement, healthcare, financial institutions, the energy sectors, and mathematics. Quantum computation and its implications for cryptography draw together physicists, chemists, mathematicians, and computer scientists. The advent of the Internet of Things has caused every area of industry to become one for concern, with insulin pumps being hacked, and knowledge of both security and the field of industry being important for mitigating these problems. MIT's Department of Electrical Engineering and Computer Science (EECS, or Course 6) already has a large group of subjects with a medical focus. Other examples of the value of interdisciplinary knowledge for security include fault tolerance and industrial control systems security in the electrical grid, the oil and gas industry (chemical engineering), the merging of ideas of system safety from aeronautics (course 16), targeted cyber-attacks like Stuxnet (nuclear engineering – course 21), and the current challenge of properly designing and implementing a sustainable cyber insurance program (course 14, economics).

As argued in Chapter 2, security is inherently interdisciplinary because it aims to augment other fields, and it therefore embodies. While it is infeasible to expect every security professional to understand all of these fields that themselves embody entire careers, it is more feasible to expect students learning about those other fields to in term learn about security.

As I will repeatedly state throughout this chapter, the minor in cyber security is designed to give interested students exposure to all areas of this interdisciplinary issue, ensuring exposure to both the fundamental principles of technical cyber security and to the other areas with interdisciplinary concerns. The design of the minor in cyber security is informed by the fact that cyber security means more than just cyber, and more than just security. The study of networks, Internet

regulation, social interaction, global politics, management, system design, and finance are all affected by and affect this problem called “cyber security.”

A well designed interdisciplinary program would encourage security researchers at MIT to communicate more, thereby fostering greater idea flow and convergence of terminology and goals at MIT, which can additional serve as an example for other institutions. Standardizing terminology directly, as discussed throughout this thesis, is a means of solving this communication problem, but more fundamentally, it is a symptom of a lack of communication in what is actually a small community with a shortage of persons in the workforce, or talent.

In my proposal, I assume there are four ways to alleviate the talent shortage: shifting the burden; automation and outsourcing; distributing knowledge; and broadening educational offerings. One method to alleviating the talent shortage is for companies to lower their expectations for specialized professionals, and to instead hire more general software engineers for security work. Alternatively, jobs can be eliminated by innovative business-to-business products and services – a growing trend in security that I expect will temper the desire for every organization to have any dedicated security personnel. Such positions are currently more of a trade skill than a field of engineering.

A third method for closing the talent gap is for security to be provided by many people in an organization, distributing the work and knowledge for such tasks, especially among non-engineers. That is, rather than having dedicated security roles, simply expect security from other people whose jobs are not focused on security. Still another way is to provide more widely available educational resources for cyber security, including educating engineers in security policy and management. I have designed this proposal to enable the latter two means of reducing the talent shortage (distributing knowledge and broadening educational offerings), since those are the areas that academia is largely responsible for. I expect that a combination of these four methods is necessary for individual businesses to have enough cyber security human capital to remain relatively secure with the growth of IT infrastructure.

3.3 Educational Rationale

Question: Explain the educational rationale for the program, and its context with respect to the evolving intellectual trends in the relevant fields. Identify alternatives to creating a minor that you have considered, and how they measured up to your educational objectives.

3.3.1 Motivation and Justification

Cyber security is a growing market with a history of neglect and potential for long-term application, being one of the faster growing subdisciplines of computer science; and the current cyber security landscape represents an ad hoc ex post facto patchwork [143,146,148].

Cyber security is a multidisciplinary issue, with an often misunderstood or contested definition, requiring input from not only computer science but political science, management, mathematics, physics, engineering, and economics; and most workers in these areas have little interaction with workers in the other areas; and the current course 6 curriculum does not allow for such a diverse course load in a substantive amount; and most students remain unaware of the extent of this problem and are thus unlikely to decide to pursue it independently [144,145].

Cyber security is the smallest sub-field of computer science taught at MIT, not even being included in the list of EECS concentration fields, despite 3 cyber security centers being created on campus in 2015 [149]. Instead, security classes are grouped with systems subjects. This is valuable guidance for students, but does not fully equip students who want to gain specialized knowledge in security

3.3.2 Proposal and Applications

With the support of departmental faculty, I propose the creation of a new interdisciplinary undergraduate minor program, with a focus on foundational computer science and an emphasis on solving complex systems problems; and specific applications to cyber security; directed largely at course 1, 6, 14, 15, and 17 students, but designed to be accessible to all students, consistent with cyber security's multidisciplinary nature. Alternatives I considered for MIT were:

• The creation of a cyber security major:

> This option proved too rigid for the evolving state of the problems facing cyber security, and hiring needs of businesses. While other academic institutions had little or no support for programs such as minors in cyber security (they generally only have majors or certificates or master's degrees, and next to no non-technical education in these areas) at the time of the first drafting of this proposal, the proposal was shifted away from a major, and towards a more versatile area, such as a minor, due to MIT's role as an institution to set precedent; the interdisciplinarity of the problem; and cyber security's academic history (similar to environmental engineering, which MIT has a minor for).

• The creation of individual classes

> This has provided mixed results. Without formal impetus and advertising of the minor as a concern of the Institute, awareness of such subjects has not spread, nor have many targeted undergraduate subjects been created, despite professional demand for cyber security workers with bachelor's degrees (as well as demand by graduate schools). Many of the subjects in this proposal are already very popular among students, while others, especially newer pilot courses, have seen more modest enrollment of between 5 and 20 students. A minor would allow the most successful subjects to be naturally selected and refined while

the program continues on, and for topics to be spread between multiple subjects, rather than requiring faculty engaged in subject construction to cram as many distinct seminars into a class as possible (which also would result in no depth in the field).

3.4 Program Demand

Question: Describe the professional demand for this program and your general expectations regarding student enrollment in each of its first five years of operation.

- The "talent shortage" in cyber security is estimated to rise to approximately 2 million by 2019, and cannot be solved by standalone efforts by individual faculty. This shortage is often called the largest problem for the field, and is often cited by the industry for slowing the progress of security more than anything else [169].
- The human factor is cited as the greatest threat to cyber security, with simple human error and social engineering often leading to the plurality of reported compromises [174,175]. A widespread security culture is therefore useful for all professionals.
- MIT has recently seen a resurgence of interest in cyber security research, as stated above, but this interest is largely directed at graduate students and does not sufficiently attract undergraduates – in fact, undergraduates often are unaware of many pressing issues like cyber security, either because they do not know if they can work in those areas (due to lack of Undergraduate Research Opportunities advertising, for example), or because most subjects in this field are currently upper level undergraduate or graduate subjects, despite interest being displayed in them [source – personal communication].[1]
- Nevertheless, based on interviews with students, and enrollment numbers sourced from MIT Subject Evaluations [168], indicate that the average undergraduate enrollment in the subjects in the curriculum is 92, with a variance of 122. See Table 5 for averages by category. Based on these numbers, I believe that there is sufficient interest in the subjects that to expect substantial enrollment in the minor immediately.
- In recent years, more undergraduate students have begun to show interest in pursuing research or careers in cyber security, interests in studying more subject matter in cyber security, or a desire for more coursework to be made available to students. This includes course 6 students, course 17 students, and others. In addition, graduate students in MIT departments like IDSS and Sloan are increasingly displaying interest in cyber security. I expect that the average graduating class year of interested students will decrease in the next 5 years.
- I hope by the fifth year, one-third of students in the program will be from outside course 6.
- Like many minors, low enrollment is expected compared to a major. Based on enrollment statistics for cyber security classes in MIT's January Term (Independent Activities Period, or IAP), and the mean number of students who already take the subjects in the proposed curriculum, I estimated an upper limit of enrollment of 50 students in the program in the first

[1] From consulting with students in course 6-3, Computer Science from the Cybersecurity@CSAIL research group

4 years (4 years is the expected enrollment window for the statistics of undergraduate enrollment in these subjects).

Question: Identify any existing MIT programs whose enrollment could potentially be affected by the availability of this program. Describe the consultation process you have followed in reaching out to the departments or academic units and faculty responsible for these programs. How is this proposed program unique from these other programs?

Course 6 is the largest major at MIT, and a minor in Computer Science was recently created during the development of this proposal. That minor will likely affect dual enrollment in course 6 [172]. A minor in cyber security could also negligibly affect enrollment in course 6. However, since students in course 6 can minor in cyber security, but cannot minor in Computer Science, I expect that enrollment in course 6 will go largely unaffected by a minor like this. It might more so affect enrollment in the minor in Computer Science, either positively or negatively.

Awareness of the minor's curriculum could encourage even more students to consider studying some aspect of computer science, such as the minor in computer science. It may also discourage people who are only interested in cyber security from studying computer science what they believe to be the most relevant use of computer science. Support for the proposal by the EECS department would be given with this understanding in mind, so if the proposal makes it to that stage, it would not be a barrier to creation. I would like to conduct a survey of students across the institute to gauge interest, in order to better understand the effects this could have on enrollment in the minor in Computer Science. The survey I plan to send out is shown in Table 7.

3.5 Curriculum Design

Question: Describe the program, including its structure and coherence, its educational objectives, and any other relevant aspects of the overall educational experience. If the sponsoring entity does not currently offer this type of program (degree or minor), include the rationale for establishing a program within the unit.

As was discussed in Chapter 2, in order for cyber security professionals to solve the current issues they are faced with, it is imperative for the academic institutions training them to treat cyber security as a system-wide effort, involving national security and government, everyday consumers, and the businesses who serve them; including healthcare, entertainment, and other infrastructure.

For this reason, it is myopic to only consider pure computer systems in the study of cyber security. In the spirit of multidisciplinarity, appropriate subjects from nearly every department at MIT have been identified and documented in Table 6, covering issues present or emerging across these

disciplines; and many of these subjects have been integrated into the proposal, to allow all students to be aware of applications to their industry [162-165, 177].

By identifying existing areas in industry that are or may be sensitive to cyber security vulnerabilities, and by creating this minor program, educational gaps can be identified, and new subjects can be created to fill these gaps. By "educational gaps," I mean areas of study that were identified in Chapter 2 (and described in Table 2 and Table 6 as well) that are not taught as specific subjects at MIT or are not currently included in cyber security curricula at other institutions. These subjects can be integrated into the minor over time. Hence, while cyber security, as an emerging discipline and domain of concern, is still growing, its urgency demands education sooner rather than later, and so some degree of dynamism during its nascence is to be expected. As a leader in technology and industry, MIT is poised to create curricula for, and identify areas for improvement in, cyber security education across different sectors. Educational gaps are further described in Section 3.6.3 at the end of this chapter.

There are 11 institutions designated by the US government as cyber security centers for the DOE's new CREDC initiative (Cyber Resilient Energy Delivery Consortium) [151], many of which have created programs of study in cyber security; and there are a number of other universities recognized as National Security Agency (NSA)/Department of Homeland security (DHS) NSA/DHS National Centers of Academic Excellence (CAE) in Information Assurance (IA)/Cyber Defense (CD) [152].

Cyber Security Category	Examples of Topics Covered in Category
Policy and political science	Internet governance, China's "Great Firewall," incompatibility of national jurisdictions with cyberspace, national security
Business and management	Employee culture, The NIST cyber security framework, supply-chain management, ethics, cyber insurance, reputation of companies post-attack, information valuation
Electrical engineering and computer science	Robotics and machinery safety, cryptography, computer systems, network security, hacking, internet of things, hardware, cyber-physical systems and industrial control systems, quantum computing, operating systems, reverse engineering, system forensics, biometrics, medical device security
System-wide properties, involving social science, systems engineering, and endogenous and emergent properties of cyberspace	Cyber-crime, system dynamics, online behavioral psychology, the deep web and dark web, history of the Internet, game theory, anonymity & privacy

Table 2. Examples of topics from each of the four cyber security subdisciplines. Not exhaustive.

MIT can learn from examining these programs, to build up its own educational capacity in cyber security, and MIT can assist in providing an educational model to other universities and institutions (none of which have a minor in cyber security) by identifying the aforementioned education gaps. Work in this area for businesses (rather than for universities) is already underway in the MIT Sloan-based $(IC)^3$ group, one of the three new cyber security initiatives at MIT [153]. Despite the breadth of subjects suggested in Table 2 and Table 3, this does not dilute the organization of the minor, nor does this diminish its significance. To summarize, this Minor's benefits are raising *awareness* of issues across disciplines, providing *credentialing* of students to fill the talent gap, and *modeling* of new curricula for other institutions to follow.

3.5.1 Outline of the Minor

Chapter 2 recognizes that the current focus of cyber security falls under 4 [167]. Having identified the currently most relevant cyber security-related subjects at MIT (see Table 6 for these and their industry applications), as well as of curricula at other universities [154-156], I propose that these four categories, shown in Table 2, be used as a basis for creating the minor.

Programming Prerequisite (pick 1)
1.00, 6.00, 6.006, 6.009
Required Interdisciplinary Overview Subject
15.580/17.447
Required Technical Subject
1.125 (a graduate subject with an undergraduate equivalent in development)
Electives: Pick a total of four from three categories:
Computational Security (advisor approval required for graduate subjects)
6.005, 6.033, 6.857, 6.858, 6.875
Security Politics
STS.085, 17.445, 17.468, 6.S978, 17.424, Harvard Law 2306, 17.486, 22.814, course 17 special subjects like 17.S919
Secure Management
14.160, 15.8741, 15.564, 15.565, 15.567 & 15.570, 15.569, 14.27, 15.763, EC.712
Online Sociology
6.207, STS.441, STS.434, STS.086, STS.008, CMS.628, EC.712, 21A.156, 14.31, CMS.614, MAS.S61
Research and Specialization
18.424, 18.783, Other Computational Security subjects, or any of the following graduate subjects, with advisor approval: 1.208, 6.241[J], 6.263[J], 6.820, 6.876, 16.420, 16.422, 16.63[J], 18.405, 18.435[J], 18.436[J], 20.451[J], 22.107, IDS.505, MAS.600, MAS.862, 6.443, ESD.162[J], 18.424

Table 3. Compact description and list of classes proposed for MIT's Interdisciplinary Cyber Security Minor.

Therefore, based on existing available coursework, and with the intention of encouraging the creation of additional subjects in the future to benefit students by filling educational gaps, I propose the curriculum in Table 3 for the undergraduate Minor in Cyber security consisting of seven subject requirements [147].

A more detailed breakdown of the minor is included in Table 4, which contains subject names and units, and is formatted for the MIT Catalog (and excludes graduate subjects); and in Table 5, which describes substitutions and graduate subject alternatives that require advisor approval, as well as term offerings and enrollment statistics.

As is common policy for minors at MIT, a minimum of four subjects taken for the Minor in Cyber Security cannot also count toward a major or another minor. Students must receive permission from their minor advisor prior to registering for a class at another institution (such as at Harvard Law School, where MIT students can cross-register).

3.5.2 Detailed Explanation of Curriculum

This section explains the rationale behind the design of each element of the curriculum.

3.5.2.1 Computer Programming Prerequisite

A programming prerequisite is needed in order to give all students an equal footing within the minor. However, many MIT courses (majors) already have a programming requirement – something I would like to voice support for as a General Institute Requirement (GIR). These subjects were chosen based not only on the literature review and survey, but also on the opinions of course 6 students, including students in cyber security research labs. In particular, the ability to handle a class like 6.858 after taking only a class like 1.00 was determined to be positive. Students might be able to count 6.858 towards the Minor by getting approval from their advisor. Although graduate-level subjects like 6.858 are not allowed to be required subjects in an undergraduate minor (and need advisor approval to take), some existing MIT programs also give students the option of taking a subject whose formal prerequisites are not part of the curriculum [140]. Subjects with prerequisites that lie outside of this curriculum are listed in Table 5.

Students who are majoring in a course that already includes basic computer programming in the curriculum should be encouraged (but cannot be required by MIT policy) to take an additional programming class. They may also substitute a more advanced subject for the standard prerequisite. Students who are already studying computer science (who are expected to be in the majority of enrollees, since the plurality of students at MIT are in course 6 [171]) should be encouraged to take graduate-level security subjects beyond the Minor, since they will likely take 6.00, 6.005, and 6.033 anyway. For other majors, 6.00, 6.005, and 6.033 will be more than sufficient. This is so that more students are exposed to advanced cyber security concepts that are included in subjects like 6.033. The reason students in majors without a programming

requirement should not have to take classes from the Computational Security category is because those students are less likely to apply their cyber security knowledge directly through interactions with computers via a programming interface; but the mere exposure to introductory programming compounded with the rest of the program (which includes additional programming anyway, in the form of the required technical subject) will efficiently optimize students' learning about important cyber security concepts as such concepts pertain to students' specific areas of interest.

3.5.2.2 Required Subjects

There are two required subjects. The first is a seminar-style overview of topics in cyber security designed to introduce students to the practical goals of the subject. This class is important because it cuts across disciplines, exposes students to a number of prominent researchers at MIT and elsewhere (and simultaneously fosters relations among said researchers), and situates students' studies in a shared context that they can take with them when taking elective classes. This is important because by introducing the shared context in an interdisciplinary required subject, the need for the teachers of elective subjects to drastically change the narrative or the application focus of their classes is greatly reduced to an extent such that teachers of elective classes can feel free to either slowly integrate current cyber security content, or their opinions on it, into their class, or else simply mention at the beginning of the semester that the class is part of the cyber security minor program and subsequently not dwell on emphasizing how the subject fits in, but rather leaving that to the students to organically discover. This is important because it promotes creativity in approaching the broad field of cyber security, and will lead to innovative solutions from students from all courses.

The second required class is a technical class focused on understanding the challenges facing real-world enterprise infrastructure, with applications to security as well as to related areas like data management and machine learning. This accessible course, taught by leading cyber security researchers, gives students the common minimum skillset necessary to pursue cyber security from a technical and practical perspective, and experience state-of-the-art computer programming in action. This serves to provide students with competitive technical credentials and a technical addition to their broad cyber security worldview.

3.5.2.3 Electives

Next, there are the elective categories. Why are categories necessary at all? For proper breadth in the field. It is reasonable to assume that students would naturally gravitate, for various reasons, toward subjects in their own department, e.g. a 6-3 student preferring to take course 6 classes for the minor. This defeats the purpose of exposing the long-overlooked multidisciplinary nature of cyber security that inexorably affects the field as a whole. Thus, limiting students (within the minor's curriculum) to two courses in any given category and demanding they branch out to other categories with comparable depth ensures a proper introductory understanding of cyber security. The second through fifth categories are designed

for breadth (2nd, 3rd, and 4th), and even further depth into the technical study and research of cyber security (5th), perhaps with specialization in one's primary field. Students can also be exposed to research groups from MIT and Harvard that span the four areas of cyber security if they take subjects from these four categories. This fulfils the goal of the Minor to bring researchers from the four subdisciplines closer together – especially because course instructors may have to collaborate as part of the Minor.

The extensive course list comprising the minor further provides students, whether they are interested in the full minor or not, with a resource on particularly salient coursework available at the Institute for further study outside of the minor requirements, should it pique their interest to pursue these issues in even more depth or through a partial foray (aligning with the minor's mission of awareness). Thus, it does not restrict study to a broad overview - nor does this author think the minor provides mere breadth anyway, but sufficient depth on its own; hence, fulfilling the credentialing aspect intended. In addition, the choices given to students in this proposal reflect the variety and number of choices available to students in many other minors [141].

In the first category, the "Computational Security" category, are course 6 subjects in "traditional" computer security such as cryptography and network security; as well as important subjects for learning the state of cyberspace and cyber security, their history, potential, and research agendas. This category consists of graduate subjects that typically have about a 70-80% undergraduate enrollment, and is more geared towards students wishing to immerse themselves in the technical profession of security. Since these are graduate subjects, they are not allowed to be part of the official curriculum (described in Table 4, so advisor approval is required to apply subjects in this category besides 6.005 and 6.033 toward the minor. The 800-level subjects might be appropriate as capstones for a course 6 student.

The second elective category covers issues of policy, governance, and international security; it is intended to provide the student with a national and global mindset of cyber security, and to give them basic tools to solve pressing problems in the political realm. Such problems often propagate down to the most basic functions and administration of the Internet.

The third category addresses the aspect of cyber security most neglected by academia: business. One need only read the news for regular examples of cyber security affecting business [157-161]. Managers are oblivious to the problems surrounding IT, and computer scientists are unaware of the full scope of computer security's importance in business practice [145]. Awareness of how to handle information and computing systems in the workforce is an indispensable skill for both software engineers and managers, regardless of the company size. Many MIT students go on to build their own companies. There are some estimates that small businesses comprise up to 70% of all cyber-attack victims [173].

The fourth category may be less intuitive, or less well served by MIT's existing coursework; and it may benefit most (along with EECS) from additional security-focused or system-focused subjects being created to fill educational gaps. The ability to think of complex systems problems, and to situate cyber security as one, provides for long-term continued growth for students in an ever-changing field that was once viewed as quite rigid. Moreover, an understanding of the social aspects of cyberspace and how the very nature of the ideas behind computers and the Internet creates properties of the system, such as security flaws and culture, will help professionals and entrepreneurs to identify further problems and construct meaningful solutions beyond anything a curriculum might be able to statically lay out. More than any other category, this one encourages creativity and adaptive approaches to cyber security.

Lastly, the fifth category is geared toward students wishing to pursue technical aspects of cyber security in more depth in a particular field. Advanced cryptography, industrial control systems, and healthcare Internet of Things technology are all examples of courses that might be found in this category. The design of the minor ensures experience in both technical and nontechnical aspects of cyber security. Moreover, since cyber security is an interdisciplinary field, most of the subjects in the fifth category will be beneficial for any student enrolled in the program. The minor's introductory subjects should aim to make that concept of interdisciplinarity intuitive to students.

3.5.3 Formal Program Narrative

Figure 1. Program Narrative for a Cyber Security Minor. The description that would be published in MIT's Catalog if this minor were created (modeled off the Interdisciplinary Energy Studies Minor at MIT) [170].

> "Cyber Security is a fundamentally multidisciplinary topic. Securing the world's information and communications systems requires combining expertise from numerous fields in engineering and technology, management and social science, and policy. A diversity of disciplinary perspectives is necessary to equip students to work in this complex, evolving field.
>
> The Cyber Security Minor for undergraduates is an Institute-wide program that complements the deep expertise obtained in any major with a broad understanding of the interlinked realms of technology, management, policy, and social sciences as they relate to security and associated computational challenges. The minor curriculum integrates these four domains in a thoroughly multidisciplinary program. The Cyber Security Minor Oversight Committee, including faculty representatives from three Schools, oversees the Cyber Security Minor program.
>
> The Cyber Security curriculum has two components. The first is a core that provides an integrated perspective on security and associated computational challenges in four domains, including a basis in computer programming and computational thinking, an advanced technical class (System-Level Computational Design and Architecture), and a seminar colloquium covering major challenges and modes of interdisciplinary thinking in the cyber security context, presented by leading researchers and practitioners. The second component is a customized program of electives that is selected by each student in close consultation with his or her Cyber Security Minor faculty advisor."

