NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN INNOVATION FRAMEWORK APPLIED TO A MILITARY CYBER PROFESSIONALS ASSOCIATION

by

Joseph L. Billingsley

September 2013

Thesis Advisor:	Peter Denning
Second Reader:	Susan Higgins
Third Reader:	John Davis

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
AN INNOVATION FRAMEWORK APPLIED TO AMILITARY CYBER PROFESSIONALS ASSOCIATION

5. FUNDING NUMBERS

6. AUTHOR(S) Joseph L. Billingsley

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Be it on Wall Street, Main Street, or K Street, Americans are concerned about cyber threats, as cyberspace underpins national security and prosperity in the 21st century. The concern is expressed in dinner table discussions, governmental strategy documents, and blogs, alike. A commonly held assertion is that current practices toward securing cyberspace are insufficient, necessitating innovative new approaches. In response to calls for such innovation by the Department of Defense, this work proposes a new organization designed specifically to address enduring national security priorities concerning cyberspace.

In order to bring about such an organization and put it on a firm enough a foundation to ensure sustaining endurance, a generative framework of innovation, the Innovator's Way (IW), was applied. This endeavor meets the IW criteria of innovation, which is defined as the adoption of new practices within a community. In this case, the practice is a new professionals association and the community is the American military cyber workforce (a subset of the greater American defense community).

This work is a culmination of a yearlong effort to employ and evaluate the IW framework, which emphasizes the role of adoption in the innovation process. The weight applied to adoption in this framework should resonate with those passionate about "making things happen" and helps to answer the "so what?" question commonly applied to good ideas. This case study serves as an evaluation of this generalizable framework, from which an enduring engine of national cyber development has been bequeathed.

14. SUBJECT TERMS Cyber, Cyberspace, Cybersecurity, Cyberwar, Cyber conflict, Cyber Policy, Joint, Interdisciplinary, Military Cyber Profession, Professions, Professional Associations, Military Cyber Professionals Association, Cyber Command, Innovation, Innovation Adoption, Innovation Model, Non Profit, Entrepreneur, Intrapreneur, Extrapreneur, Collective Intelligence, Social Networks.	**15. NUMBER OF PAGES** 125
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN INNOVATION FRAMEWORK APPLIED TO A MILITARY CYBER PROFESSIONALS ASSOCIATION

Joseph L. Billingsley
Captain, United States Army
B.A., University of Connecticut, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author: Joseph L. Billingsley

Approved by: Peter Denning, PhD
Thesis Advisor

Susan Higgins, CDR (Ret.)
Second Reader

John Davis, MG
Third Reader

Cynthia Irvine, PhD
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Be it on Wall Street, Main Street, or K Street, Americans are concerned about cyber threats, as cyberspace underpins national security and prosperity in the 21st century. The concern is expressed in dinner table discussions, governmental strategy documents, and blogs, alike. A commonly held assertion is that current practices toward securing cyberspace are insufficient, necessitating innovative new approaches. In response to calls for such innovation by the Department of Defense, this work proposes a new organization designed specifically to address enduring national security priorities concerning cyberspace.

In order to bring about such an organization and put it on a firm enough a foundation to ensure sustaining endurance, a generative framework of innovation, the Innovator's Way (IW), was applied. This endeavor meets the IW criteria of innovation, which is defined as the adoption of new practices within a community. In this case, the practice is a new professionals association and the community is the American military cyber workforce (a subset of the greater American defense community).

This work is a culmination of a yearlong effort to employ and evaluate the IW framework, which emphasizes the role of adoption in the innovation process. The weight applied to adoption in this framework should resonate with those passionate about "making things happen" and helps to answer the "so what?" question commonly applied to good ideas. This case study serves as an evaluation of this generalizable framework, from which an enduring engine of national cyber development has been bequeathed.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

1AD	1st Armored Division
ARCYBER	Army Cyber Command
AOC	Association of Old Crows
C2	Command and Control
CCW	Center for Cyber Warfare
CIA	Central Intelligence Agency
CNO	Computer Network Operations
CSUMB	California State University – Monterey Bay
USCYBERCOM	United States Cyber Command
DIA	Defense Intelligence Agency
DiD	Defense in Depth
DHS	Department of Homeland Security
DoD	United States Department of Defense
DoE	Department of Energy
EW	Electronic Warfare
GAB	Google Apps for Business
GAO	Government Accountability Office
HUMINT	Human Source Intelligence
IC	Intelligence Community
IIED	Institute for Innovation and Economic Development
IO	Information Operations
IW	Innovator's Way
LTC	Lieutenant Colonel
MCP	Military Cyber Profession
MCPA	Military Cyber Professionals Association
MG	Major General
MI	Military Intelligence
NCR	National Capital Region
NGE	Non-governmental entity
NPS	Naval Postgraduate School

NSA	National Security Agency
OSI	Open Systems Interconnection
PAO	Public Affairs Officer
PII	Personally Identifiable Information
POLP	Principal of Least Privilege
PSYOPS	Psychological Operations
SIGINT	Signals Intelligence
USG	United States Government
USN	United States Navy
WWI	World War One

ACKNOWLEDGMENTS

Thanks to all of the supportive professionals who have directly contributed to my efforts in the betterment of our nation. Special thanks for the guidance and support from my thesis committee, Dr. Peter Denning and Sue Higgins from the Cebrowski Institute, and Major General John Davis, senior military advisor for cyber in the Office of the Secretary of Defense for Policy.

Other supporting friends affiliated with the Naval Postgraduate School include Cynthia Irvine, Duane Davis, Owen Schoolsky, John Arquilla, Nancy Roberts, Dorothy Denning, Dan Boger, Alex Bordetsky, Erik Janssen, Lonnie Wilson, John Krautheim, Ed Rockower, David Steinberg, Kristen Wheeler, John McEachen, Wayne Porter, and Admiral Andy Singer. My classmates deserve recognition for their continuous support and true friendship: Ehab Maklouf, Christopher Callahan, Christopher Mullen, Scott Roper, Aaron Littlejohn, Hillary Lamb, Daniel Flemming, Robert Storer, Lorenza Mosley, Brent Molaski, and John Hoffner.

Those from the national capital region deserving special thanks for inspiration and support include General Keith Alexander, General Rhett Hernandez, Emma Coulson, Shana Beach, and Lisa Wiswell. Those from Silicon Valley and beyond include Celena Aponte of Cisco, Jaim Harlow of NetFuel, Chris Cleary of Vir-Sec, Larry Reeves of AFCEA, and Wayne Shaw of the Old Crows.

Thanks to my parents for encouraging a campaign of lifelong learning. At home, Anna provides indispensable inspiration and support. Before delving into this study, I had the good sense to discuss the endeavor with her. Despite being more consuming than other potential thesis topics, she imbued me with the confidence to reach farther, work harder, and make a real difference.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Whether on Wall Street, Main Street, or K Street, Americans are concerned about cyber threats as observed at dinner table discussions, governmental strategy documents, the nightly news, and throughout the blogosphere. What was largely confined to the realm of those interested in technology, information protection, and privacy has come to the forefront of military though. Through all its services, the Department of Defense (DoD) is searching for innovative approaches to implement the initiatives codified in the 2011 Strategy to Secure Cyberspace. In response to DoD calls for such innovation, the author of this work founded a new organization to support the DoD long-term efforts.

The new organization, known as the Military Cyber Professionals Association (MCPA), was designed to support the DoD's cyber professionals, including developing skills that make them more innovative as a profession. The model of innovation generation described in the book, *The Innovator's Way,* (IW) was selected as the framework for the skill sets required to establish the organization.[1] The model proved effective in taking this innovation from a concept to putting the organization on sound footing within a year.

Learning how to apply the IW model to this situation became the research project at the center of this thesis. The specific research questions addressed in this work are:

- How effective is the general IW framework for producing a specific innovation? Can it be done within numerous constraints, including a time limit of a year?
- The MCPA is a socio-technical innovation. How well does the IW model work for a socio-technical innovation compared to a pure technology innovation?

[1] Peter J. Denning and Robert Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010).

- Can the IW model, promulgated through MCPA, help the DoD with other innovations it requires in cyber and beyond?

This research was a case study in the application of a model to a real world concern. The conclusion at the end of the research was that the model is highly effective for a specific innovation, it works for socio-technical innovations, and it generalizes for other DoD innovation projects.

A. A PROBLEM

1. Strategic Direction

The American military cyber profession is in need of development, as identified in numerous official documents and statements by senior leaders within and outside DoD. Excerpts of some directly supporting statements include:

- The development and retention of an exceptional cyber workforce is central to DoD's strategic success in cyberspace and each of the strategic initiatives outlined in this strategy. The development of the cyber workforce is of paramount importance to DoD.[2]
- The Army continues reviewing models to recruit, educate, train, and retain cyber professionals. The Army must build a pipeline for both the next generation of cyber professionals as well as address Army cyber military and civilian personnel requirements.[3]
- The Army must also continue to develop the future cyber force. We must improve existing models.[4]
- DoD is looking at ways to fundamentally change the way it recruits, trains, educates, advances and retains both military and civilians within the cyberspace workforce. While cyber is always viewed as a technical area, the fact is it's always about people.[5]

---

[2] Pentagon, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Pentagon, 2011).

[3] Pentagon, *2012 Army Strategic Planning Guidance* (Washington, DC: Pentagon, 2012).

[4] Pentagon, *2013 Army Strategic Planning Guidance* (Washington, DC: Pentagon, 2013).

[5] John A. Davis, "Critical Cyber Needs Include People," Armed Forces Communications and Electronics Association International Cyber Symposium (25 June 2013), quoted in Cheryl Pellerin, "Critical Cyber Needs Include People, Partners General Says," Armed Forces Press Service, 2 July 2013: http://www.defense.gov/news/newsarticle.aspx?id=120402.

- Developing a robust cadre of cyber warriors is a top priority to ensure we maintain the advantage in the highly contested cyberspace domain.[6]

In a complex and dynamic environment, the most enduring piece of key terrain in cyber is the workforce, necessitating our focus on developing it.[7]

2. An Opportunity

The role of professional associations and the value they bring to their given area of focus are well documented. Through various means, they can influence, improve, manage and develop components of their profession.

More than just a set of people making their livelihood in a given area, a profession can be defined as a community of practice that forms to take care of people's enduring concerns in some area of life or work.[8] This study applies the above definition to the military cyber profession (MCP). A professional organization supports the members of a professional community with programs of professional development, ethics, education, and community outreach. This case includes promotion of innovation skills as part of professional development. Professional organizations already exist for many other major military communities, but not yet for the burgeoning MCP, which was identified as a gap and opportunity to conduct meaningful innovation research.

---

[6] *Concerning Digital Warrior: Improving Military Capabilities in the Cyber Domain*: Statement by Rhett Hernandez before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities. 112th Cong. 10 (25 July 2012).

[7] John R. Mills, "The Key Terrain of Cyber," *Georgetown Journal of International Affairs* (March 2013), http://journal.georgetown.edu/2013/03/23/the-key-terrain-of-cyber-by-john-r-mills/.

[8] Peter J. Denning and Dennis J. Frailey, *"The Profession of IT: Who Are We - Now?," Communications of the Association for Computing Machinery*, Volume 54 Issue 6, June 2011, http://mags.acm.org/communications/201106/?pg=27#pg25, p. 25–27.

A comprehensive study by David Ford and Norman Gibbs about the nature and structure of professional societies, a synonym used interchangeably with professional association in this study, was utilized for this study. Much of the functional offerings of the MCPA, current and planned, reflect the Ford-Gibbs model (see Figure 1).