Figure 1 and Table 4 give a formal description of the minor as it would appear to students in the MIT Catalog. These descriptions are an important part of any proposal for a new minor at MIT.

Required Subjects		
Select one of the following: [1]		12
1.00	Engineering Computation and Data Science	
6.00	Introduction to Computer Science and Programming	
17.447	Cybersecurity	12
Required technical subject: 1.125		12
Electives		
Select four subjects from at least three different categories:		48
Computational Security		
6.005	Elements of Software Construction [2]	
6.033	Computer System Engineering [2]	
Security Politics		
17.445	International Relations Theory in the Cyber Age	
STS.085[J]	Foundations of Information Policy	
Secure Management		
14.27	Economics and E-Commerce	
15.8741	System Dynamics for Business Policy	
EC.712	D-Lab: Information and Communication Technologies for Development (ICT) [3]	
Online Sociology		
6.207[J]	Networks	
14.31	Data Analysis for Social Scientists	
21A.156	Introduction to Sociology	
CMS.614[J]	Network Cultures	
CMS.628	Advanced Identity Representation	
EC.712	D-Lab: Information and Communication Technologies for Development (ICT) [3]	
STS.008	Technology and Experience	
STS.086[J]	Cultures of Computing	
Research and Specialization		
18.424	Seminar in Information Theory [2]	
18.783	Elliptic Curves [2]	
Total Units		84

[1] *Students may substitute a more advanced programming subject, such as 6.006 Introduction to Algorithms.*

[2] *Subject has prerequisites that are outside of the program.*

[3] *Counts toward either Secure Management or Online Sociology category, but not both.*

[4] *Consult minor advisor about potential substitutions.*

Table 4. Formal description of the Cyber Security Minor. Units for the requirements are shown on right.

3.6 Practical Implementation of a Minor in Cyber Security

3.6.1 Accessibility to All Students

Question: Describe how students from a range of majors and different entry points can complete the minor.

The Minor is designed to ensure students have the minimum programming experience necessary to understand cyber security, and thus integrates it into the curriculum. Based on interviews with course 6 students, the fundamental technical subjects in cyber security, (which would be of greatest concern to students outside of course 6 without rigorous programming backgrounds), are approachable with only an introductory background to programming. These subjects are graduate subjects and include 6.857, 6.858, and 6.875 (see Table 5 for subject names).

The proposed subject selection is extensive, and is designed to serve different areas of focus, interest, and ability. Because subjects in each category are drawn from multiple courses, students (especially outside of computer science), would approach the study of cyber security from a truly interdisciplinary viewpoint. Only subjects with minimal prerequisites are included as mandatory subjects in the curriculum. Some example curriculum roadmaps (a necessity for a successful proposal for a new minor at MIT) are given in Figure 2.

3.6.2 Long-Term Plans

Question: Summarize any long-term plans for further developing the curriculum and/or expanding student enrollment beyond the initial years of operation.

The faculty oversight committee will:

- create and maintain a program website.
- work with faculty and staff to devise new undergraduate coursework over time.
- devise a long-term plan for keeping the core seminar and technical subjects current.
- devote resources to advertising the program to the student population.
- expand research and education at MIT in cyber security to ensure continued support for related initiatives.

3.6.3 Individual Cyber Security Classes at MIT

The required technical subject (currently proposed as an undergraduate equivalent of 1.125) is in development right now by the professor of 1.125. This new subject may end up being a more security-focused alternative to 1.00, or a follow-on. In either case, it may then be better to require 6.00 or some equivalent introductory programming subject as the prerequisite, but perhaps not allow 1.00; and then to have this new class be the required technical subject, whether it is a replacement for 1.00 or is closer in content to 1.125.

Figure 2. Example Curriculum Roadmaps
Elective category codes: C = Computational Security, P = Security Politics, M = Secure Management, S = Online Sociology, R = Research and Specialization; A = Advisor Approval Required

Timeline-based roadmaps

Student beginning program as 1st semester sophomore	
1st semester sophomore year	6.00
2nd semester sophomore year	15.580[J] Cybersecurity
1st semester junior year	STS.085[J] (P); 1.125
2nd semester junior year	14.31 (S)
1st semester senior year	14.27 (M)
2nd semester senior year	STS.086[J] (S)

Student beginning program as 2nd semester sophomore	
2nd semester sophomore year	21A.156 (S)
1st semester junior year	1.00; STS.085[J] (P)
2nd semester junior year	15.580[J] Cybersecurity
1st semester senior year	1.125; 17.445 (P)
2nd semester senior year	15.8741 (M)

Student beginning program as 1st semester junior	
1st semester junior year	6.00; 14.27 (M)
2nd semester junior year	15.580[J] Cybersecurity; CMS.614 (S)
1st semester senior year	1.125; STS.085[J] (P)
2nd semester senior year	15.8741 (M)

Course-based roadmaps

Course 14 student with no programming experience	
Programming Prerequisite	6.00
Security Politics	STS.085[J]
Secure Management	15.8741; 14.27
Online Sociology	STS.008

Course 7 student with some computing background	
Programming Prerequisite	1.00
Secure Management	15.8741
Online Sociology	21A.156
Research & Specialization	MAS.600; 20.451[J] (A)

Course 6 student interested in broadly exploring cyber security	
Programming Prerequisite	6.00
Computational Security	6.005; 6.033 (or 6.857 (A); 6.875 (A))
Security Politics	17.445
Secure Management	14.27, EC.712 D-Lab
Research & Specialization	18.435

Course 6 student with an interest in research	
Programming Prerequisite	6.005 (A)
Computational Security	6.8033; 6.858 (A)
Security Politics	STS.085; 17.445
Research and Specialization	6.820 (A); 18.783

As was mentioned earlier, the required subject "Cybersecurity" is a seminar class that covers a range of nontechnical cyber security topics. This class has only been taught twice as of this writing, and would benefit from involvement from faculty from an even wider range of departments (currently it draws on course 6, 15, and 17, as well as from industry lecturers)

Lastly, MIT would benefit from additional technical cyber security subjects, as would many universities. Examples of such subjects are reverse engineering or anomaly detection and other applied machine learning. Research Scientists in the Computer and Artificial Intelligence Laboratory (CSAIL) have been considering creating subjects like these, but course 6, and MIT in general, does not like to give students "bags of tricks," [source: personal communication, quoted from David D. Clark].

3.6.4 State of Development at MIT

Creating a new minor at MIT requires the support of a group of faculty above all else. For this particular effort, as of this writing, a group of faculty from multiple departments who are willing to be part of the oversight committee for the Minor has been assembled. I have also spoken with members of the CoC and CUP on several occasions. The next steps would be for those faculty to work with one or more departments to secure a commitment for funding for administrative costs of the program. In order to accomplish this, a "champion" faculty is usually needed. Most faculty that I have asked to champion the proposal have been too busy to commit to anything other than simply teaching their current cyber security subjects or advising students in the minor.

The next steps are then to ask the few remaining faculty that I have not asked who are involved in security teaching and research if they would like to take ownership of this idea at MIT. Once that is accomplished, letters of approval from the deans from each of the departments of subjects that are part of the core curriculum are required, along with some kind of commitment from the course instructors and acknowledgement that enrollment in their subjects may be affected by the existence of this program. After that, the proposal can move forward to the CoC and CUP, and with luck may succeed in the 2018 academic year.

3.6.5 Applicability to Other Universities

This chapter explored and detailed many concepts regarding the design of an ideal higher-education interdisciplinary cyber security program. The presentation of this design in the context of a specific effort at MIT may make it difficult for non-MIT readers to immediately be able to apply these design concepts to other universities. In the spirit of providing a model curriculum design that is applicable to other institutions, I conclude this chapter by summarizing the major steps to take when creating similar programs at other institutions or creating online courseware.

- Curriculum designers should read Chapter 2 to understand the scope of cyber security

- Curricula should be designed by faculty or students from multiple departments
- A review of existing coursework from the entire university should be done, and subjects should be classified into security categories with the aid of Table 1
- Subjects should be balanced in the curriculum to ensure that students are given programming experience and some breadth and depth in as many security categories as possible (see Table 2 and Table 6 for some applications to try to cover), with a slight preference for flexibility in allowing students to design their curricula
- Subjects should be developed or refined to round out the security categories
- Keep in mind that, although this design can be extended to create or revise majors in cyber security studies, the primary intention of this design is to make it accessible to as many students as possible; hence this design is specifically for a minor

This concludes the discussion on how to bring the disparate disciplines of cyber security closer together in understanding through educational programs. As described in this chapter, there are many other benefits to creating interdisciplinary cyber security education programs as well; and the concept of a minor in cyber security is the primary novel contribution of this chapter.

The next chapter continues off from Chapter 2 and discusses the state of terminology differences between the four categories identified in the literature review. In Chapter 4, I propose methods for harmonizing security terminology across disciplines. I also propose a few standard words and phrases by identifying emergent trends in scholarly usage; and I discuss the benefits of using consistent terminology in scholarly cyber security articles.

3.7 Appendix

New Program Proposal

Changes saved but not submitted

Viewing: MIN-6 : Minor in Cybersecurity

Sponsor(s)/Author(s)

Name	E-mail	Phone
Robert Ramirez	- redacted -	- redacted -
Stuart Madnick	- redacted -	- redacted -
Nazli Choucri	- redacted -	- redacted -
Abel Sanchez	- redacted -	- redacted -

Effective Catalog
2017 - 2018
Academic Level
Undergraduate
Program Type
Minor
Name of Program
Minor in Cybersecurity
Administrative Department
Electrical Engineering and Computer Science (6)
Is this program Interdisciplinary?
Yes
Does the sponsoring entity currently offer an undergraduate degree?
Yes
Identify all participating academic departments

Department(s)
Electrical Engineering and Computer Science (6)
Civil and Environmental Engineering (1)
Economics (14)
Political Science (17)
Mathematics (18)
Management Programs (15)
Comparative Media Studies / Writing (CMS)
Science, Technology, and Society (STS)
Edgerton Center (EC)
Anthropology (21A)

Figure 3. Proposal Form Cover Page. Image of the current proposal for a minor in cyber security on the CoC website. Note that "cybersecurity" is spelled as a single word here.

Table 5. Detailed list of Cyber Security Minor subjects. Latest enrollment in parentheses.
Graduate subjects may be taken w/ advisor approval.
U = undergraduate, G = graduate
F = fall, S = spring, O/E = offered every odd/even year (with respect to the fall semester)
† Subject has 1 external prerequisite or corequisite
‡ Subject has 2 external prerequisites or corequisites

Programming Prerequisite (pick 1): (average enrollment: 145)

Pre-Approved subjects *(starred subjects may not double-count towards a major)*:
*1.00 Engineering Computation and Data Science (31) – U/S
*6.00 Introduction to Computer Science and Programming (186/131) – U/F/S:
6.006 Introduction to Algorithms (272) – U/F/S
*6.009 Fundamentals of Programming (117) – U/F/S
Or any 9+ unit course 6, 1, or ESD/IDS programming class (advisor approval required)

Required Interdisciplinary Overview Subject: 15.580/17.447 Cybersecurity – U/S/E

Required Technical Subject: 1.125 Architecting & Engineering Software Systems (19) – U/F (currently only a graduate listing exists – undergraduate listing WIP)

Electives: Pick a total of four from three categories:

Computational Security: (average enrollment: 335 undergrad, 195 all)
6.005 Elements of Software Construction (241) – U/S‡
6.033 Computer System Engineering (428) – U/S†
6.857 Network and Computer Security (127) – G/S‡
6.858 Computer Systems Security (126) – G/F‡
6.875 Cryptography and Cryptanalysis (54) – G/S‡

Security Politics: (average enrollment: 13)
STS.085[J] Foundations of Information Policy (21) – U/F
17.445 International Relations Theory in the Cyber Age (5) – U/ F
6.S978 Privacy Legislation in Practice: Technology and Law (40) – G/S
17.468 Foundations of Security Studies (10) – G/F
17.424 International Political Economy of Advanced Industrial Societies (5) – G/S
22.814 Nuclear Non-Proliferation (10) – G/S
Harvard Law: Communications and Internet Law and Policy (2306) (20)
Other subjects with advisor approval

Secure Management: (average enrollment: 146 undergrad, 85 all)
14.27 Economics and E-Commerce (16) – U/F/E
15.8741 System Dynamics for Business Policy (~268) – U/F/S
EC.712 D-Lab: Information and Communications Technologies for Development (7) - U/F
14.160 Behavioral Economics – G/F†

15.564 IT Essentials II: Advanced Technologies for Digital Business in the Knowledge Economy (N/A) – G/S
15.565 Digital Evolution: Managing Web 3.0 (24) – G/F
15.567 & 15.570 (both):
15.567 The Economics of Information: Strategy, Structure and Pricing (85) –G/F
15.570 Digital Marketing and Social Media Analytics (171) – G/F
15.569 Leadership Lab: Leading Sustainable Systems (N/A) – G/F
15.763[J] Manufacturing System and Supply Chain Design (75) - G

Online Sociology: (average enrollment: 32)
6.207[J] Networks (68) – U/S/O†
16.400 Human Systems Engineering (46) – U/F
STS.008 Technology and Experience (16) – U/F
STS.086[J] Cultures of Computing (14) – U/S
CMS.614 Network Cultures (12) – U/F/S
CMS.628 Advanced Identity Representation (N/A) – U/F
21A.156 Introduction to Sociology (25) – U/F
14.31 Data Analysis for Social Scientists (43) – U/S
MAS.S61 Social Physics – G/F
STS.441 Technology and Self: Technology and Conversation (7) – G/F
STS.434 Mobility & Global Society (1)

Research and Specialization: (average enrollment: 17 undergrad, 19 all)
18.424 Seminar in Information Theory (15) – U/F‡
18.783 Elliptic Curves (18) – U/S/E†
Other Computer Security Foundations subjects, or any of the following graduate subjects, with advisor approval
1.208 Resilient Infrastructure Networks (7) – G/F†
6.241[J] Dynamic Systems and Control (21) – G/S†
6.263[J] Data-Communication Networks (7) – G/F/O†
6.820 Foundations of Program Analysis (35) – G/F/O†
6.876 Advanced Topics in Cryptography (15) – G/F/O
16.420 Planning Under Uncertainty (15) – G/F/O†
16.422 Human Supervisory Control of Automated Systems – G/F/O
16.63[J] System Safety (5) – G/F
18.405 Advanced Complexity Theory (23) – G/S/O‡
18.435[J] Quantum Computation (76) – G/F
18.436[J] Quantum Information Science (20) – G/S
20.451[J] Design of Medical Devices and Implants (12) – G/S
22.107 Computational Nuclear Science and Engineering (5) – G/S/E
IDS.505 Engineering, Economics, and Regulation of the Electric Power Sector (29)-G/S
MAS.600 Human 2.0 (9) – G/S
MAS.862 The Physics of Information Technology (9) – G/S

Table 6. Examples of Cyber Security coursework and topics at MIT. Issues in cyber security with existing relevant coursework at MIT. Only issues with related MIT subjects are listed.

Transportation, City resources, robots, human augmentation, automatic data collection privacy, national security, nuclear power, e-commerce, business, airlines, developing countries, cryptography, online culture and identity, interactive environments

Course **1**: 1.041, 1.208, 1.234, 1.274 (trains and planes, industrial control systems, supply chain faults)
Course **2**: 2.737, 2.782 (mechatronics, manufacturing faults)
Course **3**: 3.154, 3.156, 3.43 (electromagnetic threats and faults, photonics security, microelectronics hacking)
Course **4**: 4.217 (disaster resilience)
Course **6**: 6.805, 6.852, 6.857, 6.858, 6.875 (information policy, network security, system security, cryptography)
Course **9**: 9.40 (neuronal networks)
Course **11**: 11.205, 11.520, 11.457, 11.477 (GIS, Smart cities, energy infrastructure)
Course **14**: 14.27 (e-commerce)
Course **15**: 15.564 (business in the digital age)
Course **16**: 16.420, 16.63, 16.891 (system safety, space policy)
Course **17**: 17.448 (international relations cyberpolitics)
Course **18**: 18.436, 18.783 (quantum computing, elliptic curves)
Course **20**: 20.451[J] (medical device security)
Course **21A**: 21A.156, 21A.504 (sociology, online culture)
Course **22**: 22.107 (computational nuclear engineering)
Course **AS**: AS.401 (national security)
Course **CMS**: CMS.828 (online identity evolution)
Course **EC**: EC.712 (IT for developing societies)
Course **ESD**: ESD.162 (power sector)
Course **MAS**: MAS.664, MAS.600, MAS.836, MAS.862 (physics and IT, cyborgs, security and the media, interactive environments)

Table 7. Survey to undergraduate students at MIT.

Gauging Interest in a new Undergraduate Interdisciplinary Minor in Cyber Security

Students and faculty from course 6 and other departments at the Institute have been developing a proposal for a new Minor in Cyber Security. The intention of this survey is to gauge potential enrollment in such a program, awareness of current cyber security subject offerings at MIT, and any effect this program might have on enrollment in the recently created Minor in Computer Science, or in course 6. Some of the core subjects in the current proposal for a Minor in Cyber Security are given below. Many other similarly-themed electives are also included in the proposed curriculum.

Prerequisite:

6.00 Introduction to Computer Science and Programming
Required Subjects:

17.447 Cybersecurity

1.125 Architecting & Engineering Software Systems*

Select four subjects from at least three different categories:

Computational Security:**

6.005 Elements of Software Construction

6.033 Computer System Engineering

Security Politics:

17.445 International Relations Theory in the Cyber Age

STS.085[J] Foundations of Information Policy

Secure Management:

14.27 Economics and E-Commerce

15.8741 System Dynamics for Business Policy

Online Sociology:

6.207[J] Networks

21A.156 Introduction to Sociology

Research:

18.424 Seminar in Information Theory

18.783 Elliptic Curves

***an undergraduate equivalent is being developed**
****G-level security subjects like 6.857, 6.858, and 6.875 require advisor approval to count towards the minor**

* 1. Are you an undergraduate at MIT?

- ◯ Yes
- ◯ No

* 2. What is your expected graduation date?

- ◯ 2017
- ◯ 2018
- ◯ 2019
- ◯ 2020
- ◯ 2021

* 3. What is your course? Select all that apply.

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5
- ☐ 6-1
- ☐ 6-2
- ☐ 6-3
- ☐ 6-7
- ☐ 7
- 8
- ☐ 9
- ☐ 10
- ☐ 11
- ☐ 12
- ☐ 14
- ☐ 15
- ☐ 16
- ☐ 17
- ☐ 18
- ☐ 20
- 21
- ☐ 21A
- ☐ 21G
- ☐ 21H
- ☐ 21L
- ☐ 21M
- ☐ CMS
- ☐ 21W
- ☐ WGS
- ☐ 22
- ☐ 24
- STS

* 4. Would you enroll in a Minor in Cyber Security if one existed?

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Yes, if it had existed sooner

* 5. Do you plan on enrolling in, are you currently enrolled in, or would you have enrolled in, the recently created Minor in Computer Science?

- ◯ Yes
- ◯ No

* 6. Would the existence of a minor in cyber security discourage you from enrolling in A) the course 6 Major or B) the Minor in Computer Science?

- ☐ Yes (major)
- ☐ No (major)
- ☐ Yes (minor)
- ☐ No (minor)

* 7. Having read this description of the proposal for a Minor in Cyber Security, do you feel more aware of the extent of current Cyber Security-related subject offerings at MIT?

- ◯ Yes
- ◯ No

* 8. In your opinion, did you know what Cyber Security as an academic discipline was before reading the proposed curriculum?

- ◯ Yes
- ◯ No

4 Harmonizing Terminology Across Disciplines

DISCLAIMER
This chapter is heavily based on an edited version of prior work.

4.1 Introduction

Chapter 2 commented on a disparity in the jargon used by authors from the different subdisciplines of cyber security. This disparity is evident in both the differing focuses of the separate fields, as well as in the differing phraseologies of the fields which were nevertheless used to describe similar concepts – with conflicts sometimes existing even within a single article [84]. This chapter expounds on this finding, and further examines the lack of consistency in cyber security nomenclature. I use the articles from the literature review covered in Chapter 2 as a basis for analyzing how common domain-specific terms are in recent literature, and how they have evolved over time. For those who have not read Chapter 2, the four categories of cyber security are Policy, Infrastructure, Business, and General Research. See Table 1 for details.

The contributions of this chapter are threefold. First, guidelines are proposed for authors and standards bodies to consider when selecting terms to use in writing (for example, for keyword indexing, or for communication in general), or for developing standard lexicons in the future. Examples of guidelines include prevalence and occurrence of terms, linguistics, and the involvement of governing bodies. Second, some recommendations for using specific words and phrases in cyber security writing are proposed and justified, based on these guidelines. Third, using the four general silos that cyber security research falls into, the terminology tendencies of each of the fields are quantitatively identified, further confirming the initial observation of disparate disciplines working on similar problems.

This chapter is laid out as follows. Section 4.1 describes the research method, the need for standardized cyber security terminology, and prior work. Section 4.2 describes the data and suggest guidelines for future terminology standardization efforts. Section 4.3 presents the terminology differences between the four categories of cyber security. Section 4.4 applies the guidelines from Section 4.2 to some of the keywords (often used by journal databases for indexing purposes, and often author-supplied) that were extracted from the literature review, to propose terminology standards. Section 4.5 is a broader commentary on other issues of jargon for describing cyber security and Internet-technology Section 4.6 concludes.

4.1.1 Method

To analyze the most relevant terminology used in the papers reviewed, I extracted all the author-supplied keywords from the reviewed articles. In addition to author-supplied keywords, some

terms of interest were also extracted from titles. Scopus and IEEE Xplore were searched for articles published from 2010 to 2015 to determine the recent incidence of these terms. For added completeness, the following terms were added to the set of search terms: computer security, cyber domain, cyber war, cyber bullying, cyber physical, semantic web, semantic web search, cyber safety, cybernetics, sustainability, darknet, dark web, deep web, surveillance, cryptography, cryptology, encryption, and cryptanalysis. These searches were performed on Scopus c. 10/7/2015 – 10/13/2015, and on IEEE Xplore c. 10/12/2015 – 10/13/2015. The author-supplied keywords were enclosed in quotes to ensure exact matches (up to capitalization). Scopus and IEEE Xplore treat hyphens as spaces, so they did not differentiate between "cyber security" and "cyber-security." The number of hits for the terms (that is, the number of articles published that include these keywords) returned by Scopus and IEEE Xplore are graphed on a logarithmic scale in Figure 6. Terms in Figure 6 are sorted alphabetically. Note that, due to the large number of articles indexed by Scopus, searches of IEEE Xplore returned about an order of magnitude less hits than Scopus, for most terms.