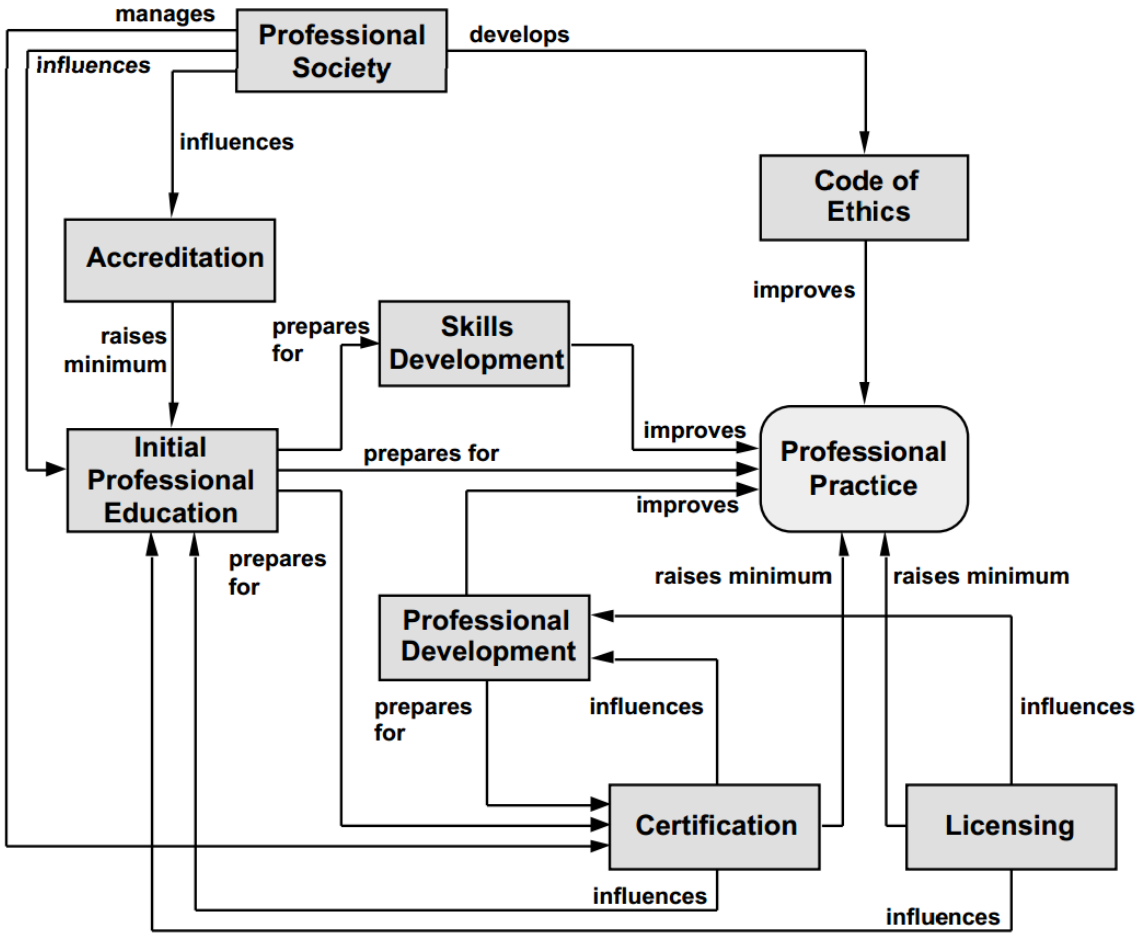

Figure 1. Interactions among components of a profession.[9]

[9] Gary Ford and Normal E. Gibbs, "A Mature Profession of Software Engineering," Software Engineering Institute, Carnegie Mellon University, Technical Report CMU/SEI-96-TR-004, 1996. http://www.sei.cmu.edu/library/abstracts/reports/96tr004.cfm, p. 7.

The widespread acceptance of the roles of such organizations is demonstrated by their pervasiveness, including across the American defense ecosystem. Examples of such military related professional associations include:

- U.S. Army Signal Corps Regimental Association (signalcorps.org)
- Naval Intelligence Professionals (navintpro.org)
- U.S. Military Strategists Association (militarystrategists.org)
- Air Force C4 Association (afc4.org)

At the outset of this study in late 2012, a review of existing military focused professional associations with an interest in the American MCP identified that none specified this relatively new profession as their primary focus, identifying a gap and opportunity. The published mission statements of two such interested organizations are noted here:

- AFCEA is an international organization that serves its members by providing a forum for the ethical exchange of information. AFCEA is dedicated to increasing knowledge through the exploration of issues relevant to its members in information technology, communications, and electronics for the defense, homeland security and intelligence communities.[10]
- To advance strategy, policy and programs for EW/IO (electronic warfare / information operations), and electromagnetic spectrum operations.[11]

Of the nonprofit nongovernmental entities (NGE) with a stated focus on developing cyber, none purported to be professional associations, providing an opportunity to establish an association dedicated to developing the American MCP. Examples of cyber focused NGEs include:

- Cyber Conflict Studies Association (cyberconflict.org)
- Cyber Security Forum Initiative (csfi.us)
- Journal of Law and Cyber Warfare (jlcw.org)

---

[10] Armed Forces Communications and Electronics Association, "Mission Statement," (n.d.), http://www.afcea.org/mvc.asp.

[11] Association of Old Crows, "Mission Statement," (n.d.), http://www.crows.org/about/mission-a-history.html.

Numerous descriptions of the MCP are available, each naturally influenced by parties with competing theoretical and/or budgetary priorities. This study was conducted within such an environment, and under the assumption that the personnel structure will evolve as threats and missions do.[12] Operating within the aforementioned assumptions, for practical reasons of this study an approximate number of the population still had to be established, which begins with identifying boundaries. Congress's 2009 definition is utilized, which reads,

> the term ''cyber operations personnel'' refers to members of the Armed Forces and civilian employees of the Department of Defense involved with the operations and maintenance of a computer network connected to the global information grid, as well as offensive, defensive, and exploitation functions of such a network.[13]

Using the above definition as guidance, a 2011 DoD report identifies specific cyber operations related career professions, which this study uses to determine the approximate size and composition of the target population. Although the profession includes non-uniformed personnel, the published list of uniformed personnel is found as an appendix of this document for the reader's orientation. A further mapping of the profession is included in the body of this work. The lack of a professional association focused on developing cyber in the DoD was found to be a gap and an opportunity for a strategically meaningful study.

---

[12] Department of Defense, "Cyber Operations Personnel Report," (n.d.), http://www.nsci-va.org/CyberReferenceLib/2011–04-Cyber%20Ops%20Personnel.pdf, under "Composition of the DoD Cyber Operations Workforce."

[13] *National Defense Authorization Act for Fiscal Year 2010*, Public Law 111–84,*Study on the Recruitment, Retention, and Career Progression of Uniformed and Civilian Military Cyber Operations Personnel* (2009); Section 934-c, http://www.intelligence.senate.gov/pdfs/military_act_2009.pdf.

B. INNOVATION FRAMEWORK

After a review of innovation frameworks to guide the design and formation of the organization, the IW framework was selected because of its focus on concrete actions that generate innovations. With innovators as its target audience, the IW framework focuses on practices and has been useful for guiding innovators with successful technology transfer. The outcome of a successful transfer is *the adoption of new practice in a community*. The IW framework specifies eight practices to be used by the innovator in producing this outcome. Each practice contributes an essential element to the innovation outcome.

Each practice is a skill set that produces its element and guides the innovation in coping with *breakdowns* that arise when doing the practice. A breakdown is any event that blocks the path to the desired outcome. Innovators constantly encounter breakdowns, such as the inability to see a possible solution for a problem or unexpected resistance by a faction of the intended community. Gracefully coping with breakdowns is part of the innovator's skill set. A summary of the eight IW practices and associated breakdowns is provided below (see Table 1).

Structure	Practice	Anatomy	Characteristic breakdowns
The main work of invention	Sensing	Sense and articulate opportunities and their value. Locate possibilities through networks, checklists, or disharmonies.	Inattention. Blindness. Inability to notice or articulate sensations, hold the thought, or see opportunities in disharmonies.
	Envisioning	Weave vivid, concrete, compelling stories about the new worlds embodying possibilities; and means to get there.	Complex, abstract, emotionless, unreal, non-credible stories; inability to design plans of action.
The main work of adoption	Offering	Draw listeners into a discussion about ways to produce the new outcomes. Modify proposals to fit listener concerns. Establish trust in one's expertise to fulfill the offer.	Little awareness and respect for customers. Inability to listen, connect, enroll, articulate value, or see people as fundamental in the process. Unwilling to respond to feedback.
	Adopting	Achieve initial commitment to the new practice. Demonstrate value. Show how to manage risks and contain resistance. Align action plans for coherence with existing practices, concerns, interests, and community adoption rates. Recruit allies. Develop marketing strategist for different groups. Overcome resistance.	Force adoption through compulsion. Failure to anticipate opposition and differing adoption rates of different community segments. Failure to articulate the value from adoption. Lack of enabling tools and processes for adoption.
	Sustaining	Achieve commitment to stick with new practice. Develop supporting infrastructure. Integrate new practice with surrounding environment, standards, and incentives. Assess for negative consequences. Abandon bad or obsolete innovations.	Failure to plan for support and training, to change enabling tools and systems, to align incentives with the new practices, to align political support, or to integrate with other practices and standards.
The environment for the other practices	Executing	Create an environment for effect action in the other practices. Build teams and organizations. Manage commitments, resources, and capacity for reliable delivery.	Failure to manage commitments, satisfy customers, deliver on time, or build trust.
	Leading	Create an environment for recruiting followers and articulating guiding principles in the other practices. Declare new possibilities in ways that people commit to them. Move with care, courage, value, power, focus, sense of larger purpose (destiny), fluency of speech acts.	Inability to listen for concerns, offer value, work with power structures, maintain focus, operate from a larger purpose, or perform speech acts skillfully.
	Embodying	Create somatic awareness, accounting for emotion and body in the other practices, and develop the skill of blending with concerns, energies, and styles of others. Nonverbal communication. Emotional intelligence. Ascend ladder of competence. Connect. Produce trust. Develop open and inviting "presence."	Inability to read and respond to body language, gesture, etc. Inability to connect and blend. Failure to recognize and overcome one's own tendencies, to appreciate differing levels of skill and their criteria, or to practice regularly in the other practice areas.

Table 1. Eight practices summary chart.[14]

[14] Peter J. Denning and Robert Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010), 381–383.

A distinction of the IW model is its emphasis on adoption, resulting from it belonging to the adoption school of thought about innovation, as opposed to that of ideation.[15] Of the eight practices of the IW model, only the first and second are the invention process, the third, fourth, and fifth the adoption practices, and the sixth, seventh, and eighth the environmental practices (see Figure 2).

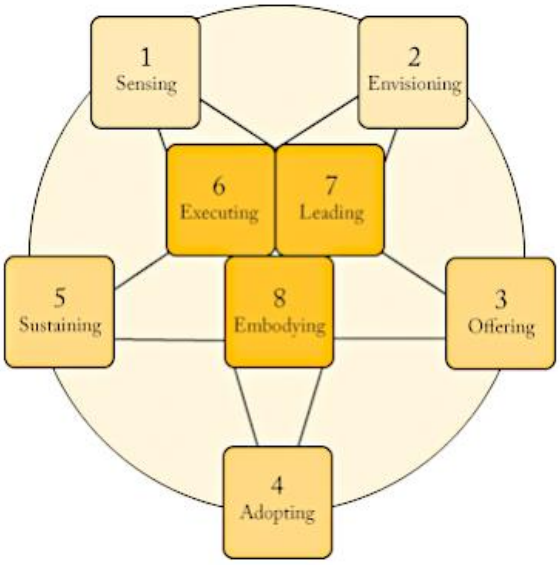

Figure 2. The essential practices of successful innovation.[16]

The IW framework makes it clear that success lies in the intersection of the innovator's domain expertise, social interaction skills, and ability to recognize and move into realizable possibilities. In this case, the author-innovator met such prerequisites. As an Army cyber scholar, the author possessed sufficient domain expertise and social skills. Similarly, the proposed association has been well recognized as a fruitful form of social interaction. The proposed organization responds to the opportunity to develop more cyber related innovation expertise among the cyber workforce. The success interaction is depicted below (see Figure 3).

---

[15] Peter Denning, "Quick Guide to Innovation," Cebrowski Institute, 2013, https://dl.dropboxusercontent.com/u/1893401/Innov-Overv-Sep13.pptx.

[16] Peter Denning and Robert Dunham, "Image," *The Innovator's Way*, 2010, http://innovators-way.com/practices/.

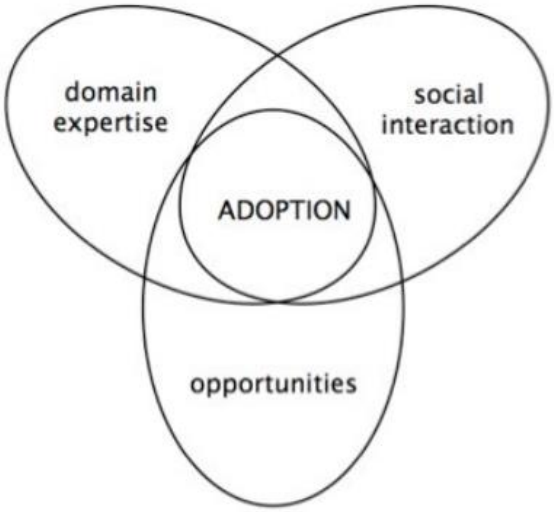

Figure 3. Success intersection.[17]

The structure of this case study is guided by the IW framework. Although many of the IW practices are actually executed in parallel, this study presents them sequentially as a means of structuring the discussion. Figure 4 is provided to visualize the parallel nature of the effort and to confirm that the author found all eight practices necessary to achieve the goal.

[17] Peter Denning and Robert Dunham, "Success interactions," *The Innovator's Way* (2010): 23, quoted in *Scott Avery Voigts: Organizational Use of a Framework for Innovation Adoption* (Monterey, CA: Naval Postgraduate School, 2011), 4.

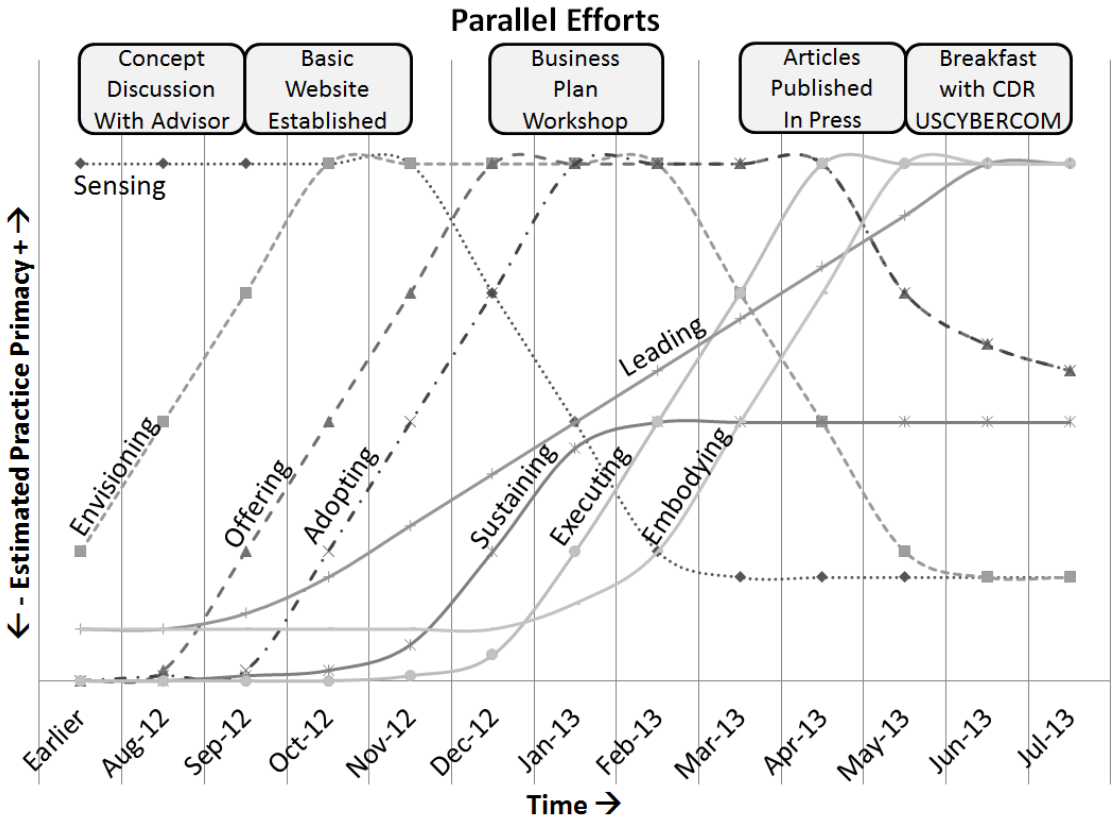

Figure 4. Author's estimate of practice primacy over time.

C. THESIS PLAN

1. Research Questions

This thesis addresses the following three research questions while seeking to produce the innovation outcome of establishing the MCPA.

a. Model Validity

Based upon past calls to validate the model within the defense community, how effective is the IW innovation model for producing a specific innovation?[18] Can it be done within a year?

[18] Scott A. Voigts, "Organizational Use of a Framework for Innovation Adoption" (master's thesis, Naval Postgraduate School, 2011).

b. Socio-technical Innovation

How well does the IW framework work for a socio-technical innovation, such as the MCPA, compared to a pure technology innovation?

c. Generalizability

Can the IW model, promulgated through MCPA, help the DoD with other innovations it requires in the development of cyber and beyond?

2. Research Objective

The primary research objective was to answer each research question with a case study of the IW framework used to start a new organization well suited to contribute to developing a strong cyber workforce for DoD. By recording this demonstration of model validity, this case study contributes to general knowledge about innovation and cyber in the DoD.

3. Summary of Findings

a. Model Validity

The generative framework for innovation presented by Denning and Dunham was found to be well fit and valid in this innovation case. Due to the substantial risks that would have otherwise resulted from ignorance or skipping of an IW practice, each of the eight IW practices was found to be necessary over the course of this successful process of innovation. As delivered by the model, great value was garnered by the recognition and avoidance of common breakdowns, specific examples of which are discussed in the body of the study. The process was completed within numerous constraints, including a time limit of a year. Completing the process within that time without the guidance of the model was assessed to be doubtful and risky, especially considering the essential nature and characteristic breakdowns of each practice.

b. Socio-technical Innovation

This innovation is socio-technical. In part a social organization, this innovation heavily leverages technology assets and in assembled of people with a generally strong interest in technology. Grounded in and validated for pure technology innovation, the IW model had not yet been validated for the formation of such a social organization, especially within a restricted deadline. This study validates the model with the successful design and establishment of a robust young organization within a year.

The author has assesses that more time and effort is demanded of the invention process, also called the sensing and envisioning practices, in such a social innovation, as opposed to a purely technical innovation. Such a finding is due to the complexity and chaos inherent of social systems, and social systems were largely the components of this innovation. Based upon meticulous notes by the author-participant, a detailed account of the process is provided in this study.

Within only a few months since beginning to accept members, the organization produced by the framework has demonstrated success by delivering benefits to the intended recipients. Anecdotal evidence supporting the delivery of benefits is found in the body of the study. Scoping and expectation management was found to be critical in this process of social-technical innovation as numerous tasks met delays and resources finite. This young organization is an incremental step that enables and encourages further work toward a mature professional organization.

c. Generalizability

The most notable evidence of generalizability resulting from this study is the successful use of the model for a socio-technical innovation when the model has previously been closely associated with innovations of technology transfer. Because of its coherent guidance on all the aspects of making an innovation work, the IW model has been assessed as generalizable and is expected to be helpful to other DoD innovators interested in cyber or other areas.

Of particular interest to inspiring future innovation is a strand of innovation professional development that has been weaved into the MCPA. The IW model has been encouraged in the hopes of growing more effective innovation expertise throughout the DoD in the future.

Recent interest by aspiring military innovators seeking to develop their own communities has demonstrated the generalizability of this model within the DoD. Such hopeful military innovators may find the extrapreneur approach (discussed below) an effective complement to the IW framework. Further, the approach may prove useful to other aspiring innovators within the government or any large organization where internal resistance poses a risk to successful innovation.

d. Benefits to the DoD and Organizational Summary

Appendix B lists benefits of this study to stakeholders like the DoD, followed by a summary of the MCPA at the conclusion of this study.

4. Method

a. Case Study

The case study observer-participant method is used due to its flexibility in incorporating insights derived from various sources, including subtle social and cultural nuances. Such an approach lends itself to making the best use of the rich data recorded from the participant-observer in answering this set of research questions. Unless otherwise cited, the origin of material documented in this paper is a result of first hand observations made by the author.

Given approximately one year from thesis proposal to submittal of the final draft, no sponsor funding, and no thesis co-authors, the author of this study restricted himself to complete a case study in which he was an extrapreneur using the IW framework. This study examines the case of the design, establishment, and implementation of a MCPA using the IW principles of innovation. This narrative records observations and insights of interest to

innovators, entrepreneurs, intrapreneurs, extrapreneurs, policy makers, and military cyber professionals.

The author of this work may use *Cyber* and *cyber* interchangeably, and no difference in meaning should be assumed by the case difference. Similarly, the author's preference in connecting or disconnecting the preface *cyber-* from words such as *security* are just that, a preference, and the choice does not hold some special meaning or significance. Other authors may argue that point, but this one does not. Unless otherwise stated, this discussion is scoped to the United States of America (USA). The American situation both suffers from and enjoys unique cultures, laws, capabilities, and perspective.

b. Extrapreneurism

An extrapreneurial approach was used to simultaneously work inside and outside of the federal government. Generally defined, an extrapreneur is a member of a large organization who goes outside (extra-) the large organization that they are loyal to in order to affect change/innovate within, complement, or enhance that large organization.

An extrapreneur stands in contrast to an intrapreneur in that an intrapreneur remains within (intra-) the large organization while they innovate. An intrapreneur is essentially an entrepreneur working on the inside. A wide range of interpretations of the terms can be found, some of which equate extrapreneurs with subcontractors, disgruntled former employees, or agents of societal change. Some instances even appear to connote the prefix *extra-* with *more* (as in intrapreneurs with *extra* skills), as opposed to *outside*.[19] The author of this study finds the latter meaning (outside) more appropriate for this case.

In this case, the extrapreneur is a full time government employee that established a non-governmental entity in order to affect governmental change. Such a context is coupled with certain environmental characteristics that

[19] Jill Hender, *Innovation Leadership: Roles and Key Imperatives* (London: Grist Ltd, 2003), 18.

may differ from other sectors, such as the role of profit. The author has developed Table 2 to clarify the main differences in approach in leading innovation in the context of the USG.

Innovation Approach	For Profit	Operates Inside Org	Operates Outside Org	Mutual Trust and Loyalty Required	Perceived Resistance
Entrepreneur	Yes	No	Yes	Normal	Normal
Intrapreneur	No	Yes	No	Normal	Low
Extrapreneur	No	Yes	Yes	High	High

Table 2. Author's comparison between contextualized approaches.