Table 11 sorts the terms by their number of search hits, and categorize the searched terms based on their incidence in IEEE Xplore, Scopus, and in total, with respect to powers of 10. Double-counting in the union of Scopus and Xplore term hits was not accounted for in this study, as only a general measure of academic use of these terms is important for drawing conclusions. Hits from the individual databases (Scopus and IEEE Xplore) are considered in conjunction with the totals when conclusions are suggested herein.

4.1.2 Discussion of Data and Argument for Terminology Standardization

Inspection of Table 11 revealed many terms that will undoubtedly be unfamiliar or seem informal to most readers. The lack of consistent nomenclature observed in Table 11 is not solely attributable to the unanswered question of how to properly form compounds and phraes with "cyber," which itself is a significant question; the discrepancies extend to whether "cyber" is always the most appropriate term; why we speak of "e-commerce" and not "online commerce," why "*online* psychology" but "*cyber* bullying" or (recently) "cyberpsychology" [85].

While these latter terms may seem somewhat familiar to readers, many other terms that one encounters when reading cyber security articles, especially nontechnical articles, are used rarely or only a few times, and can often seem ad hoc. Often when they are used, they are not rigorously defined or properly contrasted with other, perhaps more appropriate terms: should we speak of "cyber *security*," "cyber *resilience*," or "cyber *safety*" [79,82]? Many of these terms, given different definitions of cyber security, are actually subsumed by it: cyber security has been categorized into such stages as Identify, Protect, Detect, Respond, and Recover; or Confidentiality, Integrity, and Availability. *Resilience* and *safety* are arguably covered in those categorizations [83].

In some ways, use of cyber security terminology has begun to resemble the loosely-defined grammar of online fora, with contributors communicating in a mostly (but not always) mutually

intelligible language that is just good enough [86]. With the rapid growth of cyber security, terminology standards that are currently just "good enough" will soon be overdue. Fields such as healthcare, chemistry, and electrical engineering all devote much effort to standards, including terminology [87-89]. While cyber security is not as old as these fields, losses from cyber-crime alone amount to approximately 1% of world GDP, and although this is not yet as large as health expenditures, that number does not include gains from the growing global dependence on computers [103-104].

A search of IEEE Xplore's standards dictionary returns only two records of standards terminology documents referring to "cyber" [90-92]. The lack of cyber security terminology standards is not only problematic for consistency of communication, but for comparative studies and validating research, or developing metrics. Cryptography gives rigorous definitions of whether an encryption scheme is "secure," which allows schemes to be compared; but newer branches of cyber security, as well as broader "cyber" areas of study, are severely lacking in such definitions. Potential benefits of terminology standardization include the following:

- Creation of precise laws and policies
- Repeatable, mutually intelligible, comparable, and interdisciplinary research
- Preservation and availability of knowledge through indexed and easily searchable databases

Defining terms and eliminating unnecessary synonyms or ambiguous phrases from scholars' vocabulary facilitates the creation of precise legal constructs for cyberspace and of industry standards and best practices, such as the NIST Cybersecurity [sic] Framework, which suggested standards for ensuring proper cyber security in business operations [83]. If there were more consensus between academia and the government, NIST Framework could be formally defined, and we would likely see other similar successful efforts.

The ability for scholars to understand each other is of paramount importance in research. As is true with the goals of standardized chemical nomenclature, the most important goal of terminology standardization efforts for cyber security should be ensuring no ambiguity in terms; a secondary objective should be to minimize alternative names for the same concept.

This second objective would improve database searches for new journal articles. If terminology constantly evolves, much knowledge can potentially be overlooked, with only the most common terms being searched for and recognized, and with papers using ad hoc or nonstandard nomenclature winding up ignored, or not even turning up in search results despite their valuable contributions. Even if search engines use topic modeling to improve their search results [133], if the four subdisciplines of cyber security are divergent in their terminology, they might not appear even in such advanced search algorithms. Therefore, standards would benefit the entire body of security research, and would ensure accurate and comprehensive searches. Authors who choose not to adhere to such standards could risk having a negligible impact on the field. There is a strong incentive, then, to adopt such standards, if a plurality of researchers have already adopted them –

and in many cases even if they have not yet done so [87]. Adhering to terminology standards (some of which I suggest below), whether sooner or later, may thus improve authors' articles' search engine prevalence.

4.1.3 Prior Work on Terminology Standards

Standardizing the field of cyber security has been an ongoing process for many years, and, there have been a number of attempts to create a glossary of terms. The largest of efforts is the NICCS Glossary of Common Cybersecurity Terminology, a compilation of terms by US CERT from various lexicons issued by standards bodies [102]. These lexicons have been issued over the years by organizations like NIST. The East-West Institute has also led two smaller efforts in collaboration with the United States and Russian governments to create short agreed upon definitions of some terms, but these terms have been more specific to the defense sector [99-101]. The Cybersecurity 500 website also lists 5 different cyber security glossaries [134-138].

Many of these cyber security lexicons seem themselves ad hoc or outdated, with terms like "misnamed files" and "mobile code;" and inspection reveals that many of the standards documents cited in them are over 10 years old [117]. Because its sources are old, NISTIR 7298 includes floppy disks and other removable media in its definition of "mobile devices," despite current usage of that term referring almost exclusively to smartphones. The field of cyber security is still new, but before 10 years ago it was in its infancy, especially from a government perspective, where most of the source documents cited in these dictionaries originated. Ten to fifteen years ago may have been too early to standardize cyber security terminology, at least without periodically updating it. CNSSI 4009, the most cited source used by NISTIR 7298 and the NICCS glossary (the two primary cyber security glossaries), was revised in 2006, and states that a glossary must be continuously updated to remain useful, and should keep pace with changes in cyber security [120]. While some of these glossaries have been updated over time, such as SP 800-53, many of these sources are outdated.

Various terms from papers surveyed in the literature review do not appear in any of these dictionaries; terms like "big data," "cyber," "cyberbullying," "cyber-physical," "darknet," "internet of things," "smart grid," "web," and "Stuxnet," many of which have become prominent in the past 10 years, are notably missing from public sector definitions. Based on the contrasting terminology used in dated and government-defined dictionaries, I believe it is time that a coordinated effort took place between academia and industry, with input from governments, to update a comprehensive and representative cyber security dictionary of terms.

In addition to glossaries, other work related to research standards-setting includes a short and general research directive for allocating funds for cyber security research, The Cyber Security Research and Development Act (Nov 2002), which gave the US Office of Science and Technology Policy the responsibility for coordinating cyber security research and development. Besides this, there have been many cyber security research initiatives, largely supported by governments, but no broad industry- or academia-wide efforts to create research standards; rather, these have been

left to evolve organically [119]. The problem with this approach is that it takes too long; it took thousands of years for cryptography to evolve organically. Even concerted efforts have focused not on research standards, but security standards themselves, such as those for control systems, or for businesses [83, 118]. To my knowledge, a meta-level approach to cyber security (e.g. how to decide on research goals) has been largely neglected in research.

4.2 Terminology Harmonization Recommendations

In this section I propose guidelines for authors and the global multistakeholder community to consider when standardizing cyber security terminology. I developed these guidelines by inspecting the data in Table 11. In the next section I apply the guidelines to the author-supplied keywords from the articles in the literature review.

4.2.1 Guidelines

To reap the benefits stated above, I propose using the following guidelines when considering whether to include a cyber security term a universal glossary:

1. Clear linguistic basis as evidenced by etymology and adherence to proper rules of language.
2. Enjoys popular and historical trends in usage by the global multistakeholder community
3. Gives meaningful search results
4. Well defined and not ad hoc.

As stated in Chapter 1, herein I do not attempt to create new standards; rather, my goal is to infer standards based on inclinations of published works, in order to facilitate research and discourse in the field. I hope to clarify emergent standards and avoid overburdening the research field with unintelligible phraseology. I use these guidelines to present specific recommendations for terminology in Section 4.2.3 onward. Throughout this chapter, the following metric was used when suggesting standards: I recommend a term for standardization if it either: 1) explicitly satisfies at least 2 guidelines and does not explicitly fail to meet the other 2 guidelines; or 2) satisfies at least 3 guidelines. I do not disqualify a term based on any one criteria.

While not all of these requirements may be *necessary* to recommend a particular term for standardization, by being strict and conservative in my selection of terms, I aim to satisfy more than *sufficient* criteria for acceptance. Future researchers may wish to more precisely incorporate dictionary terms to avoid the risk of overlooking important terms. In other words, in applying these guidelines in this exercise, I only sought words and phrases to accept, rather than terms to reject outright. Nevertheless, in the following sections I do note whether I recommend or do not recommend a given term for acceptance by the community. *Acceptance* of a term reference to "acceptance by the community," and that I therefore recommend it for formal defining or at least continued widespread use, whereas *Non-Acceptance* means I recommend using the term only sparingly, especially in prominent places such as titles or keywords, pending greater acceptance by the research and multistakeholder communities. This thesis makes no recommendation either

way about terms that I do not explicitly comment on, insofar as whether I would suggest including them in a cyber security lexicon at this time.

The above guidelines are for when a term has no close synonyms or competing terms. If competing terms exist, the term that satisfies more guidelines is proposed; if they satisfy the same guidelines (such as in the case of two nearly identical terms that are different only in that one uses a "cyber" modifier and the other uses a "cyber" prefix [explained below]), whichever one satisfies more guidelines to a greater extent (e.g. greater current incidence, earlier use or greater use over time, or greater acceptance by the global multistakeholder community) is given as I suggestion for the standard term.

Further elaboration on the measurement criteria I use in this chapter for each of the above proposed guidelines follows below (numbered according to the corresponding guideline). Future researchers may choose to use different metrics to satisfy the same guidelines I suggested.

1. Various linguistic accounts, including journal publications, The Elements of Style, use by country, and usage in government documents, were consulted for insight into proper English use and etymology [97].

2. Trends of usage over time from Scopus and IEEE Xplore (or other journal databases) provide evidence of historical acceptance. To a lesser extent, use by agencies and working groups in the global multistakeholder community are also examined for consistency with results from databases. Because the primary goal of this chapter is to propose nomenclature for *research*, not for individual working groups or agencies for internal use, the primary sources will be results returned from academic journal databases. For this guideline I determine when terms first began to enjoy use among researchers.

3. Meaningful search results for journal database searches is determined by a range of result incidence which is not too low nor too high; I outline this range below. This range was empirically derived based on the incidence of a few clearly currently accepted terms or candidate terms, such as the incidence range of "cryptography" or "cyberspace". The purpose of defining such a range is to include all relevant terms, while excluding ad hoc terms and terms that are too broad to be meaningful outside of more specific contexts, such as "information." This ideal range will vary between databases, but is used in this chapter to determine whether to accept or exclude terms, which is the primary goal of this section. By adhering to data from a consistent set of databases, it is possible to identify accepted terms. Because the ideal range will vary, the specific range I use should only be reused by other researchers on the same databases and within the same range of years (2010-2015).

4. The presence of rigorous definitions in journal articles is required to satisfy this guideline. Even for a popular term, this requirement might not be satisfied. This is also measured by the number of overlapping or conflicting terms, e.g. online psychology versus cyberpsychology,

the latter of which is not easily understandable. Definitions (extracted from dictionaries and journal articles) go beyond proposing words for broad concepts, and rigorously define these terms. For example, terrorism is a well-accepted term, but the definition of terrorism is highly contested [93].

4.1.2 Metrics for "Meaningful" Search Results

Guideline 3 requires more formalization to be useful. In Guideline 3 I claim that it is important to consider searchability of terms when agreeing on a standard dictionary of academic terms. By searchability, I mean that performing a search (that is, with a particular keyword or phrase) gives meaningful search results, corresponding to articles the searcher was looking for. In other words, searchability is akin to search engine optimization for journal papers. That is, the intended meaning of the keywords in any given journal article corresponds to the use of that keyword in papers in the databases I use for comparison (Scopus and IEEE Xplore). The more appropriate the author-selected keywords, the more likely the author's paper is to appear in an appropriate search. As I stated before, search engines can only do so much on their part to optimize results; at some point, it becomes the author's responsibility to use appropriate jargon in their titles, keywords, and abstracts, to ensure that their publications are located.

As far as search terms go, this metric is useful by itself for helping authors increase their article visibility when writing a title, abstract, and keywords (and again, search results is not the only metric I recommend for identifying accepted terms in general). I estimate the optimal range where candidate standard terms can be found at [100,1000) total hits in Table 11, whereas the extreme range for candidate terms is [10, 100000). The following paragraphs elaborate on this claim.

In Table 11, terms in category 1 are clearly poor search terms. They have no value as keywords because of their gross ambiguity and universality. I suggest they never be used as keywords when writing articles. Similarly, taken as a whole, the terms from Scopus in category 2 give a broad idea of concepts in cyber security, but individually, these terms can also have many meanings independent of cyber security (e.g. space, ecosystem, sustainable, and planning). Even "internet" and "security" are a little too broad for the purposes of identifying a minimal vocabulary (i.e. one with the strictest inclusion criteria to ensure that all terms selected are unequivocally cyber security terms; they would be used in article returned by a reasonable search for cyber security publications, and they would not be used in articles returned by searches in unrelated fields, like biology).

Scopus category 3 contains some words which clearly belong in the field and which would make for good search terms that only return appropriate publications; for example, terms like cyber, encryption, network security, and smart grid. However, other terms in category 3, like geography, supply chain, and ontology, have many applications to other fields, which makes them terms unlikely to return useful results on their own. Moreover, researchers should not be expected to sift through 10,000 of more papers to find relevant ones, unless perhaps they intend to do a broad literature review, such as the one in this paper. While the terms in Scopus category 3 highlight key high-level aspects of cyber security, like cryptography in actuality, a search for "cryptography" by

itself will not yield anything specific enough to be of value without analyzing the search results in more depth. Therefore, this range of incidence is not narrow enough on its own to be of value for Scopus searches.

The above conclusions similarly apply to IEEE Xplore's categories 1-4. My recommendation is that category 3's upper bound (100,000 hits) only be used as the upper bound for the *least* specific keywords an author uses when writing an article.

Scopus category 4 terms are nearly all unambiguously and readily identifiable as specific to cyber security. However, they still have broad meanings within cyber security, and when used as standalone search terms they are more appropriate for literature reviews within cyber security. Nevertheless, they do give meaningful search results. This, may be an appropriate upper bound of incidence when considering candidate terms as journal article keywords. When adapting these guidelines for other databases, the same holds true for the range of the terms in category 4 in the other databases, of course. However, because the 3rd guideline aims to recommend concrete guidelines to describe minimal set of appropriate cyber security search terms, category 4's range is still too high. These terms would, however, be expected to yield very specific meaningful results in searches when combined with other terms.

Every term in Scopus category 5, perhaps with the exception of the phrase "index terms," is clearly a relevant cyber security term. Furthermore, search results for these terms are manageable for identifying papers of interest. This range's upper bound (1000) is my recommendation as the upper bound for the *most* specific keywords used in journal papers.

Scopus category 6 contains a number of terms like "cyber law," "cyber insurance," and "hacktivist" that do not yield very many search results, even though many may argue that they are valid vocabulary. However, these terms are not yet universally accepted or distinguishable from some other concepts in cyber security. "Cyber conflict" is not easily distinguishable from "cyber war," and the advantage of using terms like "safety" and "resilience" in place of "security" has not yet been justified by papers employing such terms [95,96,99]. Furthermore, many readers may find some of these terms unfamiliar. to maximize visibility and yield results in meaningful searches, category 6 is not recommended except perhaps as the lower bound for the most specific terms used as keywords. Category 6 may, however, outline areas where further research is needed.

Category 7 needs no discussion, since I have already identified the ideal range of search hits for a term. Category 7 is peppered with ad hoc terms of little value (further supported by their low incidence). Category 7 may be a useful reference to identify emerging research directions, but I do not recommend that any terms in this category ever be used as journal keywords.

In summary, the optimal range where candidate standard terms can be found is [100,1000) (i.e. category 5), whereas the extreme range for candidate terms is [10, 100000). To yield the most meaningful search results when using terms from categories 3 and 4, researchers can combine

multiple terms from categories 3-6. This key insight can aid future cyber security literature reviews, and is a valuable contribution of this thesis. To ensure that publications are locatable, I suggest that at least some easily searchable keywords be used in every article's author-supplied keywords; querying databases that index target journals can aid authors in this decision.

When applying these results to future research, it is important to consider the specific terms in the categories of the ideal ranges, rather than the ranges themselves, since the number of published articles will continue to grow over time. In addition, these results can be replicated and updated periodically to assess the state of adoption of terminology by the cyber security community.

Using sub-optimal terms and phrases is certainly an indispensable aspect of the progression of research. However, when suggesting standard terms and rejecting others, I considered the optimal range of [100,1000) total hits when assessing whether guideline 3 was satisfied by a given term (see Table 8, below).

4.2.3 Recommendations for Specific Terms

The keywords extracted from the papers found in the literature review, as well as a dozen other terms that are important in cyber security, are categorized in Table 8 based on my recommendations for standard usage. All terms were evaluated using the terminology guidelines outlined in this paper, and were then sorted into three categories, of either *Accepted*, *Not (yet) Accepted*, or *Partially Accepted*, based on the degree of their adoption by researchers and other members of the global multistakeholder community, as determined by the number of guidelines they satisfied. As stated before, terms that 1) explicitly satisfied at least 2 guidelines and did not explicitly fail to meet the other 2 guidelines, or 2) satisfied at least 3 guidelines were classified *Accepted*.

As stated earlier, I make no explicit recommendation that terms found not to be commonly accepted never be used. Table 8 only labels words according to their current use in cyber security. Some words that are not yet accepted by the community include "cyber" by itself (and in its myriad ad hoc combinations), "cybernetics," "cyber-risk" and "ontology". Although some such "not accepted" terms may be understood by the reader, and may be well-defined in other fields, these terms are not yet generally understood within most of the cyber security academic and multistakeholder community. I would advise standards bodies or glossary maintainers not to include such terms in current glossary updates until they become more universally accepted and identified with cyber security.

Partially Accepted terms in Table 8 are recommended to be prominently used only occasionally in papers, such as in the title or author-supplied keywords, with discretion. For example, while "risk" may be an inappropriate author-supplied keyword, it is an acceptable term for use when describing topics in cyber security elsewhere in a paper. As stated before, these "partially accepted" terms only satisfied one of the proposed guidelines, without outright failing to meet the other three, or met two guidelines but failed the other two.

Summary of Proposed Terminology Standards				
Accepted	Not (yet) accepted			Partially accepted
CISO	academia	hierarchical access	research strategy	accountability
cloud computing	active air defense	impact assessment	risk assessment	attack
computer abuse	active air defense	index terms	scientific paper	availability
critical infrastructure	active cyber defense	information exchange	secure software engineering	big data
cryptanalysis	adaptation tactics	information extraction	security analysis and monitoring	cascading failure
cryptography	ami	information schema	security automation	cio
cryptology cyber crime	anti-forensics attack description language	information security education	security countermeasures security issues	cni computer crime
cyber law cyber operations	attribution cikr	information structure insider	security methodologies security ontology	Common vulnerabilities and exposures
cyber physical	classification	instrumental crimes	security solution frames	computer ethics
cyber physical systems	communication	international	self-organisation	Computer security
cyber security	complex networks	international cooperation	risk assessment	computer system security
cyber threat	computational part	international policy	scientific paper	context-awareness
cyber war	cpss	internet security	secure software engineering	cps
cyber warfare	cross-domain attacks	internet study	security analysis and monitoring	cyber bullying
cyberspace	curriculum development	jurisdiction	security automation	cyber insurance
darknet	cyber	knowledge base	security countermeasures	cyber stalking
DDOS	cyber assurance	knowledge model	security issues	Cybercrime
deep web denial of service	cyber attacks and countermeasures	law layered network	security methodologies security ontology	Cybersecurity dark web
digital signature	cyber conflict	learning objects	security solution frames	darknet
embedded computer	cyber domain	legal issues	self-organisation	e-commerce law
encryption	cyber education	legal rights	semantic	evidentiary
espionage	cyber psychology	literature review	semantic operability	forensics
hacker	cyber readiness	mac security	semantic security	hacktivist/hactivist
ict	cyber resilience	mapping	semantic web search	industrial networks
ids	cyber safety	meta-adaptation strategies	semantic web technology	information
information technology	cyber space	military operations	Slovenia	information systems security
internet	cyber targeting	model-based design	social cybernetics	insider
intrusion detection system malware	cyber treaty cyber world	morality of law socialization	sovereignty space	missile defense risk assessment
national security	cybergeography	motivation	state-level	risks

network security	cybernetics	multi-agent systems	sustainability	security
phishing	cyber-physical-social systems	national cyber strategies	sustainable	security architecture
privacy risk management	cyber-risk cybers	networked computer technology	system dynamics systematic literature review	security controls security patterns
scada	cybersafety	neutralization	system-level requirements	self-defense
steganography stuxnet	cyberspace security cyber-territory	ontology ontology architecture	systems strategic security management	semantic web sensitivity analysis
system security	definitional gaps	ontology design	taxonomy	signals intelligence
	denial of sustainability	ontology security	technology	situational awareness
	deterrence disgruntlement	ontology-based context models	Terrorism textbook	smart grid social-networking
	distributed systems security	organizational justice	theoretical foundation	software piracy
	e-consumer protection	papa framework	traceability	supply chain
	ecosystem	people	u.n.	supply chain management
	emerging cyber threats	percolation theory	us cyber security act 2012	threat
	emerging technology trends employee computer crime	physically-aware engineered systems	vishing web attacks	threat environment threat patterns
	ethical issues	planning	web space	u.s. cyber command
	expressive crimes	policy	propaganda	vulnerability analysis
	force	policy making	psycho dynamism	web
	geography	politics	regulation	
	government response	private sector		

Table 8. Commonly accepted and not-yet-accepted cyber security terminology [132]. Grouped according to whether they satisfy the guidelines from Section 4.2.1. Terms were drawn from the author-supplied keywords from the literature review covered in Chapter 2, and additional cyber security terms were added.

For example, according to Figure 6b, "critical infrastructures" is orders of magnitude more popular than "critical national infrastructure." Furthermore, the US CERT Cyber Glossary only defines critical infrastructure, not critical national infrastructure [102]. Therefore, I recommend that "critical infrastructure" be used and "critical national infrastructure" or CNI not be widely used, at this time. Of course, CNI might still become a standard dictionary term in the future.

Table 8 can serve as a quick reference to researchers simply searching for lists of vocabular that enjoy common use. Consulting Table 8 before one of the dictionaries mentioned early can give researchers a better idea of whether a term is actually accepted by the security community as of this writing. For best results, Table 8 should be updated periodically. Future work could include

developing an online learning system that perpetually updates a glossary of terms according to the four terminology standard guidelines.

4.3 The Vocabulary of the Four Cyber Security Disciplines

Table 9 categorizes the terms from Table 8 according to the four areas of cyber security identified in Chapter 2. Table 9 also includes the percentage of papers from each category that use *Accepted* and *Partially Accepted* terms, respectively, as well which papers use both. *Accepted* and *Partially Accepted* keywords are roughly equally distributed across categories, meaning that every category individually does use a fair amount of accepted terminology. Next, I will summarize the general terminology of each category.

Public has military terms like "cyber operations" and "espionage", as well as national security terms like "CNI" and "Stuxnet". *Infrastructure* has technical cyber security terminology like "cyber physical systems", "digital signature", "accountability", and so forth; *Business* includes many business aspects like "cloud computing", "CISO", "cyber insurance", and "computer abuse". *General* has a wide variety of unspecific concepts: "information technology", "computer ethics", "dark web", "social-networking", and "cyber threat".

Proposed vocabulary for harmonization, by category		
Category	Accepted (A)	Partially Accepted (B)
Public (48.4%, 45.2%) (22.6% both)	cyber crime, cyber operations, cyber security, cyber warfare, cyberspace, DDOS, espionage, internet, national security, Stuxnet	Attack, CNI, Cybercrime, Cybersecurity, evidentiary, hacktivist/hactivist, information, missile defense, self-defense, signals intelligence, threat environment, u.s. cyber command, web
Infrastructure (60.0%, 80.0%) (60.0% both)	critical infrastructure, cyber physical systems, cyber security, DDOS, digital signature, network security, privacy, scada, steganography	Accountability, Availability, cascading failure, context-awareness, cps, industrial networks, risk assessment, information, Security, security architecture, sensitivity analysis, situational awareness, smart grid
Business (54.5%, 72.7%) (36.4% both)	CISO, cloud computing, computer abuse, cyber crime, cyber law, cyber security, cyberspace, internet, privacy, risk management, scada	Attack, cio, computer crime, cyber insurance, Cybersecurity, e-commerce law, information, insider, risks, Security, supply chain, supply chain management, threat patterns
General (68.4%, 89.5%) (63.2% both)	cyber crime, cyber law, cyber security, cyber threat, cyberspace, DDOS, denial of service, ICT, IDS, information technology, internet, intrusion detection system, malware, national security, phishing, privacy, system security	Attack, big data, Common vulnerabilities and exposures, computer ethics, computer system security, cps, cyber stalking, cybercrime, cybersecurity, dark web, forensics, information, security, semantic web, social-networking, software piracy, threat, vulnerability analysis, web

Table 9. Proposed vocabulary for harmonization [132]. Terms from Table 8, extracted from the literature review papers, and the categories of articles from the literature review that they appeared in. Some words appear in more than one category. Percentages indicate the percentage of papers that had at least one Accepted or Partially Accepted Term in a given category, respectively, and which had both.

Next I present some additional observations from Table 9 regarding which categories certain popular terms appearing in articles are from.

The *Infrastructure* category is the only one that doesn't mention cyber-crime, internet, or cyberspace. "National security" is shared between the *Public* and *General* categories. "Cyber law" shows up in *Business* and *General*, but, interestingly, not in *Public*. More practical or application-driven terms like "malware", "intrusion detection systems", "forensics", "big data", etc. are present only in *General*. "Cyber security" shows up in all four categories, as would be expected, and "information" shows up everywhere as well. "DDOS" is common to *Public* and *Infrastructure*. "Privacy" shows up in every category except for *Public*, interestingly; and "security" as a standalone word shows up consistently in all other categories, yet only appears in one paper from *Public*. Some other interesting observations include: "attack" is not a term used in any papers in the *Business* category. "Cybersecurity" [sic] as a single word shows up everywhere but *Infrastructure*, perhaps indicating that that spelling is less common in computer science. *Infrastructure*, on the other hand, is the only category with "smart grid."

In general, as expected, the literature review revealed that articles that use accepted terminology are lacking, but not entirely scarce; and papers typically use more partially accepted terminology than accepted terminology (with some papers using both). Articles that can be classified into the *General* category use more of both kinds, which is consistent with the definition of this category – they should use more accepted terminology because they are expected to be understood by a larger audience. Articles aimed at the *Public* sector actually use the most non-standard terminology, which further calls into question governments' roles as authorities in cyber security glossaries. Glossaries of cyber security terms should be managed and agreed upon by an interdisciplinary community, since cyber security is indeed multidisciplinary.

Table 4 provides another illustration of the four categories I derived from the literature review, and adds support to the notion of their existence. In addition, Table 9 gives some very real evidence of differences in communication between these four areas. If a larger sample size were taken, of 1000 papers or more – perhaps 10,000 – complete with distributions of which categories terms more commonly show up in as keywords or title words, it could be used in the formation of research agendas for improving interdisciplinary cyber security research.

4.4 Specific Nomenclature Conventions

This section elaborates on some of the more prominent cyber security terms in Table 8, and their associated hindrances to the creation of a standard glossary of terms. It aims to determine appropriate usage of some important terms and resolve longstanding confusions.

4.4.1 Cyber as a Modifier: One or Two Words?

To resolve the conflict of whether authors should use generally "cyber-" as a separate word (with or without a hyphen) as in "cyber attack" or "cyber-crime", or instead as a prefix of a word as in

"cyberspace," the historical incidence of terms containing "cyber" was determined, and linguistic analyses were performed. This analysis was done for this general nomenclature construct; it is not applicable to specific terms that are by themselves already commonly accepted (or not accepted).

First, IEEE Xplore was searched for articles containing "cyber" only as a word, and for those containing "cyber*" as either a word or as part of a word, where the asterisk indicates a wildcard. The difference between the two terms' results was taken in order to yield the incidence of only cyber* as a prefix/part of a word. The usage of "cyber-" as a word and of "cyber*" as a prefix from 1990 to 2015 were plotted after being controlled for the occurrence of "cybernetics." (Figure 4) This was done to ensure that only terms relevant to cyber security or the broader "cyber" research field were accounted for (cybernetics is a separate field related to system dynamics).

The majority of the words that are combined with "cyber" (joined by a space or hyphen) in journal papers come from just a few phrases: cyber physical, cyber security, cyber-attack, cyber threats, cyber-crime, cyber warfare, cyber world, and cyber war. Google Ngram also gives other common terms like cyber space [sic] [94]. The top terms containing "cyber" as determined by Google Ngram and Figure 6 were also plotted between 1990 and 2015 in Figure 4. Curves that also control for other more common terms that dominate some of the "cyber" categories, like cyber-physical and cyberspace, were plotted as well. These curves are bolded and labeled as "controlled." This was done in order to compare whether "other" generic terms, including ad hoc terms and terms that are simply less common, were more commonly used with "cyber" as a separate word or as a compound word; that is, whether "cyber" as a word or "cyber" as part of a compound is more commonly used in research articles.

Similarly, Scopus was queried for the most common terms using "cyber." However, Scopus does not have a wildcard search parameter as of this writing, so it is not possible to extract the exact number of terms that use "cyber" in a compound. However, summing the hits for the most commonly used "cyber" terms (other than cybernetics) for the two types (separate vs. compound words) yields an approximation of the totals of the two types. These approximations, along with the hits of some of the most common terms, are plotted Figure 5

The results indicate that both when controlling for and when not controlling for the most commonly used terms containing "cyber," use of a separate word for "cyber-" is vastly more commonplace than is use in a compound word, as of 2009; prior to 2009, both had comparable incidence. Therefore, it is recommended that "cyber-" (i.e. a separate word) be used in most cases. In Figure 5, the controlled "cyber-" word (i.e. phrases formed with cyber as a separate word) is even beginning to overtake the incidence of all (non-cybernetic) compound words; whereas the use of compound words (outside of the few most common ones) is not gaining additional acceptance by the academic community. Figure 4 tells a similar story. "Cyber-physical" is by far the most prevalent term with "cyber" as a separate word, threatening by itself to overtake the incidence of "cyber" in all compounds. The usage of "cyber" as a separate word far outstrips the compound usage in total non-cybernetic hits.

Figure 4. **IEEE Xplore incidence of publications that use most common "cyber" compounds [132].**

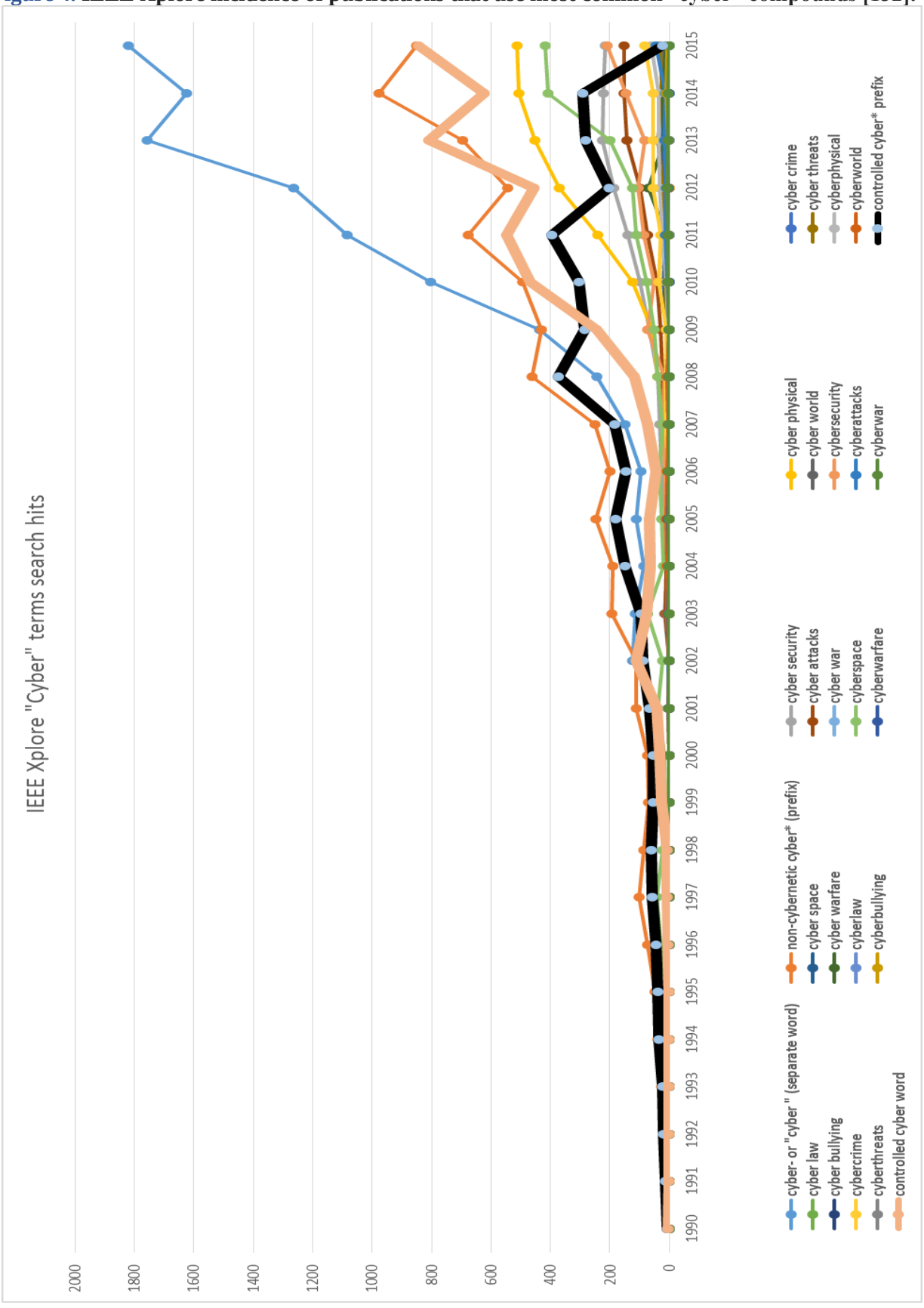
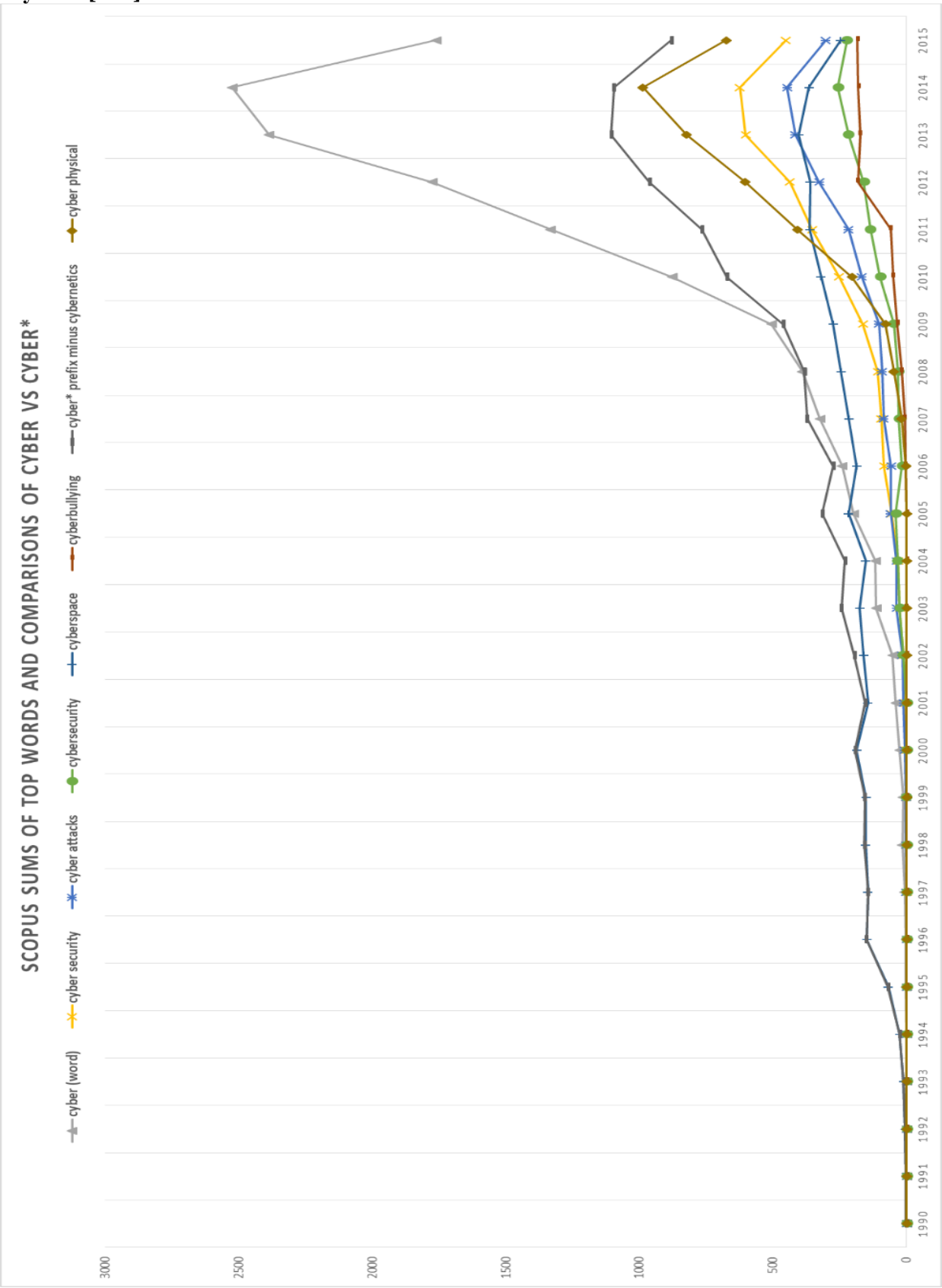


Figure 5. **Scopus incidence of journal publications with common words compounded with "cyber" [132].**



It is clear from Figure 4 and Figure 6 that "cyber-" as a separate word, possibly hyphenated (according to preference or other convention), should be the standard format for authors to use to ensure articles' searchability, i.e. search engine optimization. In database search engines that do not allow wildcard searches for word prefixes, searching for "cyber" as a separate word is extremely valuable, as it allows new and unfamiliar terms to be discovered. If a single compound word is used to search, appropriate articles can be located only by already knowing the exact word one is searching for (which is sometimes unlikely, given the nascence of the field).

This conclusion is consistent with proposed guidelines 2-4 for standardizing terms, but is not consistent with the 1st guideline. However, using "cyber" as a separate word is far better than the alternative, which only satisfies the first guideline. Historically, as can be seen from Figures 1 and 2, "cyber" as a separate word enjoyed less usage than similar compound words. Only around 2008 did it overtake the historical word; however, the separate word's usage so vastly outpaced the compound word's, that it is impossible to resist its current prevalence. Further evidence of this trend is from dictionary searches: the two results from a search of IEEE Xplore's standards dictionary were for "cyber security," not "cybersecurity"; one was from 1997, and the other was from 2010 [90-92].

Finally, as was just implied, in order to give it proper treatment under Guideline 1, the linguistics of *cyber* should be considered. The Greek root *κυβερνήτης* is not a compound word, and "cyberspace" and "cyberwar" can be thought of as portmanteaus of "cybernetics" and "space" and "war", respectively [128]. Portmanteaus are nearly always single words, not containing hyphenated word fragments or word fragments separated by a space. However, unlike many portmanteaus, the second word is present in its entirety in both of these examples. Alternatively, since "cyber" is a standalone word that originated as an abbreviation of "cybernetics", it might make more sense for it to appear as a separate word in compounds, especially when the full word it modifies is retained in the phrase. The ambiguous linguistic status of *cyber* is almost enough for Guideline 1 to yield little guidance, but the etymology of the word *cyber* favors a separate word usage in most forms.

Despite these observations, there are terms that are commonly used in a compound form. Among these are "cyberspace" and "cybersecurity." Curiously, cyber security and cybersecurity have comparable incidences in all of the figures that they appear in, although the separated-word phrase is still used about twice as often as the compound word. These terms are commented on more in the next two subsections.

4.4.2 Cyberspace

"Cyberspace" meets the 2nd and 3rd of the proposed guidelines for standardization, and does not explicitly fail to meet the 1st and 4th guidelines, and should therefore continue to be used frequently. "Cyberspace" emerged in 1990 according to Scopus, enjoys popular use, gives meaningful search

results (see Table 11), and is consistently favored over “cyber space”. It has definitions in dictionaries, but it might be left open for debate whether there exist truly rigorous definitions for “cyberspace.” Therefore, I propose “cyberspace” as a commonly accepted term, and I recommend the spelling “cyber space” never be used.

4.4.3 Cybersecurity Versus “Cyber Security”

“Cybersecurity” meets guidelines 3 and 4, but among journal papers, does not enjoy pluralistic usage over “cyber security,” and in fact emerged after “cyber security,” which has enjoyed more popular usage than “cybersecurity” in nearly every year according to both Scopus and IEEE Xplore’s databases. In addition to this, while two words usually become one after a period of hyphenation (or separation with a space - journal databases treat hyphenated words as separate words), the research community does not seem ready to accept cybersecurity as a single word yet [97]. However, due to their reasonably comparable incidences over time, “cyber security” or “cybersecurity” are both common and generally acceptable. However, this requires that searches for papers referring to cyber security include “cyber security” OR “cybersecurity” for complete coverage. This is of course tedious, and at this stage “cyber-security” or “cyber security” is recommended as the standard term over “cybersecurity” because it satisfies all four guidelines, whereas “cybersecurity” only clearly satisfies 2, 3, and 4, and satisfies 2 to a lesser extent than “cyber security” does. That said, since both terms have been accepted by the community, practical usage could simply be a matter of personal preference. Researchers should feel free to use whichever of the two spellings they prefer. In addition, while UK and European English sometimes appear to favor “cyber security” over “cybersecurity” (often favored by the US government), regional preferences have blurred recently.

4.4.4 Cryptography, Cryptology, Cryptanalysis

Cryptography refers to the art of designing cryptosystems; cryptanalysis refers to the art of breaking cryptosystems; and cryptology is the union of cryptography and cryptanalysis [98]. However, “cryptography” and “cryptology” are sometimes used interchangeably, despite these terms being fairly well-defined in principle. In practice, “cryptography” is used far more widely than either “cryptanalysis” or “cryptology”, according to Figure 6b**.** This simply means that in the field of cryptology, significantly more effort has been devoted to cryptography than to cryptanalysis or to discussions of the general field. Both “cryptography” and “cryptology” satisfy all four guidelines for common use.

Given the definition of the words, I recommend that “cryptology” and “cryptography” be used properly in the future. However, there is, by definition, overlap in the two terms; so in cases of overlap, the more specific term, which is also the more prevalent term, “cryptography”, should be used.

"Cryptanalysis" seems to have fallen into disuse and should therefore not be used as a primary search term when "cryptography" is a better alternative, given that, by definition, cryptanalysis seeks to break the cryptosystems of cryptography; that is, cryptography is implied in cryptanalysis, but not vice versa. Since "cryptography" is the most exclusive, or most essential, of these three terms, it is recommended that this trend in usage be followed by authors to ensure visibility of publications. Again, this is not to say that "cryptanalysis" is a poor word choice. This thesis makes no claims about the usefulness of words; it only suggests which terms can be readily turned into universal standards.