Depending on the policies of the larger organization and the position of influence of the extrapreneur, such activities may be prohibited, require written approval, discouraged, or encouraged. In this case, such an approach was widely regarded as highly uncommon, yet still possible and was supported by key decision makers. The extrapreneur received written approval for outside employment in accordance with the DoD's Joint Ethics Regulations and other organizational requirements.[20] The request for approval included clarification that the association is not for profit, the founder (extrapreneur, author, observer, and participant) is not receiving any additional compensation (working for free), time allocation plan, and duty description to guard against potential conflicts of interests. Some other relatively recent demonstrations of extrapreneurism by members of the American defense community include:

- CompanyCommand.com (now companycommand.army.mil)
- MilitaryCAC.org
- SteinbeckInnovation.org

[20] Secretary of Defense. *Joint Ethics Regulation.* Washington, DC: 2011. http://www.dtic.mil/whs/directives/corres/pdf/550007r.pdf.

II. SENSING

This chapter of the work begins the case study. Sensing, the first practice of the IW framework, is discussed here. Although the practice of sensing began well before this study, the past observations of the author are integrated and applied in the context of the IW framework.

The practice of sensing can be described as listening and observing for disharmonies and asking what is possible if the disharmony could be resolved.[21] In this case, the observable disharmony was the lack of a military cyber professionals association, alongside the plethora of professional associations catering to professions within the U.S. military, each of which provides services that have come to be expected within the American military culture. Classic services rendered by such organizations include events, awards, and a journal.

A. THE CYBER BALL

For the author, the conceptual seed of a new cyber organization was planted in the winter of 2010–2011, during the 2011 European Cyber Ball. Such events are one of the services that have come to be expected by many subsets of the American military community. Such events promote both social and professional development within the community, and typically include presentation of association awards, entertainment, guest speakers, dinner, and dancing.

Each year, the community of U.S. Army Signal Corps members in Europe plans and executes a ball that is sponsored by the Signal Corps Regimental Association. Inspired by the then recent establishment of U.S. Army Cyber Command, planning for the annual *Signal* Ball was modified to planning for the first *Cyber* Ball. At the time of this event's planning, popular understanding of

[21] Peter J. Denning and Roberts Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010), 111.

cyber in the Army circles roughly translated to a synthesis of elements of the Signal and Military Intelligence branches of the U.S. Army.

This shift from a Signal to Cyber event was represented in the event logo. During the previous events, the logo had featured the patch of the most senior Signal organization in Europe (the 5th Signal Command) embellished with wig wags (signal flags), which are an enduring symbol of the military communications profession.[22] The logo for the Cyber Ball removed one of the flags and replaced it with the key, which represents the security and intelligence community in military heraldry.[23] The 2010 and 2011 event logos are provided in Figures 5 and 6.

[22] U.S. Army Signal Center of Excellence, "*Signal Corps Regimental History*," (n.d.), http://signal.army.mil/history/00_wig_wag.html, under "*The Wig Wag*."

[23] The Institute of Heraldry, "*101 Military Intelligence Battalion*," (n.d.), http://www.tioh.hqda.pentagon.mil/Heraldry/ArmyDUISSICOA/ArmyHeraldryUnit.aspx?u=3832, under "*Symbolism*."

Figure 5. Event logo of the 2010 European Signal Regimental ball.

Figure 6. Event logo of the 2011 European Cyber ball.

In addition to modifying the event logo used to adorn advertising material and commemorative items, invitation was extended to the U.S. Army Military

Intelligence community in Europe. At the time of this study, a video invitation can be accessed on YouTube that starts with an invitation to the Signal and MI communities.[24] The guest speaker of the 2011 Cyber Ball was the commander of ARCYBER, LTG Rhett Hernandez, and Signal Week events were executed under the banner of Cyber Week. The modifications made to the Signal event covered above did not seem enough to garner notable participation from the MI community, who by and large, still perceived this ball as a Signal event.

The growing body of literature developing cyberspace as a domain of warfare (or conflict and other activities), appeared to reinforce the concept that those who are chartered to provide cyberspace as a service (the Signal or greater communication community) to warfighters may not be the best armed to lead the development of cyberspace as a domain of warfare. The experience of the Cyber Ball, reinforced by service in Signal, MI, SIGINT, and Joint environments, drove the author to the conclusion that there should be a new association supporting the cyber area.

As described above, those prescribing to Kuhnian thought may interpret the 2011 Cyber Ball as the first physical manifestation of inconsistencies of the existing paradigm, as observed by the author of this study.[25] Such paradigms will be discussed later in this chapter.

B. AVOIDING BLINDNESS

The IW framework cites characteristic breakdowns during the practice of sensing to include inattention and blindness. Denning and Dunham offer practices for coping with such setbacks during this phase of innovation (see Table 3).

[24] 5th Signal Command, “European Cyber Ball commercial,” http://www.youtube.com/watch?v=qOhY-gea0ow, 2011.

[25] Kuhn, Thomas S., “The Structure of Scientific Revolutions,” Second Edition Volume II Number 2, Chicago, 1970, page 76.

Type of Not-Seeing	Strategies	Practices
Inattention	(1) Switch attention within one's own frame set. (2) Enlarge awareness.	Journaling Daily meditations Use of checklists
Cognitive blindness	(1) Learn a new frame from someone else. (2) Create a new frame.	Above, plus: Speculation Learning
Community blindness	Create a new frame.	Network following Mind mapping Domain mapping Question the paradigm Get a coach Diverse team of advisors

Table 3. Practices for coping with inattention and blindness.[26]

The author of this study practiced a number of the breakdown mitigation practices displayed above in a deliberate effort to avoid cognitive and community blindness. Some examples of the author's practices in support of sensing directly applicable to this case are listed below. The author of this work sought enlargement of awareness and learned new frames by:

- Attending an officer advanced course (MI) outside of the author's basic branch (Signal), followed up with a specialization course in SIGINT/EW
- Voluntarily served on a U.S. Navy ship during an exercise
- Enrolled in naval programs of study
- Completed a weeklong Information Dominance Warfare Officer (IDWO) course, which encompassed each are of the Navy Information Dominance Corps (IDC), including information operations (IO), meteorology, and space.

The author conducted a mapping of the MCP domain, during which a new frame was articulated. The mapping heightened awareness of the community, including an appreciation for its diversity and proportions. After the below graphics, a relational mapping makes up the remainder of this chapter.

[26] Peter J. Denning and Roberts Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010), 136.

Figures 7, 8, 9, 10, and 11 help to illustrate the diversity and proportions of the MCP. The codes displayed are those used by each of the military services to identify a particular specialty/occupation/ community/branch. The codes displayed on the following pages are largely limited to those listed as cyber related in a 2011 DoD source document, an excerpt of which is found in Appendix A. Although not listed in the 2011 source document and proportions not provided in this study, codes of some of today's most important elements of the MCP have been inserted into the below charts for the reader's situational awareness. Some such codes include Army IO Officers (FA30), Army Cryptologic Network Warfare Specialists (35Q), Navy Information Warfare Officers (1810), and Navy Information Professional Officers (1820).[12] The author obtained the data for these charts from the Defense Manpower Data Center.

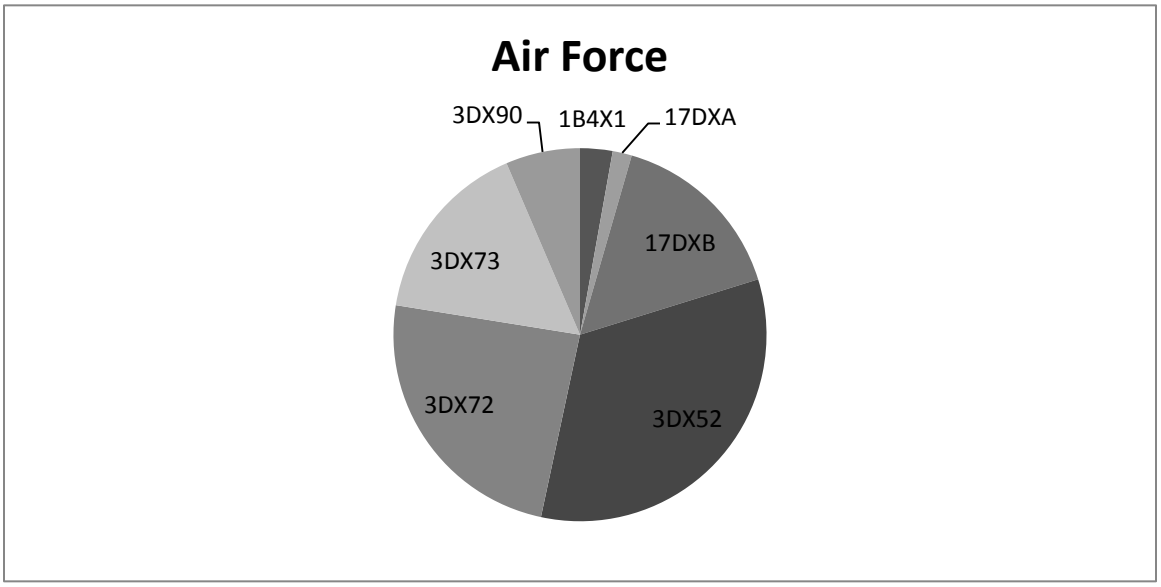

Figure 7. Distribution of authorized military cyber-related uniformed-personnel across the Air Force, including Active, Guard, and Reserve components.

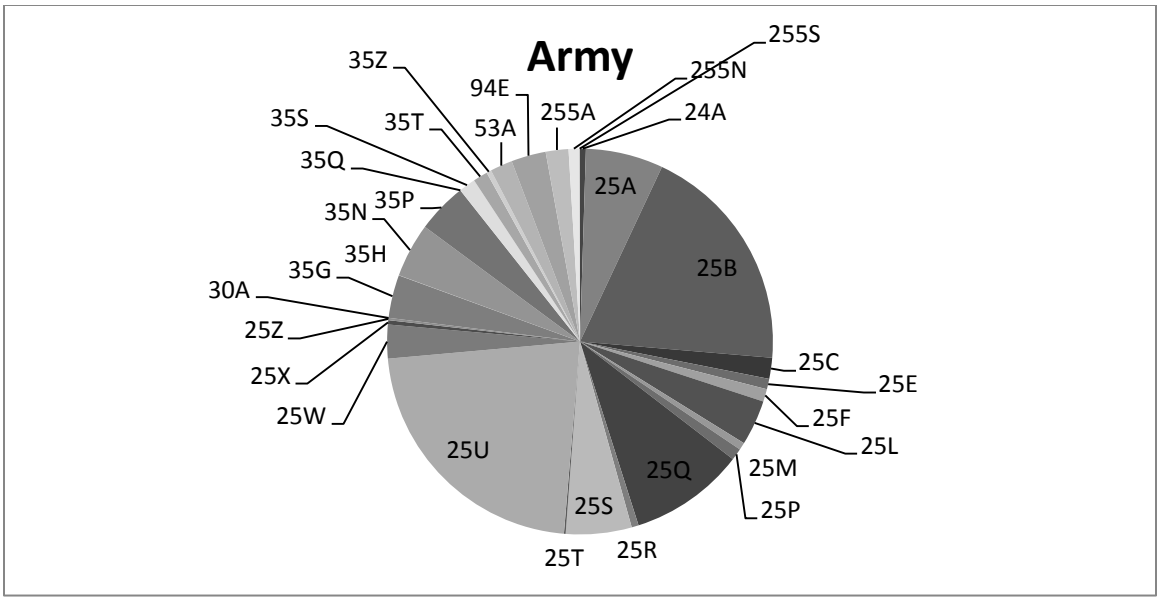

Figure 8. Distribution of authorized military cyber-related uniformed-personnel across the Army, including Active, Guard, and Reserve components.

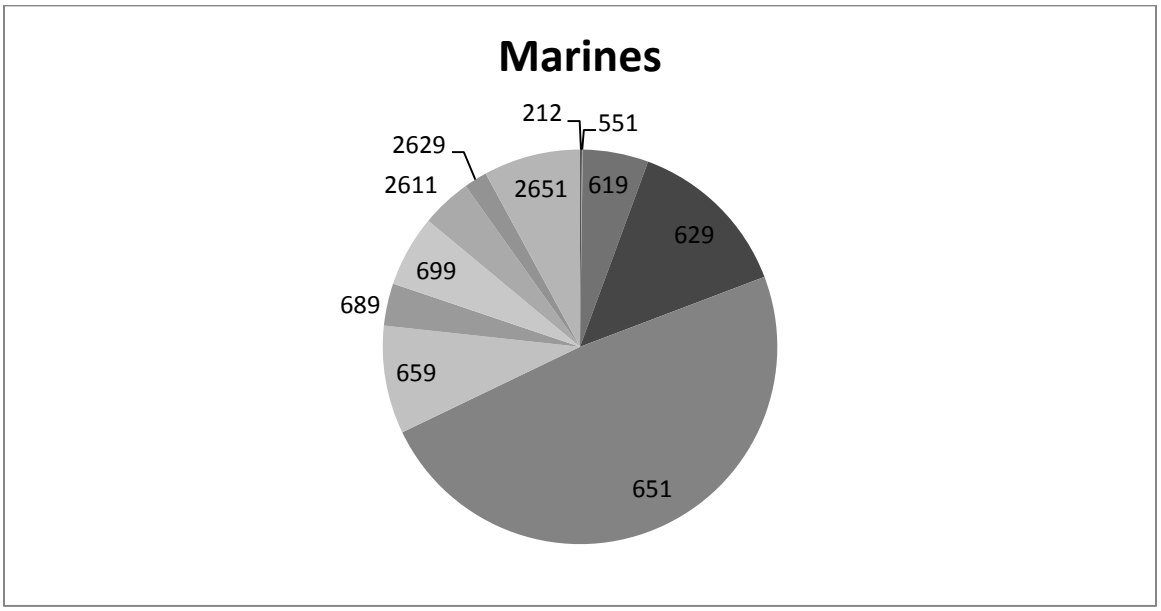

Figure 9. Distribution of authorized military cyber-related uniformed-personnel across the Marines, including Active and Reserve components.

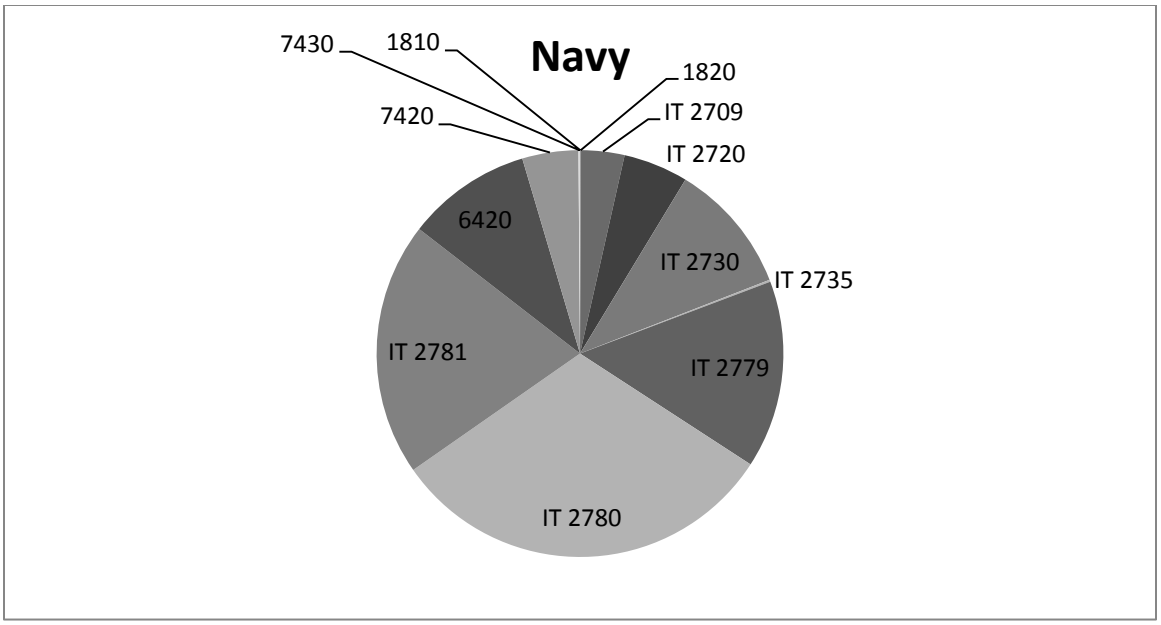

Figure 10. Distribution of authorized military cyber-related uniformed-personnel across the Navy, including Active, Guard, and Reserve components.[27]

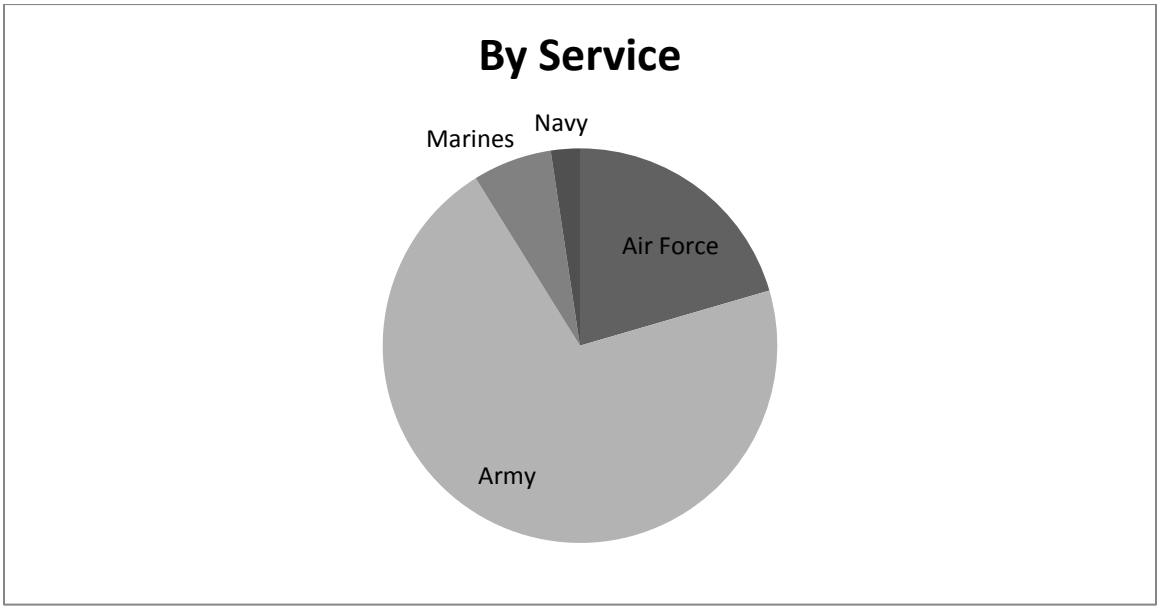

Figure 11. Distribution of authorized military cyber-related uniformed-personnel across the services, including Active, Guard, and Reserve components.

Although a critical part of the DoD cyber workforce, non-uniformed personnel and others were excluded from this mapping effort as a practical

scoping measure, and should not be interpreted as diminishing the recognized service rendered by such personnel. One expecting a comprehensive mapping that is also enduring and widely accepted is bound for disappointment due to the emergent and evolving nature of this complicated domain. The quantitative data comes from the Defense Manpower Data Center and has been displayed in a manner that does not convey hard numbers, which may have resulted in limiting the distribution of this work. After the graphics, the remainder of the chapter is devoted to a subjective qualitative mapping of the domain (see Figures 7, 8, 9, 10, and 11).

C. RELATIONAL MAPPING

As Kuhn described the collapse of one reigning paradigm in eventual favor of a successor that better explains our world and positions the community for further progress, this study finds long-held understandings associated with electronic and information warfare to be insufficient in understanding the phenomenon of cyberspace and cyber conflict in its entirety.[25] A more holistic understanding of cyber exists and is being developed at various nodes of thought around our world, but the focus of the remainder of this chapter is centered on mapping out the profession's domain for the purposes of this study only. The below mapping includes summaries of a few of the various camps in and around the MCP, their relationships, current state, conceptual framework, and applicable terminology. The subjective nature of this section is clearly stated and appropriate in this case due to the lack of available documentation explaining the nuances and emerging relationships of each of the discussed elements.

It is the perspective of the author that much of the work in developing the paradigm that some in military circles may describe as a cyberist world view has yet to be done, explaining the use of various tenses to include the future. In this discussion, a cyberist perspective in one in which the understanding of cyberspace as a domain (of warfighting, commerce, personal expression, and other activities) serves as a point of theoretical departure. Further, cyberists take

the concept of a domain to be very broad and deep in nature, necessitating appropriate attention and resources.

1. Cybersecurity

Cybersecurity has a relatively long history compared to the cyber profession in general, although not as long as electrical engineers who can be thought of as the builders of cyberspace or at least the technology that makes up cyberspace. Much of what today is called cyber security originated in early operating systems for the goal of protecting information entrusted to the system.[27] Systems accommodated many users and needed to ensure that each one's information could not be accidentally or intentionally compromised by another. The goal of allowing users to freely share files and other objects greatly escalated the complexity of systems and frustrated those who wanted to formally verify that operating system software and hardware would properly protect information. The situation got much worse in the 1980s because the spreading Internet enabled almost anyone in the world to attempt access to a system, often anonymously, and created new kinds of threats such as malware, professional hackers, and thieves.

Today, cybersecurity in the context of the DoD is most commonly associated with the persistent defensive measures used to secure individual devices or nodes like laptops, routers, and computers. A steadily increasing baseline of cybersecurity training for the end user is also included when discussing cybersecurity, as the human is sometimes the weakest link in a defense in depth (DiD) strategy to secure a network. The aforementioned activities are also known as cyber hygiene.

Cyber hygiene normally includes patching, updating, and configuring systems in accordance with local policies and government guidelines. They are focused on execution of tasks and hold as their mantra the policy of least

[27] Jerome Saltzer and Michael Schroeder, "*Protection of information computer systems*." *Proceedings of the IEEE, Volume 63* Issue 9, September 1975, 1278-1308.

privileged (POLP), providing services only where they are required and disabling the rest, as each service includes vulnerabilities that can be exploited by those with malicious intent or users unprepared for such responsibility. Examples of the latter may be an entry level federal employee that gains access to the administrative password on his or her government issued device and disables local security policies that prohibit users from installing programs on the device so he or she can install his or her favorite game or media software. First, the media by which the transfer of the program is made on to the computer may include malware that takes advantage of having administrative privileges and ultimately ruins the device itself or even the whole network. Second, if the local administrative account grants access to download software from any website, which may be of use when updating device drivers, then the user may use the account to surf the web and download software at will, some of which will probably include some vulnerability.

Cyber hygiene is acknowledged as the first and most important line of defense in a DiD strategy, which is today's prevailing model. If one conducts a search online for cyber security jobs, the majority of positions will be that of information technology specialists or the like. If cyber attacks that lead to real physical destruction could be covered under the term cybersecurity then the term would be acceptable, but such offensive activities do not neatly fall under cybersecurity so this term is not the best fit. Such issues of fitness transfer to the components of cybersecurity as well, such as information assurance. The MCP is much too broad to be limited to the covering description of cybersecurity.