4.4.5 Cybercrime and Computer Crime

According to Scopus, "computer crime" first appeared in the literature in 1972, well before any spelling of "cyber-crime". Therefore, "computer crime" satisfies guideline 1 and "cybercrime" fails at guideline 1. However, many organizations in the global multistakeholder community make reference to "cybercrime," including Symantec, Interpol, and the U.S. government, though some stakeholders do refer to "cyber-crime," non-US countries especially [113, 114]. **"**Cyber-crime" as a hyphenated word appeared in the literature a few years before "cybercrime" in the mid-1990s, but "cybercrime" has in recent years begun to outpace "cyber-crime" in journal article usage. Both "cybercrime" and "cyber-crime" fall in the ideal search incidence range of [100,1000) hits from 2010-2015 on Scopus and IEEE Xplore combined, but "computer crime" actually has far more hits, with 11,171 from Scopus alone. Although this is outside the ideal range, it is within the acceptable range. Thus, "cybercrime" and "cyber crime" meet Guideline 3 for meaningful search results, and "computer crime" partially satisfies Guideline 3. Lastly, only "cyber-crime" is defined by EWI or NICCS, satisfying guideline 4 [100-102]. I summarize these conclusions in Table 10, below. From this, one can see that "cyber crime" (or the hyphenated version) meets the most guidelines of the conflicting terms. Clearly, cyber-crime (and related phrases) is a term in great need of standardization, given the varied uses of its forms and synonyms. However, "cyber crime" passes the tests to be *Accepted*, while the other two terms are only *Partially Accepted*. Thus, "cyber-crime" is my recommendation for harmonizing terminology for maximum idea exchange across disciplines.

Table 10	**Guidelines satisfied**			
Term	1	2	3	4
Computer crime	O	X	?	X
Cybercrime	X	O	O	X
Cyber crime	?	?	O	O

Table 10. Forms of the phrase "cyber-crime". X indicates guideline is not satisfied, O indicates satisfied, ? indicates partially satisfied/not failed. "Cyber crime" (or "cyber-crime") satisfies the most guidelines [132].

4.5 Broad Nomenclature Standards

While the previous discussion revolved around keywords extracted from a literature review of current trends in cyber security, it is by no means a comprehensive analysis, nor can such an analysis be done in this thesis alone. For this reason, in this section I slightly expand my analysis and give cursory consideration to some other terminology trends that affect cyber security communication and idea flow. Attention in the literature has recently been called to the variety of terms used to describe Internet-related concepts. Various different prefixes have emerged since the Internet's creation, and have achieved fluctuating levels of dominance over the years [115,116]. This section attempts to shed light on the uses of these potentially confusing terms, and gives some recommendations for authors and standards bodies on future usage, although it does not thoroughly vet these terms using the guidelines laid out in Section 4.2.1.

4.5.1 Internet-Related Prefixes

These words include *virtual*, *digital*, *e-*, *cyber*, *smart*, *net*, and *online*. If a proper systematic nomenclature is eventually to be constructed for researchers, the distinction between these words, if any exists, should be understood, and redundant prefixes should be eliminated. The descriptions below refer to these words when used as prefixes or modifiers in computing**.**

1) Virtual

Virtual refers to that which seems real but isn't: simulation ("real" being loosely defined here, as are all of the terms considered in this subsection). In the field of optics, *virtual* images are a phenomenon that results in the appearance of an image where no photons are actually present, i.e. that which seems real, but is not [124]. Virtual machines act like real ones but aren't. In fact, "virtual reality" could possibly refer to anything virtual (though obviously it conventionally refers to the human immersion in a virtual world). *Virtual* is typically used for things whose purpose is high-level abstraction. A virtual machine is not made to examine electrical signaling in computing, but to be operated by a user at the high level, for various purposes. Likewise, a *virtual* meeting room cares not about *how* the meeting takes place; it cares about the *contents* of the meeting, and simulating a meeting. This is of course the essence of high versus low levels of abstraction: low cares about *how*, high cares only about *what*.

2) Digital

Digital refers to something real, where the majority of the purpose of its being *digital* operates at a low level that is not visible. Alternatively, "digital" can encompass broad concepts with a hidden implementation, i.e. not something humans can see right in front of them the way they can see *virtual* things. Again, here, I use a loose interpretation of "real;" in fact, because of this loose definition, something can feasibly be both digital and virtual. For example, currency or the pixels of an image may be implemented at a low, bit level, i.e. digitally. Digital refers specifically to the digits involved in the implementation – the bits of a computer. Digital processing of currency,

images, and so forth, concerns itself with precisely *how* low level operations are performed. It is how pixels are programmed and represented, *in reality*, which makes an image digital.

Bitcoin is then arguably a digital-virtual-currency, and is very concerned with the cryptographic algorithms involved in "mining" bitcoins. Bitcoin's digital currency status is, however, as of this writing, still controversial, so it is unclear how one should classify it. Digital currencies can typically be transformed between computers and a physical form, whereas virtual currencies cannot be transformed [125].

A final note on the terms "digital" and "virtual": Digital currency and virtual meeting rooms are largely useless without the Internet. However, *digital* and *virtual* are not unique to networked technology. *Virtual* machines and *digital* images have no need for the Internet in order to function. Therefore, *virtual* and *digital* may more broadly be considered general "cyber" prefixes rather than Internets-specific prefixes. Furthermore, there is a clear distinction to be made between *virtual* and *digital* when used correctly. These two terms are primarily applied to words they modify to distinguish from "regular" versions of the words – e.g., a virtual machine, as opposed to a regular machine. Because of this, they do not directly contrast with each other, and can sometimes be used interchangeably.

3) E-

E- means electronic, and refers to people-centric concepts like email, e-commerce, and e-residency. *E-* thus carries a distinct Internet and "popular accessibility" air with it. It is very much a 21st century term. If any of the prefixes in this section is synonymous with *Internet*, it is *e-* or *net*. E-services or electronic services do not require the Internet to operate, though, but they generally do require some kind of network functionality. The IETF requires request for comments (RFC) documents spell email lowercase with no hyphen [126].

4) Cyber

Cyber of course has its history in *cybernetics,* meaning *skilled in steering or governing*, and saw popular adoption and subsequent "official" usage by government and industry. It is a primary focus of this paper and needs no further introduction. *Cyber* is very much an Internet-age term, although it is not an exact synonym for *Internet*, but is rather typically much broader in scope. I will not revise the definition of *cyber* here, since many other articles already define it – although none of the preeminent glossaries mentioned earlier does so [99-102,117,120]. Curiously, while "cybersecurity" [sic] saw large adoption as a security term in reference to computers, other terms (pre)modified by *cyber* have begun to emerge so quickly in recent years that they seem not to refer to "cyber" equivalents or corresponding aspects of real world phenomena, but to such phenomena as aspects of cyberspace; that is, "cyber" has become somewhat more of a possessive term and a noun adjunct rather than a modifying adjective. For example, it is conceivable that authors now speak of the security of cyber(space), rather than the cyber (aspect) of security, perhaps

unknowingly. Lastly, many authors claim that we have passed the “digital” age and are entering the “cyber” age [81].

5) Smart

Smart is a buzzword that emerged slowly in the 1990s as a reference to technology before taking off into mainstream vocabulary in the 2000s and skyrocketing in use in the early 2010s.[2] I predict that usage of smart will diminish in the coming age of the Internet of Things, since eventually appending “smart” to something will be superfluous – people may say, “Well of course it’s smart! It’s electronic!” when discussing a modifier like this in the future. Therefore, I recommend it be used with caution and with the knowledge that it may be as obsolete in 10 years as many terms in the cyber security glossaries of 10 years ago are today.

6) Net

”Net," used as an adjunct noun when modifying another noun, refers explicitly to the Internet or sometimes another network, as a noun, rather than an adjective like *e-* does. It is thus the nominal synonym of Internet, whereas *e-* is the adjectival synonym. *Net*, like *e-*, has a narrow use than *cyber*. Unlike with *cyber*, which is ambiguously a noun or an adjective, in English it does not matter, in principle if net, as an adjunct noun, forms compounds as one or two words, though in practice *net* typically forms single-word compound nouns, such as netizens, NETmundial, and Netscape.

7) Online

Lastly, *online* and *e-* perform exactly the same function, but *e-* is always a prefix (perhaps hyphenated, perhaps directly compounded) in a single-word compound, whereas *online* is a separate modifier.

8) Information Technology

So far, these discussions have not included information technology (IT) or information and communications technology (ICT), except that Table 8 shows them as accepted terms. For instance, Russia sometimes refers to information security, rather than cyber security; and IT has a different connotation than *cyber* [129]. The ITU heavily promotes usage of “ICT”, and IT/ICT security is sometimes viewed as a subset of cyber security focusing only on information and no other concerns. Nevertheless, the exact definition of ICT is generally highly contested [130-131]. Oftentimes “IT” is considered a physical substrate for cyberspace. In addition, “cyber” is a more flexible English modifier than “IT” or “ICT”. In my opinion, despite meeting the proposed

---

[2] http://www.scopus.com/term/analyzer.url?sid=7148782FEA989C1354BD1E385A58EF9B.I0QkgbIjGqqLQ4Nw7dqZ4A%3a60&origin=resultslist&src=s&s=%28TITLE-ABS-KEY%28smart%29+AND+TITLE-ABS-KEY%28computer%29OR+TITLE-ABS-KEY%28internet%29%29&sort=plf-f&sdt=b&sot=b&sl=76&count=31202&analyzeResults=Analyze+results&txGid=0

guidelines, “IT” and “ICT” are unstable terms that might become outdated, and, for the time being, “cyber” should be used instead, where possible. It is important to maintain clear and consistent language to facilitate knowledge sharing across disciplines. This includes eliminating unnecessary synonyms or ambiguous terms.

4.5.2 Beyond Cyber Security: A Unifying Academic Discipline Name

While cyberspace is becoming an increasing security concern, it is also becoming ubiquitous as an aspect of the human experience, which is becoming less separable every year from issues cyberspace combines. Social engineering is a prime example of cyberspace and cyber security bleeding into the human psychological realm. It is equally important for scholars to unite in research surrounding this general “cyber” field, just as they should with security. This conjugation of cyberspace and physical space, and the constant growth of new *cyber* terminology, ad hoc or not, is leading to the formation of a new, broader academic discipline: a so-called *Cybermatics* field according to Ma et al. (defined below), which emphasizes creating new terms to describe characteristics of *cyberspace* such as “cyber-something” in either *real* or virtual terms, rather than seeking to describe characteristics of the *real world* in terms of computers and *cyberspace* (such as security, adapted for cyberspace: *cybersecurity* [sic]), as was done in the early years of the Internet. This influx of terms warrants closer inspection and regulation, lest valuable knowledge generated by scholars go unnoticed by researchers unfamiliar with these ad hoc terms. An equally troublesome outcome for idea exchange would be for the idea of generating more ad hoc terms to catch on, rather than for specific terms to be agreed upon by the community. This poses a potential problem when searching journal databases without knowing the right keywords to search for, as stated earlier.

Although the term *cyber* is being used more and more frequently, it is used in a variety of contexts, both technical and nontechnical in nature. This domain of research and knowledge extends beyond cyber *security* and includes general issues of Internet governance and online behavior. Recently, Ma et al. proposed the term “Cybermatics” to describe this new field that encompasses all things cyber and cyber-related [81]. This includes both concepts within cyberspace (Ma et al.’s so called “Cyber World”), such as cyberbullying, and concepts of utilization of cyberspace (“cyber-conjugated” or “cyberization”), such as cyber-physical systems.

In their paper, Ma et al. first define “cyber entities” as “anything that exists digitally in cyberspace, either purely synthesized by a computer, or closely correlated and further conjugated with a real entity in physical, social and mental spaces” [81]. They go on to define “Cybermatics” as a holistic field which studies cyber entities and their properties, models, and representations, including their relations and conjugations, and their technologies and applications.

Although the intention of this thesis was to improve interdisciplinary communication within cyber security, many conclusions drawn from it are shared throughout Cybermatics. Next, I briefly

linguistically analyze whether Cybermatics is an appropriate name for the even broader "Cyber" knowledge domain, and propose alternative labels.

1) Etymology Of Cybermatics

I believe it is necessary to standardize a term to unify the academic study of cyber-related concepts. Ma et al. (2015) give the etymology of their proposed term "Cybermatics" for the new "cyber" field:

> 'The suffix *-matic* comes from *matos* in Greek that means "willing to (perform)". The suffix *-ic* comes from *-ikos* in Greek, meaning "behaving like" or "having the characteristics of". The suffix *-ics* can be used to form a noun to name a field of study, for instance, mathematics, automatics, kinematics, systematics, and so forth. The term "*cybermatic*" can be regarded as "cyber + *matos* + *ikos*", which may describe a thing willing/able to be, behaving like or having cyber characteristics. In a linguistic sense, "Cybermatics" can be understood as a field in which cybermatic things, i.e., various cyber entities existing in cyber-enabled worlds as distinct phenomena, are studied' [81].

Given Ma et al.'s description of Cybermatics throughout their paper, it may be possible that the concept of Cybermatics is an overarching field for all things "cyber" – whether in the "Cyber World" or whether they are "Cyber-conjugated". However, the name "Cybermatics" itself is unlikely to be widely accepted, and at this stage it is too early to confidently predict acceptance by the community (though I predict it will go overlooked). To facilitate the adoption of an overarching term, I believe it is helpful for the academic community to choose from a number of candidate terms. The "academic community" referenced here should consist of all parties with a stake in this field. While "cyber" has its basis in computer science, its transdisciplinary nature necessitates input from many bodies.

2) Alternative Academic Discipline Names

I now suggest potential alternative transdisciplinary field names, for consideration by scholars. These suggestions are meant only as possibilitities, and I hope that if any of these terms is adopted, only one is. However, considering multiple terms for adoption is a good way to determine the most appropriate one for standardized usage.

An examination of a large number of academic disciplines revealed some of the following suffixes: *-matics, -ology, -nomics* or *-nomy*, science, *-ry, -ic, -istics, -ation*, studies, and *-graphy* [108]. Of these suffixes, three stand out: "Cyber science", "Cyberistics", and "Cybernomics". "Cyber science" ironically does not have the futuristic feeling of the other two (or Cybermatics), and its etymology requires little exploration. I do, however, propose it as a possible field name. It should be noted, however, that Ma et al. propose Cyber Science as only one subdiscipline of Cybermatics. For "cyberistics," *istics* is made from two suffixes, *-ism* and *–ic*, and the latter is used is

Cybermatics and is etymologically sensible. However, *-ism* refers to a doctrine, practice, or system, and derives from Greek *-ismos*, meaning the practice or teaching of a thing. [109] "Cyber" is not a practice or doctrine, so this suffix is not appropriate. Of the above three candidates, "cybernomics" is the most interesting (pronounced like genomics). While genomics derives from a neologism "-omics," which has specifically biological applications, the root of economics refers to law, custom, rule, ordinance, or management [110, 111]. One might speak of the laws governing cyberspace (artificial or natural), or what might speak of the entirety of activities related to cyberspace, as the biological –ominics can carry the sense of "all constituents considered collectively."

Considering the above linguistic analysis, "cybernomics" could be a reasonable candidate term encompassing the "cyber" academic discipline, in competition with "Cybermatics", "Cyber science", and indeed, perhaps the frontrunner candidate, "Cyber". Based on the results of this thesis, the standalone "cyber" is likely to emerge the winner among these terms because of its prevalence, but this thesis does not advocate adoption of any *particular* term. I do, however, recommend adopting a standard term for this even broader field in the near future, by official standards bodies, governing bodies, research institutions, and governments, in the same way that I propose creating an updated, centralized cyber security dictionary.

4.6 Summary

Many authors still use ad hoc terms despite the existence of standards glossaries, and spelling or phrasing of many terms is still not agreed upon. The lack of collaboration across disciplines inferred from the literature review emphasizes the need for more comprehensive standard terminology for both cyber security and broader cyber research. Except when radically new concepts are written about, greater use of more widely accepted terms is recommended, though not at the expense of innovation. Authors should, before submitting for publishing, search the databases for their potential keywords to ensure that all are in the [10,100000) range, and that at least one is in the [100,1000) range to ensure good searchability. Because the papers reviewed were necessarily all recently published, and not all from the same year, (2010-2015), it is difficult to determine any correlation between type of vocabulary used and citations. Future research could aim to verify whether such a correlation exists – a positive one could bolster efforts toward adoption of standard vocabulary. However, I believe that regardless, there are compelling reasons to update existing cyber security glossaries.

I outlined guidelines to use when considering keywords to use in future publications and when crafting terminology standards, and resolved some long-held misconceptions in spelling and phrasing. I encourage use of these guidelines and the following recommendations, as well as the use of the standard glossary projects from EWI, NICCS, and other complementary sources like NISTIR 7298. These existing dictionaries are, however, mostly constructed by the public sector, and may or may not reflect academic and private sector areas of study and work regarding cyber

security. Therefore, greater effort from outside of governments, and collaboration with the greater global multistakeholder community, is essential when creating or updating cyber security glossaries.

I proposed a classification of research areas concerned with cyber security, which can be refined by a more comprehensive study of keywords comprising it. These keywords can be used to craft research agendas for each area, as well as in crafting cross-disciplinary research agendas for cyber security. Within the categories I identified, use of standard terminology is fairly common. However, there is clear room for improvement among authors and working groups. Other possible categorizations may consist of the common social sectors of civil society, industry, academia, and the government that many articles cite [127]. I encourage future researchers to delve further into categorization and ontology creation of cyber security for the formulation of research agendas.

Specific spelling and phrasing conventions should be adhered to in order to ensure visibility of publications. Most importantly, except in the cases of cyberspace, "cyber" terms should be written with cyber as a separate word, as in "cyber physical," possibly hyphenated. While cyber security is the prevailing spelling, it is reasonable to assume that the single word spelling, cybersecurity, is still acceptable. Cyber-crime has no definitive spelling, but I predict it will lean toward being condensed to cybercrime in the future.

Herein I attempted to lay the groundwork for standardizing communication within cyber security. I believe formalizing cyber security terminology would accelerate the pace of research, improve policymaking and business practice, and lead to greater integration with the rest of the scientific community. Additional efforts that may be important to formalizing cyber security as an academic discipline include the creation of more businesses out of research, the creation of a committee within an Internet governance body, or the formation of a multistakeholder project to address this, and systematic efforts by academics to propose, assess, and rigorously define vocabulary based on the four guidelines given in this thesis. The ultimate goal of such formalization should not merely be a lexicon of terminology, but methodologies or framework for cyber security research. With the growing prevalence of cyberspace and the emergence of a so-called Cyber or Cybernomics or Cybermatics field, it is urgent to bring together the disparate efforts in these areas and share knowledge, lest it be overlooked and progress delayed.

Disclaimer: [132] was funded by the Cooperative Agreement between the Masdar Institute of Science and Technology (Masdar Institute), Abu Dhabi, UAE and the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA - Reference 02/MI/MIT/CP/11/07633/GEN/G/00

4.7 Appendix

Figure 6.

Logarithmically-scaled Scopus, IEEE Xplore, and combined, number of publication search results using keywords extracted from reviewed articles, arranged alphabetically [132].

Figure 6a shows publications containing "academia" through "cpss"
Figure 6b shows publications containing "critical infrastructures" through "cyber threats"
Figure 6c shows publications containing "cyber treaty" through "ecosystem"
Figure 6d shows publications containing "embedded computing technologies" through "information technology"
Figure 6e shows publications containing "insider" through "multi-agent systems"
Figure 6f shows publications containing "national cyber strategies" through "scada"
Figure 6g shows publications containing "scientific paper" through "sovereignty"
Figure 6h shows publications containing "space" through "web space"

Figure 6a. Scopus, IEEE Xplore, & total incidences, of "academia" through "cpss"

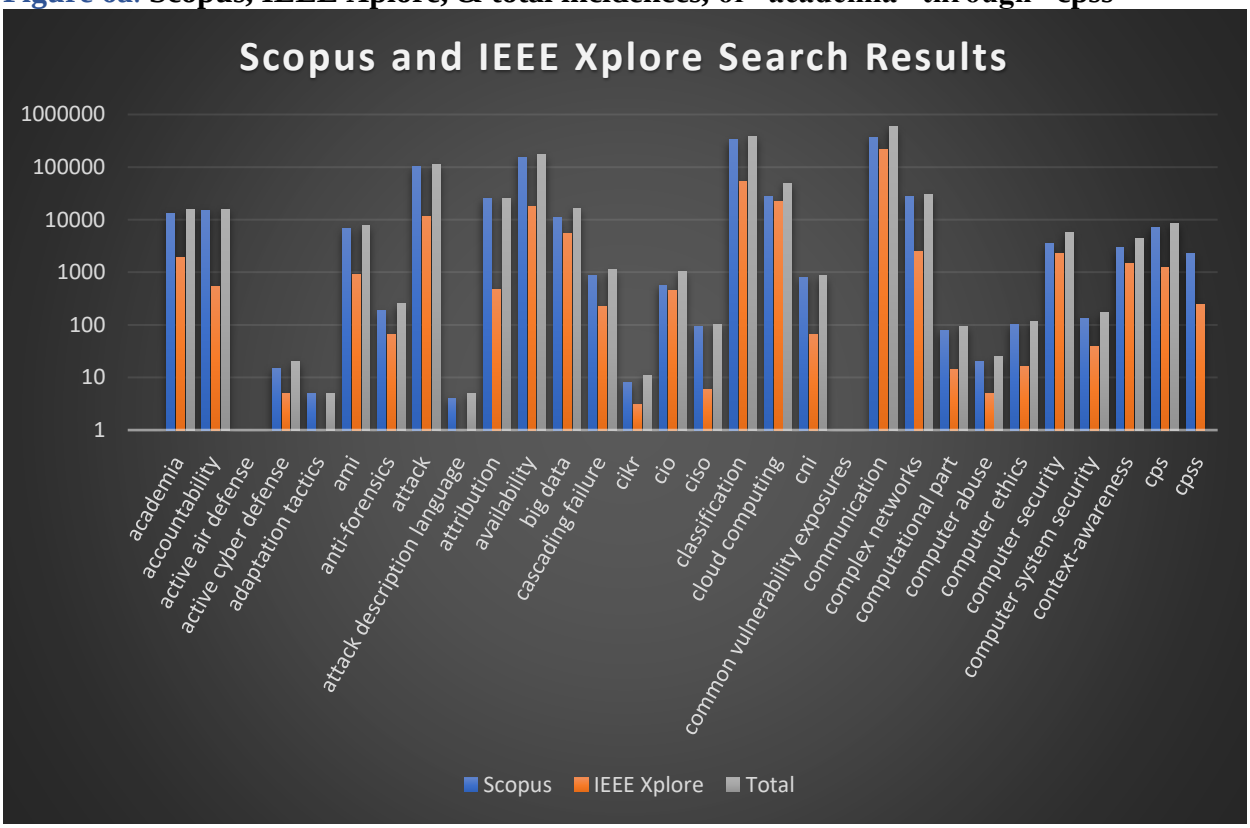


Figure 6b. Scopus, IEEE Xplore, & total incidences, of "critical infrastructures" through "cyber threats"