Another method of understanding the term cybersecurity comes from a military strategist line of thought and would be a better candidate for an umbrella term for the MCP for those knowledgeable with the mechanics of the large machine bureaucracy that is the United States government (USG). According to doctrine taught at places influenced by the likes of Carl von Clausewitz, such as the War Colleges of the United States, one of which is the Army War College in Carlisle, Pennsylvania, plans and policies can be stratified into levels such as the

tactical, operational, strategic, and grand strategic. In this context, the military is the main actor of the strategic level and below. The capstone policy document at the strategic level is the National Defense Strategy.

A document of similar importance at the grand strategic level is the National Security Strategy. Note that the National *Military* Strategy derives guidance from the National *Security* Strategy. From this perspective, it is clear that the term *security* signifies encompassing of more than just one element of national power (which are doctrinally listed as Diplomatic, Informational, Military, and Economic). If not for the much more prevalent presence of the earlier discussed interpretation of the term cybersecurity, this latter interpretation would serve best. Unfortunately for those concerned with the precision of technical terms used by the general public, strategists may find it difficult to influence what term is used on Main Street after the phrase of choice is already in common use.

2. Cyberwar

With cybersecurity effectively out of the running as the umbrella term of this area at this current time, the next likely candidate is cyberwar. War in the American culture and most surviving cultures of the world is the primary responsibility of the military, even if the military is not responsible for the war. Though a preferred term would cover the non-military elements of power, as discussed in the previous section, many capabilities associated with and thoughts about cyber for military related purposes are so distinct from that of most non-military use that the profession may be labeled as cyber warfare if certain criteria are met. The most military related of cyber activity is offensive destructive activity. The most fundamental prerequisite to using the term cyberwar is if there is an actual war. War is legally declared by the United States Congress and typically includes the mobilization and employment of great amounts of military forces in the applicable domains. If and when the United States Congress declares a war at some future point, experts today believe a cyberwar will undoubtedly commence alongside what contemporary Americans think of as war.

Hopefully, American cyberwar efforts will be in concert with other military assets and elements of national power. Current efforts in the USG, such as the establishment and promotion of USCYBERCOM, aim to lessen the reliance of hope as used in the previous sentence's goal. Because much of what is happening in cyberspace today, including by and to the American military, is not part of a declared war, the area cannot technically be referred to as cyber*war*. That being said, actions against Al Qaida may fall in to the war category, although most Americans would contest that a war includes offensive and defensive operations by at least two opposing belligerents. Once Al Qaida (or another belligerent) musters effective offensive cyber capabilities against American interests or enlists the assistance of a capable ally, the U.S. may find itself in an actual cyberwar with Al Qaida.

3. Cyberconflict

If cyberwar is not applicable to most of the activity of cyberspace due to technicality, the broader mantle of cyberconflict might appear appropriate to cover the area. This term is flexible enough to cover any level of conflict from the most tactical to the grand strategic. Despite the usefulness of the quality of flexibility, it effectively precludes entire components of the profession. An example of such a component would be the elements of the cybersecurity area which are not conflict driven and where such an umbrella term would not be the best fit in the pursuit of best understanding and progress.

4. Cyber

In form reminiscent of the negationist, Karl Popper, after such an exhaustive discussion on what is not the best fit for the title of the profession, a choice can be settled upon that holds up to the gauntlet ran over the proceeding pages. Each choice was subjected to qualitative tests in which the criteria were the desired characteristics of accuracy, fitness with reality, flexibility, popularity, and advantage to further progress. This broadest of possible choices, *cyber* is the ideal title of this profession that is still very much in flux. As stated earlier in

this discussion, much of the development of this profession has yet to be done, necessitating such fundamental debates in a spirit of questioning the existing paradigm.

One reason for progress, which some critics may describe as slow, has been the lack of durable definitions of concepts fundamental to the profession, even in the years since the establishment of USCYBERCOM. At the strategic and grand strategic levels, each word matters. One may find a lack of willingness to move forward confidently by segments of the USG when there is a persistent feeling that the words which translate to budgetary winners and losers are best attempts and quickly perishable. The current definition of cyberspace and cyberspace operations appear to be holding. According to the most current DoD publications, cyberspace is:

> a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers,

and associated *operations* as being conducted *in or through* cyberspace by members of this profession.[28] Here, *cyber* is a derivative of *cyberspace*, which itself is inspired by *cybernetics*. Norbert Wiener, a mathematician, engineer and social philosopher, coined the word "cybernetics" from the Greek word meaning "steersman."[29] The author prefers the use of *cyber* above the theoretically comparable *cyberspace*. *Cyber* is preferred, first, because a profession is not typically named after the domain with which it is primarily concerned. For example, one who conducts warfare on land is called a Soldier or Army professional, and is only referred to as a land warrior unofficially. Secondly, cyber is preferred for the simplicity of keeping in line with USCYBERCOM, which the reader may notice is not USCYBER*SPACE*COM.

---

[28] Gortney, William E., JP 1–02, "Department of Defense Dictionary of Military and Associated Terms," 15 November 2012.

[29] Stuart Umpleby, "Cybernetics: Definition and Description," *A Larry Richards Reader*, 2007, http://polyproject.wikispaces.com/file/view/Larry+Richards+Reader+6+08.pdf.

Alongside the issue of usefulness and political correctness of terminology, there are other reasons for the profession to appear less than fully operational to its ultimate guarantor, the American citizenry. That issue is classification, even within the DoD and the MCP itself. Certain capabilities and techniques are so militarily powerful and sensitive to national security that they are highly classified and legally unavailable for public consumption. The risk of an enemy learning from particularly interesting cyber tools when used outside of the lab is enough to deter those in the know to not only keep quiet, but also not employ such capabilities unless the situation is grave enough to warrant it.

As a result of this relatively small pool of thought applied to developing the MCP, the U.S. suffers from a lack of knowledge and understanding about the true boundaries of this domain. Little could be worse to the many members of the MCP that seek to and are mandated to prepare appropriately for the anticipated threats (or *train like you fight*), but are not *allowed* to know what the true threats actually are. Similarly, a lack of knowledge about what assets the MCP possesses inhibits thought on opportunities to best employ said assets. At the tactical edge, how are warfighters and planners supposed to operate and train like they fight without even being allowed to know what offensive assets are available?

Even in an environment of classified leaks, the overwhelming majority of the members of this very profession do not possess the awareness of capabilities needed for effective wartime operations due to their lack of appropriate clearance and what specific programs they are read in to. One example of this POLP is the baseline *secret* clearance for those in the communication/IT/networking/signal specialties, graduating to higher levels only after there is a proven need, like filling a position in which a higher clearance level is officially required. Many such positions are known to list the higher clearance as a prerequisite to being considered for it, which presents a conundrum standing in the way of clarity across the profession. Maintainers of the current system may explain the understandable cause of such a puzzle as tied to the increased risk and

expenditure of taxpayer dollars that accompanies each new investigation and bestowment of higher classification. Such legitimate causes must be addressed in any holistic approach toward MCP development.

The profession can be described as transdisciplinary because it must leverage contributions across disciplines. Some of the disciplines that share the burdens and benefits of cyber are those of signals intelligence, network engineering, strategic planning, hacking, logisticians, and military targeting. Such a list is far from complete, but is offered to remind the reader an idea of the breadth of disciplines involved. The problems of cyber are shared across such traditional disciplinary boundaries so systemically effective solutions will only derive from an approach that is just as holistic.

The specifically military aspects of cyber include planning and integration of cyber capabilities with various military and non-military capabilities to produce some greater effect of military value. One such example may be the disruptive hacking and shutdown of targeted services that appeared in concert with military operations during the most recent Russo-Georgian conflict.[30] Another example is the Stuxnet worm that resulted in physical destruction of Iranian nuclear assets. As cyber capabilities grow and understandings about how to employ them emerge, one may anticipate their proliferation throughout the force. Both of the above examples appeared to have included military related ends, ways, or means and made great use of cyber capabilities. By contrast, those whose mantra is adversarial influence would find it difficult to envisage such military application without access to a mastery of cyber.[31] In this discussion, those of an influencing worldview will be referred to as Informationists, and are generally aligned to the Information Warfare and IO community. Similarly, those adhering to a perspective from the electronic warfare (EW) camp, who can be referred to

[30] Hollis, David, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, January 2011. Accessed at: http://smallwarsjournal.com/blog/2011/01/cyberwar-case-study-georgia-20/. Accessed: July 2012.

[31] RAND, "Information Operations," (n.d.), http://www.rand.org/topics/information-operations.html.

as Electronicists, are primarily concerned with the flow of electromagnetic waves and signals across the electromagnetic spectrum. Electronicists, too, would be hard pressed to fathom the means by which lines of computer code traveled from a lab to a faraway Iranian nuclear facility.

5. The Electronicists

Statements by some electronicists suggest they view cyber capabilities as something entirely different from their own, with little current and future overlap anticipated. This population sees their niche, typified by technologies aligned towards more sophisticated adversaries than have been directly engaged since the attacks of September 11th, as enduring. Their observable focus remains jamming radios, radars, and other such generally direct electromagnetic interferences. They are less focused on IT networks, but on devices deemed critical to an adversary. Those of their camp who focus on collecting intelligence about the devices that are emanating such signals fall under the banner of electronic intelligence (ELINT), currently a subset of signals intelligence (SIGINT). It is worth noting that the author is a graduate of the U.S. Army Military Intelligence (MI) Officer Advanced Course and the SIGINT/EW Officer Course at the Army Intelligence School at Fort Huachuca.

Electronicists, be they of the offensive, defensive, or exploitative subsets, are generally not equipped to cope with the full range of challenges posed by the networked domain of cyberspace. However, such expertise of the electromagnetic spectrum (EMS) and applicable systems is of great use to cyber. cyberism informed by EMS expertise has orders of magnitude more insight in to cyberspace, as most cyberists are more familiar with the higher levels of the OSI (Open Systems Interconnect) model. One example of such insight may be a handheld electronic emanation sensor that can bypass all the layers of security built in to software to derive the unencrypted data traveling through a device.

The EMS is generally seen by cyberists as layer 1 of the OSI model and serves as cyber’s grounding in the physical world. EMS work is entirely based in

natural sciences like physics, as opposed to software engineers that typically work in a more malleable environment. Considering the above discussion, combined with the shrinking Defense budget, one may predict electronicist lack of enthusiasm for the aggressive growth of cyber.

One solution based on compromise to meet the needs of each complimentary camp may exist in a separate and protected line of funding for purely electronicist work while EMS functions are firmly under a cyberist construct so they may achieve a unity of effort and realization of critical Cyber-EMS potential. One example of a national security topic of importance that clearly requires much more attention by a Cyber-EMS team is the challenge posed by adversary EMP (electromagnetic pulse) technology. As noted by a number of philosophers of science, the new way of thinking must have the courage to break with the past if the advantages to understanding are far greater than the retooling cost. Likewise, a complete scrapping of valuable expertise that some may describe as legacy would be a mistake of considerable consequence, for the worldview of Electronicists offer far more possibilities to understand the true boundaries of cyber. The retention of useful components of a supplanted theory is a piece of wisdom echoed by philosophers over the years, such as the retention of useful aspects of Newtonian physics which was long ago superseded by those offering more scientific advancement.

6. The Informationists

Informationists, in this discussion, are those primarily from the IO or Information Warfare communities. As with electronicists, comments made by some informationists lead one to believe they are a camp that has mixed feelings about the rapid emergence of cyberist thought and the dollars that are associated with such thought. Some erroneously equate IO with Cyberspace Operations. This is understandably due, in part, to terminology. For example, if cyberspace lives on pieces of information technology (IT) like servers and personal computers, then one could infer that the terms are interchangeable. When

considering the wide range of criteria used in the above testing of labels, one may conclude that the potential for added confusion has come with the recent renaming of Psychological Operation to Military Information Support Operations (MISO).

Another reason for the current lack of clarity is the long housing of Computer Network Operations (CNO), the predecessor of cyberspace Operations, as one of the five core competencies of IO. For example, the 1st IO Command of the Army included CNO activities that increased steadily over the years until the establishment of the Cyber Command. In line with an Informationist perspective, cyberspace was simply another avenue of influencing a target. The previous definition of IO from JP 1-02 sheds light on the limited scope by which CNO and EW were viewed:

> The integrated employment of the core capabilities of electronic warfare, computer network operations, military information support operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.[32]

Armed with such charges to use aforementioned capabilities to impact or protect decision making is critical to military operations, but very limited in scope when taking in to account the growth and challenges of cyberspace. The dramatic increase in size and scope of cyberspace may not have been anticipated and the mechanics of the machine bureaucracy had been slow to react. A recently updated joint definition of IO sheds specific reference to CNO and the other four core areas for the term information related capabilities. Such an update provides this community more flexibility, which may prove useful in prioritizing cyber as CNO is no longer specified as merely one among five other capabilities. The new definition reads:

---

[32] Gortney, William E., JP 1–02, "Department of Defense Dictionary of Military and Associated Terms," 15 November 2012.

> The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.[33]

Such pressures as discussed above, combined with shared responsibilities with Networkists (defined next), has resulted in years of building an increasingly complex plethora of taxpayer-financed networks. Such networks have prioritized quality of service and do not necessarily lend themselves to defense against an active threat. In short, many DoD related networks seem to be more of a liability than asset. The Navy's human resources initiative of bringing previously existing information-related communities under a single umbrella group, which they call a warfare community, is called the IDC.

The effort attempts to force better cooperation between the elements that populate it and rebrand them in the process to reflect the Informationist priority. The member disciplines are those of Navy Intelligence, Information Warfare, Meteorology, and Information Professional. The ambiguously named Information Professional community is more functionally aligned with the Army Signal Corps than with the Army's IO functional area (FA). Only a couple of years old at the beginning of this study, some attest that expectations and norms of the IDC have yet to permeate the Navy, DoD, or USG. The grouping increases synergy and collaboration throughout the IDC, which is good for the cyber profession because one persistent criticism has been the traditional disconnect between the worldviews of techs that understand the network and the intelligence community that understand the enemy. The IDC is the Navy's most ready tool to apply to the challenge of cyberspace and offers one potential model to the rest of the DoD if a rearrangement of existing components is the most daring redesign leaders envision and decision makers are willing to support.

[33] Gortney, William E., JP 1–02, "Department of Defense Dictionary of Military and Associated Terms," 15 August 2013.

7. The Networkists

Alongside the electronicist and informationist schools of thought that the author has determined not the best fit for leading the long-term development of cyber within the context of the military, there remains a perspective that understands computers and networks but is not sufficiently prepared to exploit cyberspace as a domain of conflict. Different services have different labels for them, such as the Information Professionals in the Navy or Signaleers in the Army, but for this discussion they will be referred to as networkists. They generally interpreted the concept of net-centric warfare to highlight the criticality of their communications networks, a truth they had always known. Such an interpretation may be denounced by epistemological constructivists as self-serving, but it is more understandable when taking in to account the lack of a holistic understanding that would have emerged if members of that community were privy to the full extent of threats to and through the network itself. It is worth noting that the author's previous occupational area was that of an Army Signal Officer.

Unlike the reduced influence of EW, which came of age in a Cold War world dominated by the clear and present danger of a well-developed Soviet military-industrial complex, the networkists are very influential as those who understand how cyberspace works to a better extent than many other communities. One may metaphorically think of them like the Army Engineers, which understand how to build, destroy, and manipulate the physical domain around them in order to enable others to do their jobs like maneuvering to engage an enemy. However, the Engineer's primary job is not to engage. Fighting is the essence of what makes the military unique versus other institutions, necessitating theoretical paradigms that best support their success.

8. The Cyberists

The most distinguishing features of a cyberist are their understanding of cyberspace as a domain and their calls to treat it as such. cyberists are generally

those that have a baseline of a technical competence, included in which is networking and how the Internet works. Armed with these legs to traverse and eyes to observe cyberspace, they have some situational awareness.

One may assume that it generally helps if they are natives to cyberspace, as opposed to immigrants, but not necessarily so. As was mentioned earlier in the discussion, many cyberists operate at the higher levels of the OSI model and dig deeper only enough to understand how their own areas of interest work. Many times this at least includes working on the command terminal or command prompt instead of the GUI (graphical user interface). GUIs like Windows became so widespread in the 1990s that usage of manual commands was no longer necessary to operate a computer, leaving those who came in to computers before GUI dominance with a more solid grounding on the fundamentals of how a computer functions. Natives, characterized by growing up with the Internet and generally not being forced to operate GUIless, may be in some ways less attuned to the actual functions of their own devices than those immigrants to cyberspace who happened upon computers later in life but still before the mid-90s. Drawing upon many disciplines, including the lessons derived from the soil of experience that is human history, cyberists believe that an effective defense must include a strong offensive capability.

Cyberists have many motivations. One line of thought from economics maintains that cyberspace is the place that will make or break the United States economy in the 21st century, upon which all other elements of national power depend. In essence, nations have some competitive advantage(s) they use to survive in the world. For some it may be their advantageous geography, or military might, or natural resources. Many believe that America has traditionally thrived upon creativity, which a free people motivated by incentive lend itself to.

When criminals or hackers of some foreign government or commercial entity steal the products of American creativity, then the drive to create evaporates. Not only are all the public and private research and development investments wasted and capitalized upon by another nation, but the potential

future revenue into the U.S. evaporates. Such a fundamental threat to the system will force the American culture to evolve. Without addressing such grand strategic challenges from cyberspace now with wise investments that poise the nation for future opportunities, the nation could potentially turn to more militant options like exploiting an ever-lessening advantage in hard power. Though massive intellectual theft has already occurred, securing cyberspace offers an opportunity to protect future American investments. The overwhelmingly defensive approach to cyber that has branded most USG efforts in the public eye is believed to be an insufficient approach to cyberists. In short, what other than a failed state would allow another to repeatedly conduct successful raids into its territory, which local authorities could not handle, without a response that would likely include military action? The same logic applies to cyberspace.

Various models are being considered across the DoD for growing and sustaining the MCP. One of which is the IDC approach, as discussed above. One other model, hinted at in the discussion on Networkists, is the future prospect of establishing a separate cyber service in the DoD, alongside the Army, Air Force, and others. A smaller and focused service, like the Marine Corps, may be the best long-term fit for the needs of the nation. The concept is worth pursuing, but does not currently seem ready to implement. Two reasons are discussed below.

First, the cyber profession within the DoD is still making sense of what cyber is and what it should be. Many of its members are periodically transferred to perform in different domains, not necessarily lending to the deeper development demanded of this little-understood domain. There is still much development to be done before a U.S. Cyber Corps is ready to stand beside the U.S. Marine Corps in defense of the Nation. A second inhibitor of a separate cyber service is policy within the DoD but certainly not limited to it. In such a dramatic reorganization, there will be those who perceive themselves to be winners and losers. Those in the latter will naturally resist efforts to evolve, unless they share a greater perspective of their role in the defense of the Nation and evolve to meet the need.

For the time being, it seems the best cyberist choice is somewhere in between the less politically charged option offered by the Navy and the eventual end result of a separate service. This incremental step is currently being developed in the Army and Air Force, where new cyber career occupations are being established. One example is the Cyber Operations Officer career field of the USAF. The Army's Cyberspace Defense Technician warrant officer field is another such example. Neither the Army nor the Air Force has taken the next step of establishing a unified cyber community comprised of all the various Cyber functions needed, like the IDC conglomerate tip toes toward. One could surmise a cyber focused intraservice grouping called a Cyber Dominance Corps (CDC).

Cyberists view cyberspace as a domain, using DoD's definition as a theoretical point of departure.[28] A domain is an all-encompassing concept, included in which is a need to address all of the functions that other domains also address. Simply consider the joint functions, listed by DoD as C2, intelligence, fires, movement and maneuver, protection, and sustainment.[34] Does an entire domain not warrant an organized and coherent effort to at least address each of those listed areas? The answer should be clear to even the most uninformed reader.

When discussing the profession or area of concern in general terms, those who choose to use the term *cybersecurity* instead of *cyber* represent one of three things: they adhere to a non-cyberist paradigm, they adhere to a cyberist paradigm and are precisely discussing cybersecurity, or they are not knowledgeable enough in the area to make the delineation. It should be expected that loose usage and understanding of the above discussed terms favors those who seek continued confusion, in which they profit. Based on a precise understanding of the terms, one may find comfort in the name U.S. Cyber Command and not U.S. Cyber*security* Command. Using the metaphor of

[34] Pentagon, *Joint Publication 3–0, Joint Operations* (Washington, DC: Pentagon, 2011), III-1.

armored assets on a battlefield, a non-cyberist would think first about an armored personnel carrier and second, if at all, about a tank.

Looking to our past for further inspiration, one may consider the development of the air domain of conflict following theoretical and technological change, eventually leading to the establishment of the Air Force. It is useful to recall that it took *decades* to progress from the first air squadrons under the Army Signal Corps before the First World War to the formation of the Army Air Corps that fought the Second World War to the establishment of the Air Force that first technically saw service in Korea.[35]

9. In Training and Education

Aside from a growing number of military training courses like the Joint Cyber Analysis Course offered by the National Security Agency, at the outset of this study there only appeared to be a handful of explicitly cyber degree programs in the U.S. at accredited degree granting institutions. Despite their small numbers, momentum is behind cyber education and programs are expected to continue to bloom. Each of those programs is relatively new, as the term cyber was not even firmly established in the public mind until the establishment of USCYBERCOM a few years ago. Each program looks different, as each is asking questions like what the nature of military or non-military cyber work is, what should be taught, and how students will gain employment after graduation if not in federal service. The federal government has made efforts toward facilitating the answering of such questions with organizations like the National Initiative for Cybersecurity Education (NICE).

One example of a cyber degree program is the masters of science in Cyber Systems and Operations (MS in CSO) at NPS in Monterey, California. As described in the school's general catalog, this particular program can be considered very cyberist, despite the Informationist leaning influence of the Navy

[35] *General Records of the Chief Signal Officer*, 1914–18, National Archives. From http://www.archives.gov/research/guide-fed-records/groups/018.html#18.2. Accessed December 2012.

IDC. Much of the research in cyber programs appear to be similar to what would be expected of Computer Scientists, but with a distinct focus on offensive and defensive topics. There are also many cyberists with non-technical interests pursuing valuable research in the many policy areas that are naturally available to an entire domain.

Various professional associations and related journals currently service the field, although almost all predate the establishment of USCYBERCOM and have primary focuses other than cyber. Touched upon earlier in this work, a non-exhaustive list of some examples follows: the Association of Old Crows (AOC) and their Journal of Electronic Defense and IO Journal, the Signal Corps Regimental Association (SCRA) and their Army Communicator Journal, the Armed Forces Communications and Electronics Association (AFCEA) and their journal Signal, the Institute of Electric and Electronic Engineers (IEEE) and their journals, and the stand-alone Journal of Law and Cyber Warfare (JLCW). Each of the above listed organizations is dominated by one of the camps discussed above, bringing them great influence. None of the listed organizations are cyberist in stance except maybe for the JLCW, which is focused on a particular aspect of cyber and not the most suitable choice for most of the field. Those listed associations are backed by their respective non-cyberist camps and are therefore not the best fit to encourage progress of the cyber profession within the military.