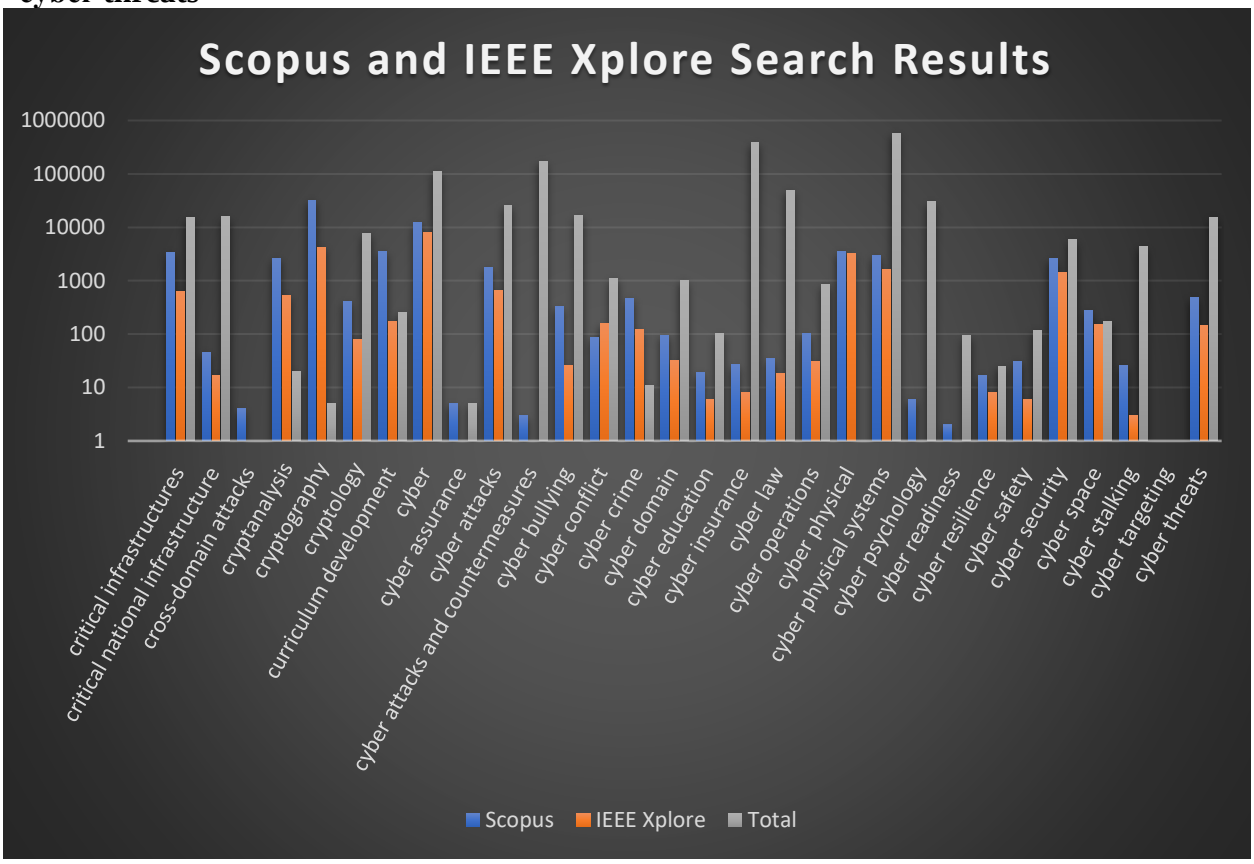


Figure 6c. Scopus, IEEE Xplore, & total incidences, of "cyber treaty" through "ecosystem"

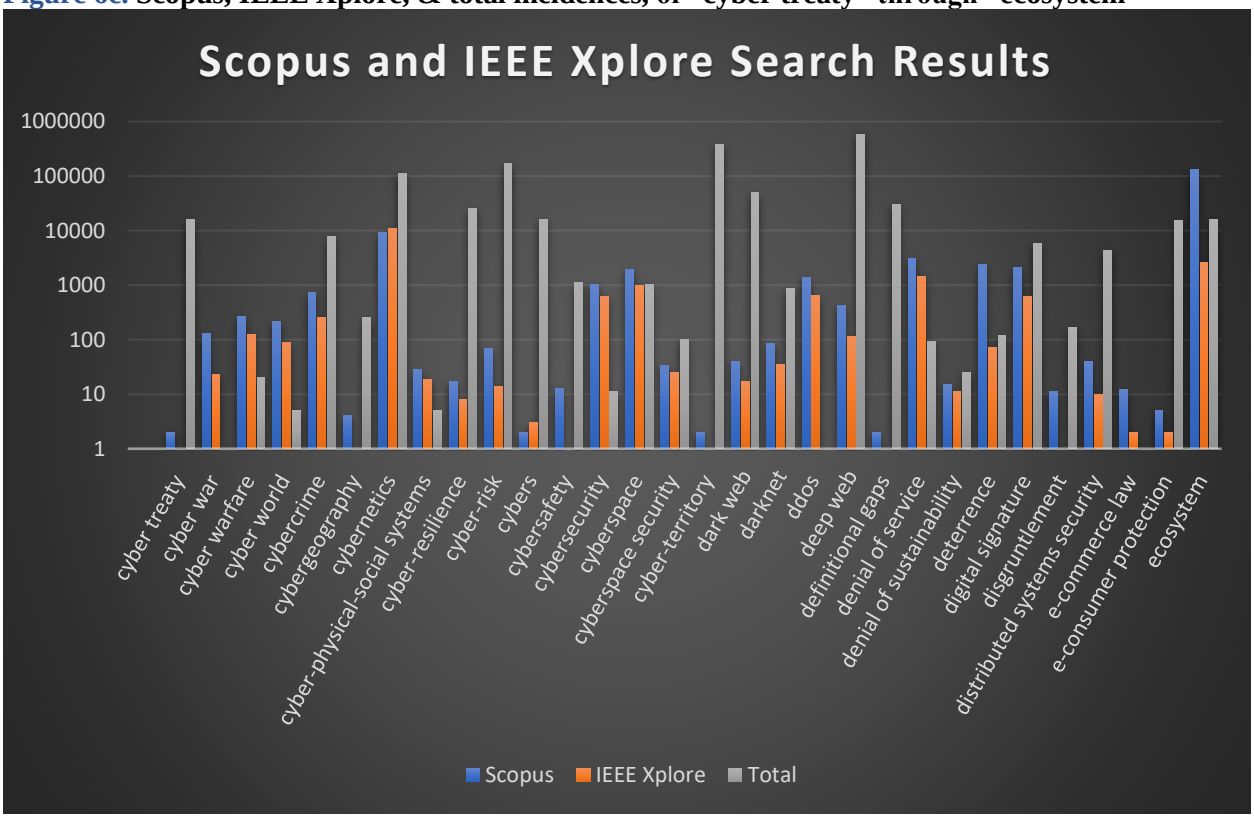


Figure 6d. **Scopus, IEEE Xplore, & total incidences, of "embedded computing technologies" through "information technology"**

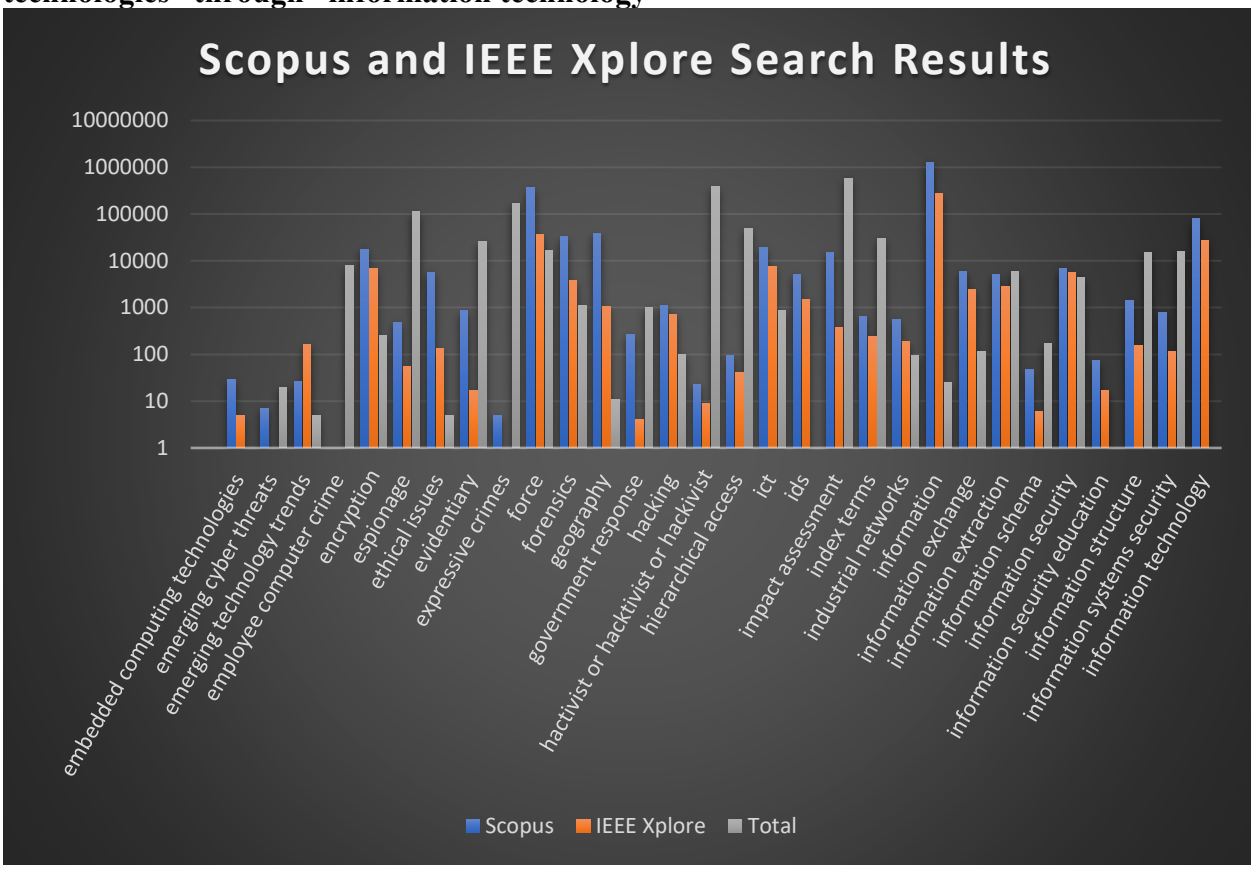


Figure 6e. **Scopus, IEEE Xplore, & total incidences, of "insider" through "multi-agent systems"**

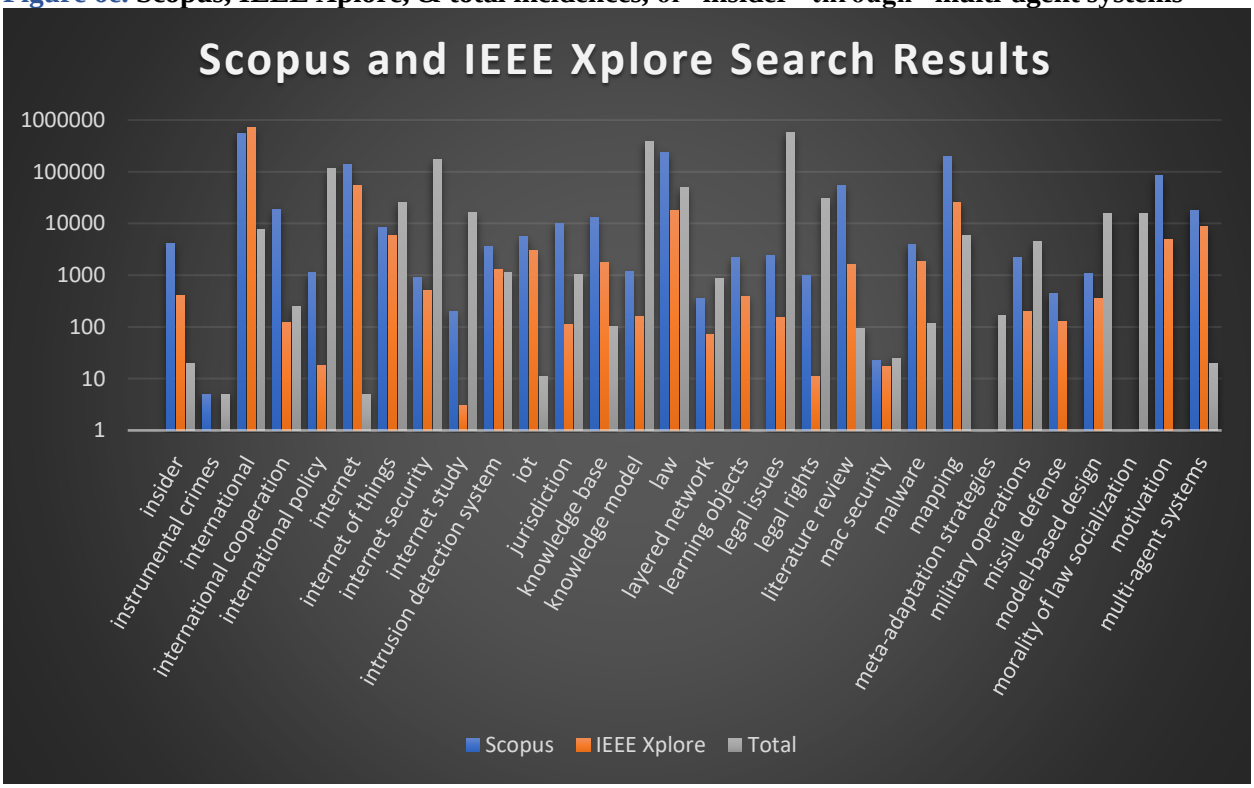


Figure 6f. Scopus, IEEE Xplore, & total incidences, of "national cyber strategies" through "scada"

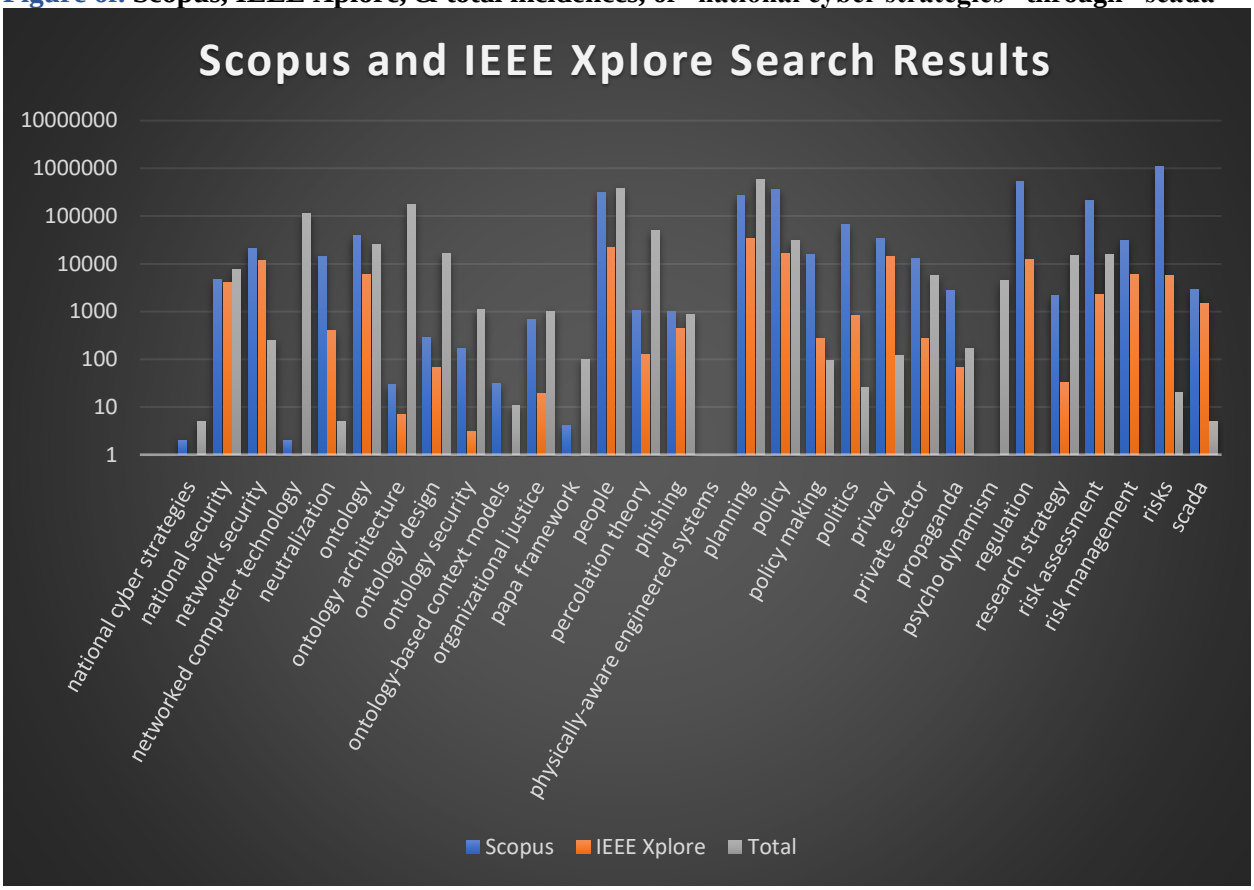


Figure 6g. Scopus, IEEE Xplore, and total incidences, of "scientific paper" through "sovereignty"

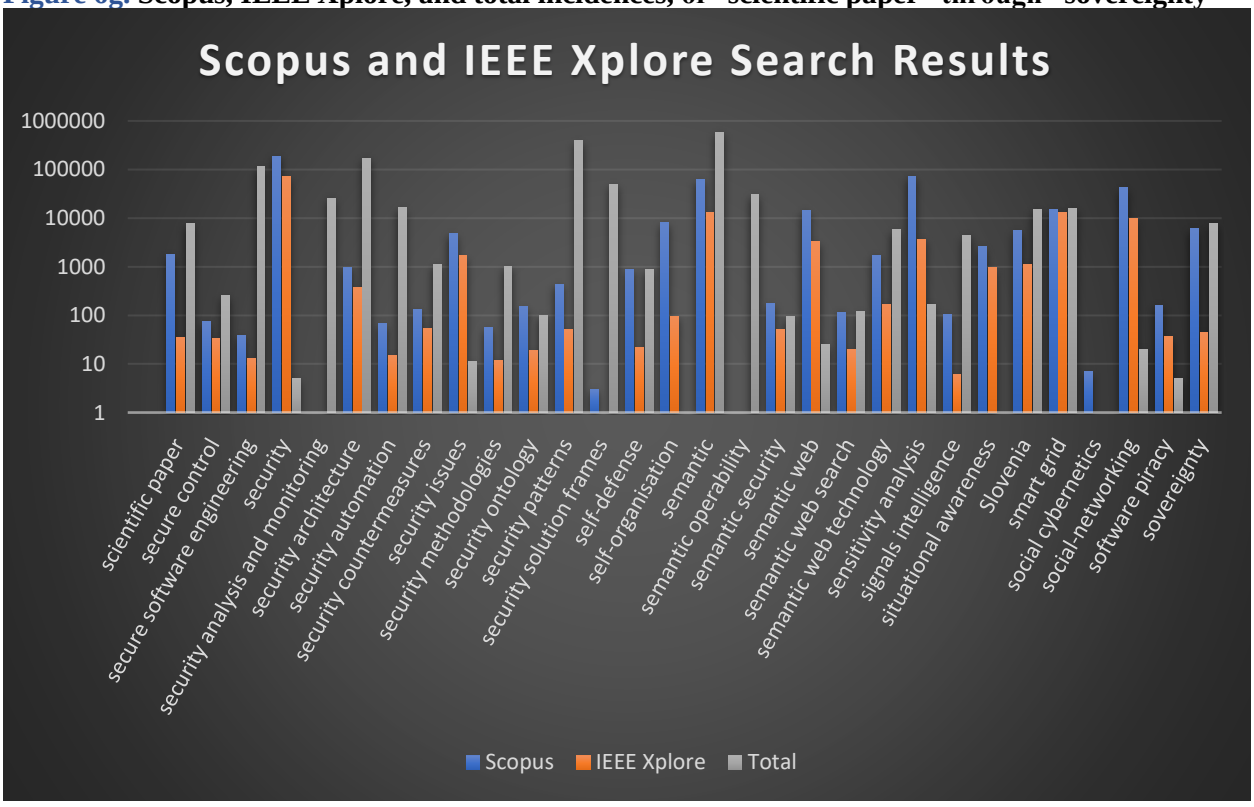


Figure 6h. Scopus, IEEE Xplore, and total incidences, of "space" through "web space"

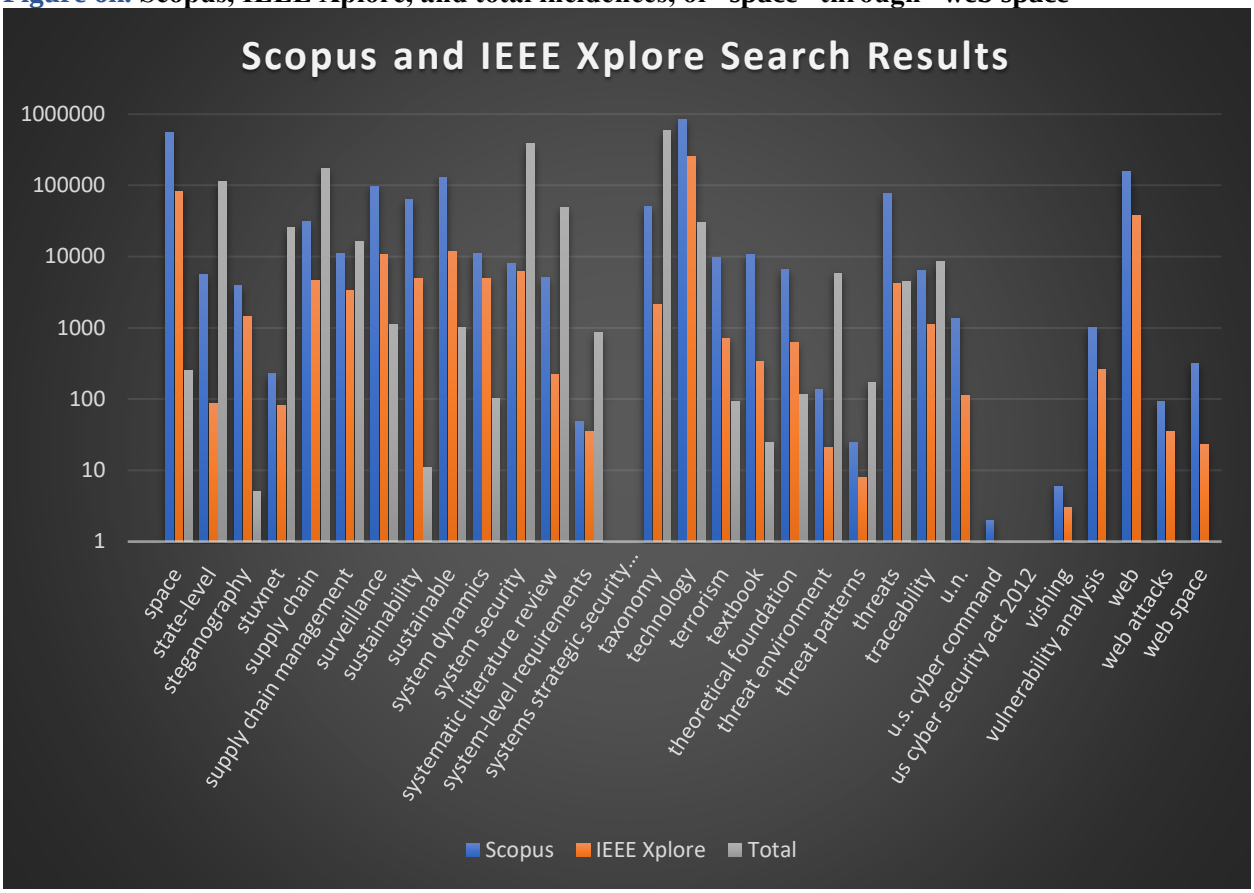


Table 11.

All keywords extracted from publications from the literature review (Chapter 2). Sorted by power of 10 of the number of publication results returned from searching Scopus and IEEE Xplore [132].

Category (number of hits)	Term (Scopus)		Term (IEEE Xplore)	
1 (1,000,000+)	information	risks		
2 [100000,1000000)	attack availability classification communication ecosystem force international internet law mapping	people planning policy regulation risk assessment security space sustainable technology web	communication information	international technology
3 [10000,100000)	academia accountability attribution big data cloud computing complex networks	network security neutralization ontology policy making politics privacy	attack availability classification cloud computing cybernetics force	people planning policy privacy regulation security

	cryptography cyber encryption forensics geography ict impact assessment information technology international cooperation jurisdiction knowledge base literature review motivation multi-agent systems	private sector risk management semantic semantic web sensitivity analysis smart grid social-networking supply chain management supply chain management surveillance sustainability system dynamics taxonomy textbook threats	information technology internet law mapping network security	semantic smart grid space surveillance sustainable web
4 [1000,10000)	ami computer security context-awareness cps cpss critical infrastructures cryptanalysis curriculum development cyber attacks cyber physical cyber physical systems cyber security cybernetics cybersecurity cyberspace ddos denial of service deterrence digital signature ethical issues hacking ids information exchange information	intrusion detection system iot knowledge model learning objects legal issues malware military operations model-based design national security percolation theory phishing propaganda research strategy scada scientific paper security issues self-organisation semantic web technology situational awareness Slovenia sovereignty state-level steganography system security	academia big data complex networks computer security context-awareness cps cryptography cyber cyber physical cyber physical systems cyber security denial of service ecosystem encryption forensics geography ict ids information exchange information extraction information security internet of things intrusion detection system iot	knowledge base literature review malware motivation multi-agent systems national security ontology risk assessment risk management risks scada security issues semantic web sensitivity analysis Slovenia social-networking steganography supply chain supply chain management sustainability system dynamics system security taxonomy threats

	extraction information security information structure insider international policy internet of things	systematic literature review terrorism theoretical foundation traceability u.n. vulnerability analysis		traceability
5 [100,1000)	anti-forensics cascading failure cio cni computer ethics computer system security cryptology cyber bullying cyber crime cyber operations cyber space cyber threats cyber war cyber warfare cyber world cybercrime deep web espionage evidentiary government response index terms	industrial networks information systems security internet security internet study layered network legal rights missile defense ontology design ontology security organizational justice security architecture security countermeasures security ontology security patterns self-defense semantic security semantic web search signals intelligence software piracy stuxnet threat environment web space	accountability ami attribution cascading failure cio cpss critical infrastructures cryptanalysis curriculum development cyber attacks cyber conflict cyber crime cyber space cyber threats cyber warfare cybercrime cybersecurity cyberspace ddos deep web digital signature emerging technology trends ethical issues hacking impact assessment index terms industrial networks	information structure information systems security insider international cooperation internet security jurisdiction knowledge model learning objects legal issues military operations missile defense model-based design neutralization percolation theory phishing policy making politics private sector security architecture semantic web technology situational awareness systematic literature review terrorism textbook theoretical foundation u.n. vulnerability analysis
6 [10,100)	active cyber defense ciso	denial of sustainability disgruntlement	anti-forensics cni	layered network legal rights

	computational part	distributed systems security	computational part	mac security
	computer abuse	e-commerce law	computer ethics	ontology design
	critical national infrastructure	embedded computing technologies	computer system security	organizational justice
	cyber conflict	emerging technology trends	critical national infrastructure	propaganda
	cyber domain	hacktivist/hacktivist	cryptology	research strategy
	cyber education	hierarchical access information	cyber bullying	scientific paper
	cyber insurance	schema information	cyber domain	secure control
	cyber law	security education	cyber law	secure software engineering
	cyber resilience	mac security ontology	cyber operations	security automation
	cyber safety	architecture ontology-based	cyber war	security countermeasures
	cyber stalking	context models	cyber world	security methodologies
	cyber-physical-social systems	secure control secure software	cyber-physical-social systems	security ontology
	cyber-resilience	engineering security	cyber-risk	security patterns
	cyber-risk	automation security	cyberspace security	self-defense
	cybersafety	methodologies system-level	dark web	self-organisation
	cyberspace security	requirements	darknet	semantic security
	dark web	threat patterns	denial of sustainability	semantic web search
	darknet	web attacks	deterrence	software piracy
			distributed systems security	sovereignty
			espionage	state-level
			evidentiary	stuxnet
			hierarchical access information	system-level requirements
			security education	threat environment
			international policy	web attacks
				web space
7 [0,10)	active air defense	employee computer crime	active air defense	embedded computing technologies
	adaptation tactics	expressive crimes	active cyber defense	emerging cyber threats
	attack description language	instrumental crimes	adaptation tactics	employee computer crime
	cikr	meta-adaptation strategies	attack description language	expressive crimes
	common vulnerability exposures	morality of law socialization	cikr	government response

	cross-domain attacks	national cyber strategies	ciso	hacktivist/hacktivist
	cyber assurance	networked computer technology	common vulnerability exposures	information schema instrumental crimes
	cyber attacks and countermeasures	papa framework	computer abuse cross-domain attacks	internet study
	cyber psychology	physically-aware engineered systems	cyber assurance	morality of law socialization
	cyber readiness	psycho dynamism	cyber attacks and countermeasures	national cyber strategies
	cyber targeting	security analysis and monitoring	cyber education	networked computer technology
	cyber treaty	security solution frames	cyber insurance	ontology architecture
	cybergeography	semantic operability	cyber psychology	ontology security
	cybers	social cybernetics	cyber readiness	ontology-based context models
	cyber-territory	systems strategic security management	cyber resilience	papa framework
	definitional gaps	u.s. cyber command	cyber safety	physically-aware engineered systems
	e-consumer protection	us cyber security act 2012	cyber stalking	psycho dynamism
	emerging cyber threats	vishing	cyber targeting	security analysis and monitoring
			cyber treaty	Security solution frames
			cybergeography	
			cyber-resilience	semantic operability
			cybers	signals intelligence
			cybersafety	social cybernetics
			cyber-territory	systems strategic security management
			definitional gaps	
			disgruntlement	threat patterns
			e-commerce law	u.s. cyber command
			e-consumer protection	us cyber security act 2012
				vishing

5 Conclusion

DISCLAIMER
This chapter is partially based on an edited version of prior work.

5.1 Review of Findings and Contributions

This thesis developed arguments for the interdisciplinary nature of cyber security and presented steps for institutions and individuals to take to benefit from this nature. Three research questions were used to guide this research. The three research questions are restated below along with the findings and contributions of the thesis with respect to addressing these questions.

SUBDISCIPLINES What are the different broad categories of cyber security research, how many are there, to what extent, if any, are they actually segregated, and what specific types of research comprise these areas?

Cyber security topics were found to fall into four categories that were given the labels *Policy*, *Infrastructure*, *Business*, and *General*. These labels are misnomers, however, because each category is itself too broad to describe in a single word. Labels without semantic meaning might be a better way to refer to these categories. However, these labels are helpful for describing the topics of the four categories. This categorization groups topics and issues together based on the goals and concerns of actors, rather than by their methods. Cyber security as a discipline does not have many formal methods, and is a system that sits on top of other areas of work. As such, it is subject to be viewed independently by these groups, even though the concerns of the groups overlap and, due to pervasive computing, the systems each of these categories is concerned with also overlap.

The *Public* category includes issues of concern to governments. It includes work regarding laws, international norms, and national security. Global technical standards produced by bodies like as ICANN and W3C, while often specifying norms, are instead placed in the *Infrastructure* category.

Infrastructure topics include most technological problems of cyber security; specifically, those problems related to the actual infrastructure of cyberspace. The *Infrastructure* category includes various aspects of the cyber security of critical infrastructure, as well as security issues concerning the operation of cyberspace, such as cryptography. It also encompasses methods for intrusion detection, reverse engineering, and computer forensics, among other issues. This does not necessarily cover technical solutions to every security problem that businesses or academic researchers might address.

Business as a category concerns business practices and other organizational and human factors affecting cyber security. This includes social engineering, supply chain management, business operations, recruitment and training, and security culture, for example.

The *General* category contains all issues which pervade the entire realm of cyber security, as well as descriptions of the field in general, and characterizations of cyberspace and humans' interactions with it – including most work done in the social sciences. The topic of this thesis can be classified under the *General* category.

In 2015, the European CAMINO Project created the THOR acronym approach of "(T)echnical", "(H)uman", "(O) rganizational", and "(R)egulatory." The CAMINO Project asserts that cyber security can be comprehensively perceived as a combination of these four dimensions. These four dimensions are related to the four disciplines I independently identified, although they are slightly different. For example, the *General* and *Business* categories can include technical problems and solutions. THOR is also not self-contained; i.e. the design of THOR as a topic of study cannot be grouped into any of its categories. Human factors also bridge both the Business and General realms.

The categorization this thesis presents is useful because it intuitively presents and explains the disparities between the fields, and emphasizes that professionals from these fields do not typically work together. This disparity is evident in both the differing focuses of the separate fields, as well as in the differing phraseologies of the fields that are nevertheless used to describe similar concepts – with conflicts sometimes existing even within a single journal article, as found in the literature review covered in Chapter 2. These categories are misaligned in incentives, languages, knowledge bases, and worldviews, which causes actors in distinct categories, such as researchers and other professionals, to not communicate effectively. This tends to reinforce the separation between the groups. Addressing this problem at the root through education, to align knowledge bases and worldviews; and through communication channels, to align language, can contribute to unifying cyber security initiatives between these groups. This unification can in turn allow actors to coordinate in solving their common problems, such as CIOs and insurance companies not communicating, or academics not researching business-relevant security [42].

<u>EDUCATION</u> What changes to educating cyber security professionals, whether researchers or otherwise, can best enable the workforce to address multi-faceted issues of cyber security now and in the future?

A review of academic programs in cyber security in the United States was performed. Considering the majority of the workforce does not focus on cyber security, but nevertheless benefits from knowledge of it, specific graduate studies programs at universities were determined to be ineffectual for MIT or for solving the most pressing problems of cyber security. As such, the specific change to educational practice most needed is argued to be a multi-

departmental interdisciplinary minor in cyber security studies that encompasses topics from the four categories of cyber security. This can update the knowledge bases of the workforce (including workers who do not work on cyber security) and adjust their worldview, to optimize cyber security given the number of professional security workers. It is important for cyber security to be a built in, systemic, and widespread practice. This would also alleviate the talent shortage. It is likely unnecessary for so many people to focus on cyber security specifically, or for this knowledge to be so specialized, concentrated, and restricted. Rather, cyber security should be an integrated set of knowledge held by a large number of people.

The effort to create such a program at MIT is well underway, but requires the support of faculty to formally implement it. If enough faculty support can be garnered, then this minor may be available to undergraduates starting in Fall 2018. As of this writing, however, the effort is still in the proposal stage.

For other universities wishing to implement a similar program, Table 1 and Table 3 should be consulted. Most important for the execution of such a proposal is to design the curriculum to be broad and multi-departmental. Unfortunately, barriers to communication caused by the separation of cyber security fields might make it difficult for faculty to coordinate to get such an initiative off the ground. However, doing so would be an important and necessary step to breaking the cycle of separation of the four subdisciplines of cyber security.

TERMINOLOGY If the observations of siloed-off areas of cyber security research and innovation are informed in part by extreme differences in the vocabularies, to what extent does terminology differ between the disciplines, how has it evolved over time, and what guidelines can authors or standards bodies use when deciding how best to communicate with broad, interdisciplinary audiences about cyber security?

Specific recommendations for terminology harmonization include that authors use "cyber" as a separate word (perhaps hyphenated) in phrases (except for "cyberspace," which should always be one word), and should avoid ad hoc constructs. In addition, although "cyber security" can acceptably be written as either one or two words, two words is more common. That said, within the field of computer science, cyber security is often simply referred to as "security."

The vocabulary differences between the four areas of cyber security were shown to be great, but not so great that they cannot be merged. Within the categories I identified, use of standard terminology is fairly common. However, there is clear room for improvement among authors and working groups. As was shown in Figure 4, cyber security terminology has evolved significantly over time, but may be beginning to standardize. The best guidelines for using cyber security terminology in communications are to follow Table 8, and to only use words with definitions,

widespread use, and that yield meaningful search results. Rigorously defining these terms (which requires formalizing cyber security as a research field) would be a more powerful way to ensure that communication is standardized.

Many authors still use ad hoc terms despite the existence of standards glossaries, and spelling or phrasing of many terms is still not agreed upon. The lack of collaboration across disciplines inferred from the literature review emphasizes the need for more comprehensive standard terminology for both cyber security and broader cyber research. Except when radically new concepts are written about, greater use of more widely accepted terms is recommended, though not at the expense of innovation. Authors should, before submitting for publishing, search databases for their potential keywords to ensure that all are in the [10,100000) range, and that at least one is in the [100,1000) range to ensure good searchability.

I outlined guidelines to use when considering keywords to use in future publications and when crafting terminology standards, and resolved some long-held misconceptions in spelling and phrasing. I encourage use of these guidelines and the following recommendations, as well as the use of the standard glossary projects from EWI, NICCS, and other complementary sources like NISTIR 7298.

5.2 Future Work and Limitations of this Thesis

I proposed a classification of research areas concerned with cyber security, which can be refined by a more comprehensive study of keywords comprising it (i.e. topic modeling). These keywords can be used to craft research agendas for each area, as well as in crafting cross-disciplinary research agendas for cyber security. Other possible categorizations may consist of the common social sectors of civil society, industry, academia, and the government that many articles cite [127]. I encourage future researchers to delve further into categorization and ontology creation of cyber security for the formulation of research agendas.

Identifying different areas of cyber security research is an important step towards formalizing the research methodology of cyber security. However, one limitation of this research is that communication pathways cannot be fully opened unless terminology is formally defined. Because of this, individual actors will likely not be able to harmonize terminology. Rather, standards bodies and researchers must make security a more formal discipline, the way cryptography has been formalized, in order for ambiguity in communications to be remediated.

In addition, by design, the four cyber security categories described are only loosely defined. However, this limits the usefulness of the categories for formally analyzing actor interactions and incentives, and it causes difficulty when considering why certain actors do not coordinate. For instance, CIOs and cyber insurance companies do not communicate well [42]. Although this

could be due to misaligned incentives, it is difficult to decide whether to classify CIOs (or particular problems they work on) into the *Business* category or the *Infrastructure* category; or whether to place insurers under *Business* or *General*. The framework for understanding cyber security as four separate disciplines is useful for understanding that these disciplines do not coordinate, but not necessarily for understanding the separate disciplines, because it was designed to be comprehensive in including topics from all of security, but not to restrict these topics to single categories. Furthermore, the number of categories may change over time.

Because the papers reviewed were necessarily all recently published, and not all from the same year, (2010-2015), it is difficult to determine any correlation between type of vocabulary used and citations. Future research could aim to verify whether such a correlation exists – a positive one could bolster efforts toward adoption of standard vocabulary. However, I believe that regardless, there are compelling reasons to update existing cyber security glossaries.

These existing dictionaries are, however, mostly constructed by the public sector, and may or may not reflect academic and private sector areas of study and work regarding cyber security. Therefore, greater effort from outside of governments, and collaboration with the greater global multistakeholder community, is essential when creating or updating cyber security glossaries. For instance, SANS has a cyber security glossary, but it is much more focused on terms from the Infrastructure category than any other category. However, collaboration between SANS and other groups may be a feasible path moving forward [136].

Future work towards harmonizing terminology could include developing an online learning system that perpetually updates a glossary of terms according to the four terminology standard guidelines provided in this thesis. Researchers could continually scrape publications and databases for relevant words and phrases, and future work along this path should more systematically incorporate dictionary terms, to avoid the risk of overlooking important terminology.

Future applications of this research can also include more on how to optimize security papers for search engines, and how to optimize security literature review searches. Finally, Category 6 in Table 11 may outline other new or underserved areas of cyber security research.

Cyber security is a field of many disciplines. Bringing those disciplines together into a cohesive system will be what moves us past the challenges of today and into a future where security bridges their gaps and thereby accelerates innovation.

References

1. Andel, T. R., & McDonald, J. T. (2013). A Systems Approach to Cyber Assurance Education. Information Security Curriculum Development, 13. doi:10.1145/2528908.2528920
2. Aviad, A. a., Wecel, K. k., & Abramowicz, W. w. (2015). The Semantic Approach to Cyber Security Towards Ontology Based Body of Knowledge. Proceedings Of The European Conference On E-Learning, 328-336.
3. Ayofe, A. g., & Irwin, B. n. (2010). CYBER SECURITY: CHALLENGES AND THE WAY FORWARD. Computer Science & Telecommunications, 29(6), 56-69.
4. Bernik, I., G. Mesko, and V. Lysenko. 2012. "Study of the Perception of Cyber Threats and the Fear of Cybercrime." Inspec, EBSCOhost (accessed October 14, 2015).
5. Blasch, E., Dan, S., Pham, K., & Genshe, C. (2015). Review of game theory applications for situation awareness. Proceedings Of The SPIE, 9469(10 pp.). doi:10.1117/12.2177531
6. Busse, J., Humm, B. b., Lübbert, C., Moelter, F., Reibold, A., Rewald, M., & ... Zeh, T. (2015). Actually, What Does "Ontology" Mean? A Term Coined by Philosophy in the Light of Different Scientific Disciplines. Journal Of Computing & Information Technology, 23(1), 29-41.
7. Butrimas, V. (2013). National Security and International Policy Challenges in a Post Stuxnet World. Lithuanian Annual Strategic Review, 12(1), 11. doi:10.2478/lasr-2014-0001
8. Cheminod, M., Durante, L., & Valenzano, A. (2013). Review of Security Issues in Industrial Networks. IEEE Transactions On Industrial Informatics, 9(1), 277-293. doi:10.1109/TII.2012.2198666
9. Chertoff, M., & Rosenzweig, P. (2015, March 1). A Primer on Globally Harmonizing Internet Jurisdiction and Regulations. Retrieved October 15, 2015.
10. Chertoff, M., & Simon, T. (2015, February 1). The Impact of the Dark Web on Internet Governance and Cyber Security. Retrieved October 15, 2015.
11. Chouhan, R. R. (2014). Cyber Crimes: Evolution, Detection and Future Challenges. IUP Journal Of Information Technology, 10(1), 48-55.
12. Comninos, A. (2013, April 1). A cyber security agenda for civil society: What is at stake? Retrieved October 15, 2015.
13. Denning, D. (2014). Framework and principles for active cyber defense. Computers & Security, 40108-113. doi:10.1016/j.cose.2013.11.004
14. DEV, P. R. (2015). "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response. Texas International Law Journal, 50(2), 379-399.
15. Finlay, A. (Ed.). (2014). Communications surveillance in the digital age.
16. Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. Computers & Security, 4618-31. doi:10.1016/j.cose.2014.06.008
17. Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., & ... Philip Chen, C. L. (2014). SCADA communication and security issues. Security & Communication Networks, 7(1), 175-194.

18. Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal Of Critical Infrastructure Protection, 103-17. doi:10.1016/j.ijcip.2015.04.001
19. Gerostathopoulos, I., Bures, T., Hnetynka, P., Hujecek, A., Plasil, F., Skoda, D., & ... Crnkovic, I. (2015). Meta-Adaptation Strategies for Adaptation in Cyber-Physical Systems. doi:10.1007/978-3-319-23727-5_4
20. Glennon, M. J. (2012). State-level Cybersecurity. Policy Review, (171), 85-102.
21. Glenny, M., & Kavanagh, C. (2012). 800 Titles but No Policy—Thoughts on Cyber Warfare. American Foreign Policy Interests, 34(6), 287-294. doi:10.1080/10803920.2012.742410
22. Graham, M. (n.d). Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities?. Geographical Journal, 179(2), 177-182.
23. Grant, T., & Liles, S. (2014). On the Military Geography of Cyberspace.
24. Gunes, V. g., Peter, S., Givargis, T., & Vahid, F. v. (2014). A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems. KSII Transactions On Internet & Information Systems, 8(12), 4242-4268.
25. Harrop, W., & Matteson, A. (2013). Cyber resilience: A review of critical national infrastructure and cyber security protection measures applied in the UK and USA. Journal Of Business Continuity & Emergency Planning, 7(2), 149-162.
26. Lin, H. (2015, May 15). Thinking about Nuclear and Cyber Conflict: Same Questions, Different Answers. Retrieved October 15, 2015.
27. Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. Computer Law And Security Review: The International Journal Of Technology And Practice, 29236-245. doi:10.1016/j.clsr.2013.03.003
28. Hsu, D. F., Marinucci, D., & Voas, J. M. (2015). Cybersecurity: Toward a Secure and Sustainable Cyber Ecosystem. Computer, 48(4), 12-14.
29. Huang, Z., Wang, C., Stojmenovic, M., & Nayak, A. (2015). Characterization of Cascading Failures in Interdependent Cyber-Physical Systems. IEEE Transactions On Computers, 64(8), 2158-2168. doi:10.1109/TC.2014.2360537
30. Iannacone, M., Bohn, S., Nakamura, G., Gerth, J., Huffer, K., Bridges, R., & ... Goodall, J. (2015). Developing an Ontology for Cyber Security Knowledge Graphs. Conference On Information & Knowledge Management, 1. doi:10.1145/2746266.2746278
31. Jaitner, M. m., & MacDermott, A. a. (2015). Cyber Education? Branches of Science Contributing to the Cyber Domain. Proceedings Of The European Conference On E-Learning, 120-128.
32. Jang-Jaccard, J., & Nepal, S. (2013). A survey of emerging threats in cybersecurity. Journal Of Computer And System Sciences, doi:10.1016/j.jcss.2014.02.005
33. Jardine, E. (2015, July 1). Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime. Retrieved October 15, 2015.
34. JENSEN, E. T. (2015). Cyber Sovereignty: The Way Ahead. Texas International Law Journal, 50(2), 273-302.

35. Ju An, W., Guo, M., & Camargo, J. (2010). An Ontological Approach to Computer System Security. Information Security Journal: A Global Perspective, 19(2), 61-73. doi:10.1080/19393550903404902
36. Kewlani, J. (2014). CYBER CRIME AND SOCIAL CYBERNETICS (A SOCIO-LEGAL ANALYSIS). Government: Research Journal Of Political Science, 36-18.
37. Khan, O., & Sepúlveda Estay, D. A. (2015). Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. Technology Innovation Management Review, 6.
38. Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. (2012). Cyber Security and Privacy Issues in Smart Grids. Ieee Communications Surveys And Tutorials, 14(4), 981-997.
39. Lotrionte, C. (2012). State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights [article]. Emory International Law Review, (2), 825.
40. Matsuno, T., Kawamura, T., Ohkubo, K., Kobayashi, H., Takahashi, K., & Kayaguchi, S. (2012). Emergence of New Cyber Attacks and Future Directions in Security R&D. NTT Technical Review, 10(10),
41. Maurer, T., & Morgus, R. (2014, June 1). Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate. Retrieved October 15, 2015.
42. Messmer, Ellen. 2013. "Cyber insurance decisions leave CIO, CISO out of the loop." Networkworld Asia 10, no. 3: 8. Business Source Complete, EBSCOhost (accessed October 14, 2015).
43. MOORE, S. (2013). Cyber Attacks and the Beginnings of an International Cyber Treaty. North Carolina Journal Of International Law & Commercial Regulation, 39(1), 223-257.
44. Namazifard, A., Tousi, A., Amiri, B., Aminilari, M., & Hozhabri, A. (2015). Literature Review of Different Contention of E-Commerce Security and the Purview of Cyber Law Factors. doi:10.1109/ECDC.2015.7156333
45. Nye, J. (2014, May 1). The Regime Complex for Managing Global Cyber Activities. Retrieved October 15, 2015.
46. OECD principles for internet policy making. (2014). Retrieved October 15, 2015.
47. Oleiwi, S., & Yasin, A. (2013). Scientific paper categorization to multi class using ontology. International Journal Of Digital Content Technology And Its Applications, 7(12), 134-141.
48. Parvin, S., Hussain, F., Hussain, O., Thein, T., & Park, J. (2013). Multi-cyber framework for availability enhancement of cyber physical systems. Computing, 95(10/11), 927-948. doi:10.1007/s00607-012-0227-7
49. Pawlak, P., & Wendling, C. (2013). Trends in cyberspace: can governments keep up?. Environment Systems & Decisions, 33(4), 536-543. doi:10.1007/s10669-013-9470-5
50. Phair, N. (2014). CC14 Feature - Cyber Crime Risks and Responsibilities for Businesses. Journal Of The Australian & New Zealand Institute Of Insurance & Finance, 37(5), 5-8.
51. Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. Journal Of Strategic Studies, 38(1/2), 4-37. doi:10.1080/01402390.2014.977382
52. Rogers, R. (2012). Mapping and the Politics of Web Space. Theory, Culture And Society, 29(4-5), 193-219.

53. ROSCINI, M. (2015). Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. Texas International Law Journal, 50(2), 233-273.
54. Schmitt, M. N. (2015). THE LAW OF CYBER TARGETING. Naval War College Review, 68(2), 10-29.
55. Shafi, Q. (2012). Cyber Physical Systems Security: A Brief Survey. doi:10.1109/ICCSA.2012.36
56. Shull, A., Twomey, P., & Yoo, C. (2014, June 1). Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community. Retrieved October 15, 2015.
57. Sitnikova, E., & Asgarkhani, M. (2014). A strategic framework for managing internet security. 2014 11Th International Conference On Fuzzy Systems & Knowledge Discovery (FSKD), 947. doi:10.1109/FSKD.2014.6980967
58. Smirnov, A., Levashova, T., Shilov, N., & Sandkuhl, K. (2014). Ontology for cyber-physical-social systems self-organisation. doi:10.1109/FRUCT.2014.7000933
59. TAKESHI TAKAHASHI1, t., & YOUKI, K. (2015). Reference Ontology for Cybersecurity Operational Information. Computer Journal, 58(10), 2297-2312.
60. TAN MING MING1, t., JABAR, M. m., SIDI, F. f., & KOH TIENG WEI1, t. (2015). A SYSTEMATIC LITERATURE REVIEW OF COMPUTER ETHICS ISSUES. Journal Of Theoretical & Applied Information Technology, 78(3), 360-372.
61. Uzunov, A. V., Falkner, K., & Fernandez, E. B. (2015). A comprehensive pattern-oriented approach to engineering security methodologies. Information And Software Technology, 57217-247. doi:10.1016/j.infsof.2014.09.001
62. Veerasamy, N., Grobler, M., Von Solms, B., Filiol, E., & Erra, R. (2012). Building an Ontology for Cyberterrorism.
63. VEGH, L. l., & MICLEA, L. l. (2015). Authenticity, Integrity and Secure Communication in Cyber-Physical Systems. Journal Of Computer Science & Control Systems, 8(1), 33-38.
64. Verhulst, S., Noveck, B., Raines, J., & Declercq, A. (2014, December 1). Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem. Retrieved October 15, 2015.
65. Wali, A., Soon Ae, C., & Geller, J. (2013). A bootstrapping approach for developing a cyber-security ontology using textbook index terms. doi:10.1109/ARES.2013.75
66. Wan, K. k., & Alagar, V. a. (2014). Context-Aware Security Solutions for Cyber-Physical Systems. Mobile Networks & Applications, 19(2), 212-226.
67. Weber, R. (2014, December 1). Legal Interoperability as a Tool for Combatting Fragmentation. Retrieved October 15, 2015.
68. Willison, R., & Warkentin, M. (2013). BEYOND DETERRENCE: AN EXPANDED VIEW OF EMPLOYEE COMPUTER ABUSE. MIS Quarterly, 37(1), 1-20.
69. Wilshusen, G. C. (2011). CYBERSECURITY OVERVIEW. International Debates, 9(9), 4-9.

70. Yampolskiy, M., Horváth, P., Koutsoukos, X. D., Xue, Y., & Sztipanovits, J. (2015). A language for describing attacks on cyber-physical systems. International Journal Of Critical Infrastructure Protection, 840-52. doi:10.1016/j.ijcip.2014.09.003
71. Zekos, G. z. (2012). CYBER-TERRITORY AND JURISDICTION OF NATIONS. Journal Of Internet Law, 15(12), 3-23.
72. Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. (2012). A survey of cyber crimes. Security & Communication Networks, 5(4), 422-437.
73. Zlomislić, V. v., Fertalj, K. k., & Sruk, V. v. (2014). Denial of Service Attacks: An Overview. CISTI (Iberian Conference On Information Systems & Technologies / Conferência Ibérica De Sistemas E Tecnologias De Informação) Proceedings, 1270-275.
74. Khairkar, A., Kshirsagar, D., & Kumar, S. (2013). Ontology for Detection of Web Attacks. doi:10.1109/CSNT.2013.131
75. Choucri, N., Daw Elbait, G., & Madnick, S. (2012, November 6). What is Cybersecurity? Explorations in Automated Knowledge Generation. Retrieved January 6, 2016.
76. Resilience in the Cyber Era: Building an Infrastructure that Secures and Protects. The Economist. (2011). Retrieved January 6, 2016.
77. Lingenheld, M. (2015, April 17). The Unfortunate Growth Sector: Cybersecurity. Retrieved January 6, 2016, from http://www.forbes.com/sites/michaellingenheld/2015/04/27/the-unfortunate-growth-sector-cybersecurity/
78. Rohan. (2015, June). Cyber Security Market worth $170.21 Billion by 2020. Retrieved January 6, 2016, from http://www.marketsandmarkets.com/PressReleases/cyber-security.asp
79. Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience. 39. (2012). Retrieved January 6, 2016, from http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience
80. NIST. ANNOUNCING DEVELOPMENT OF A FEDERAL INFORMATION PROCESSING STANDARD FOR ADVANCED ENCRYPTION STANDARD. (1997, January 2). Retrieved January 6, 2016, from http://csrc.nist.gov/archive/aes/pre-round1/aes_9701.txt
81. Ma, J., Ning, H., Huang, R., Liu, H., Yang, L., Chen, J., & Min, G. (2015). Cybermatics: A Holistic Field for Systematic Study of Cyber-Enabled New Worlds. *IEEE Access,* 2270-2280. doi:10.1109/ACCESS.2015.2498288
82. Choras, M.; Kozik, R.; Torres Bruna, M.P.; Yautsiukhin, A.; Churchill, A.; Maciejewska, I.; Eguinoa, I.; Jomni, A., "Comprehensive Approach to Increase Cyber Security and Resilience," in *Availability, Reliability and Security (ARES), 2015 10th International Conference on* , vol., no., pp.686-692, 24-27 Aug. 2015 doi: 10.1109/ARES.2015.30
83. Framework for Improving Critical Infrastructure Cybersecurity. (2014, February 12). Retrieved January 6, 2016, from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

84. Neri, F.; Geraci, P.; Sanna, G.; Lotti, L., "Online Police Station, A State-of-Art Italian Semantic Technology against Cybercrime," in *Social Network Analysis and Mining, 2009. ASONAM '09. International Conference on Advances in* , vol., no., pp.296-299, 20-22 July 2009
doi: 10.1109/ASONAM.2009.20
85. Howard, M. C., & Jayne, B. S. (2015). An Analysis of More Than 1,400 Articles, 900 Scales, and 17 Years of Research: The State of Scales in Cyberpsychology, Behavior, and Social Networking. Cyberpsychology, Behavior & Social Networking, 18(3), 181-187. doi:10.1089/cyber.2014.0418
86. NETmundial Comments. Retrieved December 9, 2015, from http://document.netmundial.br/
87. What is SNOMED CT? (2014, July 31). Retrieved January 7, 2016, from http://www.ihtsdo.org/snomed-ct/what-is-snomed-ct
88. ABOUT THE IEEE STANDARDS ASSOCIATION. Retrieved January 7, 2016, from http://standards.ieee.org/about/ieeesa.html
89. Fernelius, W., Loening, K., & Adams, R. (1976). Historical development of chemical nomenclature. Journal of Chemical Education, 53(6), 354-354. doi:DOI: 10.1021/ed053p354.2
90. IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations - Redline," in *IEEE Std 692-2010 (Revision of IEEE Std 692-1997) - Redline* , vol., no., pp.1-50, Feb. 12 2010
doi: 10.1109/IEEESTD.2010.5953432
91. IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations," in *IEEE Std 692-2013 (Revision of IEEE Std 692-2010)* , vol., no., pp.1-57, Sept. 30 2013
doi: 10.1109/IEEESTD.2013.6613502
92. 2 Results Returned for 'cyber' Retrieved January 7, 2016, from http://ieeexplore.ieee.org/xpls/dictionary.jsp?stdDict=browse_keyword&pageNumber=1&def_term=cyber&def_id=&stdDictionary_tarid=&stdDictionary_tarn=null&stdDictionary_scn=Aerospace Electronics&nav=#
93. Ganor, B. (2002). Defining Terrorism - Is One Man's Terrorist Another Man's Freedom Fighter? *Police Practice and Research, 3*(4), 287–304-287–304. doi:DOI: 10.1080/1561426022000032060
94. https://books.google.com/ngrams/graph?content=cyber*&year_start=1945&year_end=2015&corpus=15&smoothing=3&share=&direct_url=t2;,cyber *;,c0;,s0;;cyber security;,c0;;cyber attacks;,c0;;cyber crime;,c0;;cyber%
95. Valeriano, B., & Maness, R. (2013). What Do We Know about Cyber Conflict ? Scope, Impact, and Restraint in Cyberspace.
96. Lin, Herb. Cyber Conflict and National Security.
97. Strunk, W., White, E. B., & Kalman, M. (2005). *The elements of style*. p 36.New York : Penguin Press, 2005.
98. RIVEST, R. L. (1990). CHAPTER 13: Cryptography. *Algorithms And Complexity*, 717,719-717,755. doi:10.1016/B978-0-444-88071-0.50018-7

99. Jackson, W. (2011, April 28). U.S., Russian groups agree on 20 definitions of cybersecurity concepts. Retrieved January 9, 2016, from https://gcn.com/articles/2011/04/28/us-russia-cyber-dictionary.aspx
100. Rauscher, K. (2011, April 26). Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations. Retrieved January 9, 2016, from http://www.eastwest.ngo/idea/russia-us-bilateral-cybersecurity-critical-terminology-foundations
101. Stern, S. (2014, March 21). Critical Terminology Foundations 2. Retrieved January 9, 2016, from http://www.eastwest.ngo/idea/critical-terminology-foundations-2
102. Cyber Glossary. Retrieved January 9, 2016, from https://niccs.us-cert.gov/glossary
103. Health expenditure, total (% of GDP). (n.d.). Retrieved January 9, 2016, from http://data.worldbank.org/indicator/SH.XPD.TOTL.ZS
104. Net Losses: Estimating the Global Cost of Cybercrime: Economic impact of cybercrime II. (2014, June). Retrieved January 9, 2016, from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
105. Information Assurance Concentration Programs. Retrieved January 11, 2016, from http://ia.asu.edu/education.php
106. Core Courses. Retrieved January 11, 2016, from http://www.uwb.edu/cybersecurity/curriculum/core-courses
107. Master of Engineering in Cybersecurity. (2016). Retrieved January 11, 2016, from http://cyber.umd.edu/education/meng-cybersecurity
108. Outline of academic disciplines. Retrieved January 11, 2016, from https://en.wikipedia.org/wiki/Outline_of_academic_disciplines
109. -ism. Retrieved January 11, 2016, from http://etymonline.com/index.php?term=-ism&allowed_in_frame=0
110. Omics. Retrieved January 11, 2016, from https://en.wikipedia.org/wiki/Omics
111. νόμος. Retrieved January 11, 2016, from https://en.wiktionary.org/wiki/νόμος
112. Cybercrime. Retrieved January 14, 2016, from http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
113. What is Cybercrime? Retrieved January 14, 2016, from http://us.norton.com/cybercrime-definition
114. Cyber crime. Retrieved January 14, 2016, from http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime
115. Kurbalija, J. (2015, April 17). Different prefixes, same meaning: Cyber, digital, net, online, virtual, e-. Retrieved January 14, 2016, from http://www.diplomacy.edu/blog/different-prefixes-same-meaning-cyber-digital-net-online-virtual-e
116. Internet-related prefixes. Retrieved January 14, 2016, from https://en.wikipedia.org/wiki/Internet-related_prefixes#Spelling_controversies

117. Kissel, R. (Ed.). (2013, May 1). NISTIR 7298 Revision 2, Glossary of Key Information Security Terms. Retrieved January 14, 2016, from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=913810
118. Robert Evans. (2009). *Control Systems Cyber Security Standards Support Activities*. United States. doi:10.2172/950989
119. Benigni, D. (2010). Cyber Security Standards. In J. Voeller (Ed.), Wiley Handbook of science and technology for homeland security. Hoboken, NJ: Wiley.
120. National Information Assurance Glossary. (2006, June). Retrieved from http://jitc.fhu.disa.mil/pki/documents/committee_on_national_security_systems_instructions_4009_june_2006.pdf
121. Applegate, S., Stavrou, A., Podins, K., Stinissen, J., & Maybaum, M. (2013). Towards a Cyber Conflict Taxonomy.
122. Rodin, D. N. (2015). THE CYBERSECURITY PARTNERSHIP: A PROPOSAL FOR CYBERTHREAT INFORMATION SHARING BETWEEN CONTRACTORS AND THE FEDERAL GOVERNMENT. *Public Contract Law Journal*, *44*(3), 505-528.
123. Roesener, G., Bottolfson, C., & Fernandez, G. (2014). Policy for US Cybersecurity. *Air & Space Power Journal*, *28*(6), 38-54.
124. Images, real and virtual. (n.d.). Retrieved February 01, 2016, from https://www.pa.msu.edu/courses/2000fall/PHY232/lectures/lenses/images.html
125. Bradbury, D. (2014, March 19). Is Bitcoin a Digital Currency or a Virtual One? Retrieved February 01, 2016, from http://www.coindesk.com/bitcoin-digital-currency-virtual-one
126. IETF. RFC Editor Terms List. Retrieved February 01, 2016, from https://www.rfc-editor.org/materials/terms-online.txt
127. Consumer data privacy in a networked world. [electronic resource] : a framework for protecting privacy and promoting innovation in the global digital economy. (2012). Washington [D.C.] : The White House, [2012].
128. cybernetics. Retrieved March 3, 2016, fromhttps://en.wiktionary.org/wiki/cybernetics
129. Gadya FS., Austin G. “Russia, The United States, And Cyber Diplomacy Opening the Doors”. The EastWest Institute. 2010
130. Zuppo, Colrain M. "Defining ICT in a Boundaryless World: The Development of a Working Hierarchy"
131. von Solms R, van Niekerk J, “From Information Security to Cyber Security”, Computers & Security (2013), doi: 10.1016/j.cose.2013.04.004.
132. R. Ramirez, N. Choucri, “Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review,” IEEE Access, Volume 4, 2016
133. Latent Dirichlet Allocation (LDA) and Google’s Rankings are Remarkably Well Correlated. (n.d.). Retrieved May 16, 2017, from https://moz.com/blog/lda-and-googles-rankings-well-correlated
134. Cyber Definitions. (2014, May 26). Retrieved May 16, 2017, from https://www.ccdcoe.org/cyber-definitions

135. Glossary of Cybersecurity Terms. (n.d.). Retrieved May 16, 2017, from https://scottschober.com/glossary-of-cybersecurity-terms/
136. SANS - Information Security Resources. (n.d.). Retrieved May 16, 2017, from https://www.sans.org/security-resources/glossary-of-terms/
137. Global Cyber Definitions Database. (n.d.). Retrieved May 16, 2017, from http://cyberdefinitions.newamerica.org/
138. Sophos Threatsaurus: The A-Z of computer and data security threats - sophosthreatsaurusaz.pdf. (n.d.). Retrieved from https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=en
139. https://www.eecs.mit.edu/academics-admissions/undergraduate-programs/6-p-meng-program
140. https://www.eecs.mit.edu/docs/ug/Checklist.pdf
141. http://catalog.mit.edu/mit/undergraduate-education/academic-programs/minors/
142. https://www.eecs.mit.edu/academics-admissions/undergraduate-programs
143. http://cacm.acm.org/magazines/2013/10/168170-trends-in-computer-science-research/fulltext
144. http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf
145. http://www.scmagazine.com/ponemon-research-shows-executives-arent-well-informed-on-risk/article/399445/
146. http://www.cs.rpi.edu/research/pdf/12-03.pdf
147. (Minors consist of five to seven subjects, with a typical program comprising six, and can include non-MIT subjects) http://web.mit.edu/catalog/subjects.html.
148. http://www.matr.net/print-17415.html
149. http://news.mit.edu/2015/mit-new-cybersecurity-initiatives-0313
150. https://www.ll.mit.edu/mission/cybersec/cybersec.html
151. https://iti.illinois.edu/news/illinois-lead-new-281m-consortium-cyber-resilient-energy-delivery-systems
152. https://www.nsa.gov/ia/academic_outreach/nat_cae/
153. http://ic3.mit.edu/newsletters/2015-10-ic3-newsletter-4.pdf
154. http://www.heinz.cmu.edu/school-of-information-systems-and-management/information-security-policy-management-msispm/curriculum/index.aspx
155. http://www.umbc.edu/cyber/schedule.php
156. http://ia.asu.edu/education.php
157. http://www.forbes.com/sites/josephsteinberg/2014/12/11/massive-security-breach-at-sony-heres-what-you-need-to-know/
158. http://www.huffingtonpost.com/kyle-mccarthy/32-data-breaches-larger-t_b_6427010.html

159. http://www.npr.org/sections/thetwo-way/2015/03/19/394039055/target-offers-10-million-settlement-in-data-breach-lawsuit
160. http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/
161. http://www.cnet.com/news/tjx-says-45-7-million-customer-records-were-compromised/
162. http://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm
163. http://www.wsj.com/articles/airline-trade-group-warns-about-cybersecurity-threats-1436444810
164. http://www.nist.gov/cps/cybersec_smartcities.cfm
165. https://hbr.org/2015/07/why-cybersecurity-is-so-difficult-to-get-right
166. http://web.mit.edu/registrar/reg/majors-minors/minor_guidelines.html
167. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7437356
168. https://edu-apps.mit.edu/ose-rpt/?Search+Online+Reports=Search+Subject+Evaluation+Reports
169. https://www.rsaconference.com/events/us16/agenda/sessions/2742/louder-than-words
170. http://catalog.mit.edu/interdisciplinary/undergraduate-programs/minors/energy-studies/
171. http://web.mit.edu/registrar/stats/yrpts/
172. https://thetech.com/2016/04/08/newminor-v136-n11
173. https://www.sym.bio/it-security-for-smbs-and-the-rising-risk-of-cyber-threats/
174. https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon
175. http://www.cybersecuritytrend.com/topics/cyber-security/articles/421821-human-error-to-blame-most-breaches.htm
176. http://student.mit.edu/catalog/index.cgi
177. https://blog.kaspersky.com/kaspersky-statement-duqu-attack/8997/