III. ENVISIONING

Denning and Dunham describe the envisioning practice as about crystallizing the possibility that arose in sensing into a story about how the possibility will appear and be valuable in the future of the adopting audience.[36] In the formation of MCPA much of this practice was initially mental, drawing upon the author's experience, observations, and logic.

The value of the IW framework was apparent in this practice, as the framework helped the author identify and avert common breakdowns. One such potential breakdown came as the limits to the author's business experience became apparent when developing a business plan. The gap was addressed by seeking assistance and attending a business plan development workshop, which will be discussed in this chapter.

One early principle in the design of the association was that it would have the look and feel of a traditional military focused professional association as a way of staying true to the niche need and building off of the trust that other associations have been developing for generations. The importance of branding also includes symbolism like the design of logos, through which, some of the vision was intended to be transmitted. Upon review of a wide range of military associations, characteristic services offered were found to include a website, recognition program, journal, events, chapters, and outreach.

A. NAME, MISSION, VALUES, AND VISION

1. Name

The name had to reflect the scope, mission, and identity of the new organization. The Military Cyber Professionals Association (MCPA) was selected.

[36] Peter J. Denning and Roberts Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010), 141.

2. Mission

The mission statement had to be simple and to the point of the organization. The first version of the mission statement reads: Our mission is to develop the American military cyber profession. A subsequent version of the mission statement was amended to include mention of investing in the nation's future through STEM outreach as a means of elevating the importance of such an effort.[37]

3. Values

The organization's values are prioritized and reflect the three most important ideals for this particular profession, according to the author.

a. Loyalty

In standing by a loyalty to the nation, the Constitution, the American people, and other members, the author addressed multiple objectives. One objective was an indirect condemnation of those who may be called insider threats. Another objective was creating a safe and trustworthy environment for this new team, complete with esprit d'corps.

b. Duty

Similar to the above, by enshrining the duty to do what is right and what is needed meets multiple objectives. Duty to do what is right includes moral courage and ethical action. This is balanced with the duty to do what is needed, which in the military profession may include working weekends and inflicting destruction upon an enemy in accordance with a given mission.

c. Excellence

An emphasis on excellence of thought, word, and action are needed in the development of this profession.[37] The author leaves it up to the

[37] Military Cyber Professionals Association, "About," (n.d.), https://sites.google.com/a/milcyber.org/about/,under "Mission."

seasoned military reader to recall experiences over the course of their military service when a lack of excellence was apparent and impactful.

4. Vision

The organization's vision includes a MCP that is accomplishing what the nation needs, expects, and deserves. Each element is meaningful and synthesizes the priorities of various stakeholders.

- Our nation needs cyberspace secured and available for economic, military, and private individual pursuits.
- Our nation expects its military to work together as a team.
- Our nation deserves a true profession dedicated to developing cyberspace as a domain and national asset.

B. LOGO

An organization's symbol is an artifact with the power to enthrall or dismiss entire populations, which may be a conclusion drawn from the event logo instance discussed above. The founder of the MCPA missed no opportunity to apply systems concepts such as symbiogenesis, in which something new is created by merging different things.[38] The author was in an ideal situation to encourage the melding of various communities. The author is an Army Strategist (Functional Area 59 Officer) with a background in Signal, MI, and SIGINT/EW, enrolled in a cyber master's degree at the Naval Postgraduate School.

In the process of creating something new, the designer(s) may go too far and alienate large segments of the target audience, so a general grounding in traditional military heraldry was decided upon, wherein simplicity and symbols reign supreme. It should reflect the organization's (inherited) heritage and mission. It should be distinct and attractive enough where members would conceivably purchase merchandise featuring the logo, in support of a business plan intent on keeping membership fees nonexistent for service members.

[38] Fritjof Capra, *The Web of Life* (New York: Anchor Books, 1996), 244.

Inspiration was drawn from many sources, including the logos and history American military units.

Holding a degree in History and having been an Iron Soldier, which is somebody who served in the 1st Armored Division (1AD), the author was aware of the symbolism of the 1AD shoulder insignia in historical context. Under order and guidance by then Lieutenant Colonel (LTC) George S. Patton, Jr., the first symbol of the fledgling American Tank Corps was designed during World War I (WWI), the modern version being that of the 1AD (see Figures 12 and 13).

Figure 12. World War I Tank Corps shoulder sleeve insignia.[39]

Figure 13. 1AD shoulder sleeve insignia.

[39] Arthur W. Bergson, Jr., "The Birth of Armored Forces," *U.S. Army Homepage*, March 26, 2007, http://www.army.mil/article/2413/.

Each component of the insignias is symbolic. The yellow (cavalry), blue (infantry), and red (artillery) are the colors of the Army branches from which armored units were formed. The modern version of the insignia features a tank tread, gun, and lightning flash was symbolic of mobility, power, and speed.[40] The nickname of *Old Ironsides* was bestowed upon the 1AD after its commander was impressed by the parallels between the early development of the tank and the Navy's *Old Ironsides* spirit of daring and durability. The Navy ship is the USS Constitution, launched in the late 1700s to fight pirates.[41]

The author has heard the numerous briefs by military leaders using metaphors to convey military cyber related concepts, some of which utilize the innovation of the tank on the battlefield many decades ago. The development of the armored corps may be a fitting inspiration from both an operational and design perspective. The MCPA logo borrows the meta-symbolism of the aforementioned insignia, in that the significance of the elements is not its own symbolism, but that of the community each element represents. The symbolism of each element is described below.

1. Sword

The broadsword is an enduring symbol of military strength. It is positioned upright and centered to emphasize the military focus of the organization. One may also note that the sword is double-edged, which is a colloquialism recognizing the assets and liabilities inherent with any tool.

2. Lightning

The lightning bolt represents the communications and technology fields. According to the mapping of the MCP, the majority of the cyber related personnel come from this community.

---

[40] The Institute of Heraldry, "*1 Armored Division*," (n.d.), http://www.tioh.hqda.pentagon.mil/Heraldry/ArmyDUISSICOA/ArmyHeraldryUnit.aspx?u=3006, under "*Symbolism*."

[41] 1AD website, "*1AD History*" (n.d.), https://www.bliss.army.mil/1AD/History.html, under "*Old Ironsides Designation*."

3. Key

The key represents the intelligence and security communities. The inspiration for this key came from that of the National Security Agency (NSA), a DoD asset. At the time of this study, the Director of the NSA is the first Commander of USCYBERCOM and also another 1AD alumnus.

4. Cloud

While not a standard of military heraldry, the cloud is a widely recognized and popular symbol of cyberspace. The other elements come in and through the cloud.

5. Binary

The organization's motto is encoded in binary, an explanation of which is found later in this section. The American Standard Code for Information Interchange (ASCII) is used to emphasize the American focus of this organization. The binary and translation are found below for the reader's orientation.

01010000011011110111011101100101011100100010000001110
10001101111001000000110001001110101011010010110110001
100100 = Power to build

01010000011011110111011101100101011100100010000001110
10001101111001000000110010001100101011100110111010001
1100100110111101111001 = Power to destroy[42]

The author's independent design process was validated upon a closer look at the logo or seal of USCYBERCOM, which is provided below. The reader will notice the presence of the key, lightning bolt, blades, and encoded message (see Figure 14 and 15).

[42] Military Cyber Professionals Association, "Binary in logo," (n.d.), https://milcyber.org.

Figure 14. The MCPA seal.[42]

Figure 15. The USCYBERCOM seal.[43]

[43] Department of Defense, "USCYBERCOM seal," (n.d.), http://www.defense.gov/home/features/2010/0410_cybersec/images/cybercom_seal_large1.jpg.

C. WEBSITE

A secure website with a professional appearance, communicating the organization's mission, vision, and strategy was initially enough to plant a stake online under an intuitive and simple URL. In this case, it was milcyber.org. As the envisioning practice progressed, so did the site.

1. Collective Intelligence

The establishment of a new social network with learning and problem solving at its essence makes possible deliberate decisions on designing an environment which supports such activities. Inspiration was drawn from works on amplifying collective intelligence, in which the author explains how groups can use online tools to make themselves collectively smarter.[44] Patters seen in the amplification of collective intelligence include:

- Increasing cognitive diversity and range of expertise
- Modularizing collaboration
- Reducing barriers to participation
- Encouraging small contributions
- Developing a rich and well-structured information commons[45]

An approach such as the one above is regularly referred to as crowdsourcing, of which there has been much written about. In this case, the term *community*sourcing was determined to be more appropriate due to the nonpublic nature of discussion forums demanded by a focused set of stakeholders that are sensitive to privacy concerns. Such aspects as communitysourcing and cultivating a collective intelligence were key drivers of the design of the MCPA web presence.

[44] Michael A. Nielsen, "Reinventing Discovery: The New Era of Networked Science," (Princeton, Princeton University Press, 2012), 18.

[45] Michael A. Nielsen, "Reinventing Discovery: The New Era of Networked Science," (Princeton, Princeton University Press, 2012), 33.

2. The Means

After paying to get a single page set up by a local business, and facing continuously billed updates to the site's structure and content, the author soon began researching more cost effective and timely alternatives. After online research, discussions with experienced web personnel, and testing, there were two main choices for the site that met overall price, security, and usability criteria; WordPress or Google Apps for Business (GAB). Each choice came with pros and cons, but ultimately the author selected GAB in large part due to ease of use, reliability, and security benefits.

With a target audience of professionals cognizant of cyber related threats and sensitive to privacy concerns, security was the biggest deciding factor. Although the average person may feel unease about the threat to their personal privacy with public access to historical data using Google Search, only the uninformed debate Google's own infrastructure security. As the site architect and designer, the author mandated the use of secure socket layer (SSL) throughout the site, including display of https in front of URLs with the intent to secure connections and lower apprehensions by suspicious applicants. During the course of this study, the author recruited a well-qualified chief information officer (CIO), whose responsibilities include managing and upgrading the site and other instances of MCPA web presence.

Early in the study, the author determined that potential members expected certain functions of the site, including membership application, merchandise ordering, and basic discussion forum. GAB includes a Forms app, which works well for capturing application submissions and populating it to a spreadsheet app. For payments, the new Google Checkout function was used in an effort to reduce vulnerabilities arising from potential interoperability issues. This service required payers to set up a Google Wallet account before they could pay, which raised the bar to participation. The widely used PayPal service was integrated alongside Google Checkout, allowing for payments by those who simply want to pay without creating any account. Soon after Google's 20 May 2013 announcement

that they would eventually retire the Google Checkout function, the association's website completely retired it.

Various models for discussion forums were observed, ranging from those totally open to public participation to those locked behind member only areas. The GAB Groups apps lends to collaboration, and in light of the past work done on cultivating collective intelligence, the author determined that a robust discussion function should be developed. Even with all communications on the discussion forums being unclassified, security and privacy were nonnegotiable in order to cultivate a trusted environment so this community could connect in the name of development and problem solving. Each local chapter was afforded a Group, which can be used as a discussion forum, e-mail distribution list, and access/permission list. Each Chapter Group was nested under an association wide group of all members, which utilizes the three aforementioned features.

The requirement for member only discussion forums led to the establishment of an association intranet using the GAB Sites app, allowing for further member only collaboration efforts. Some such efforts include a communitysourced database of cyber related professional development opportunities and the development of a Code of Ethics. As discussed earlier in this work, the term *community*sourcing is preferred above *crowd*sourcing, as crowdsourcing implies public access. Access was limited to validated members. An all-source applicant validation process was developed, an overview of which is provided (see Figure 16).

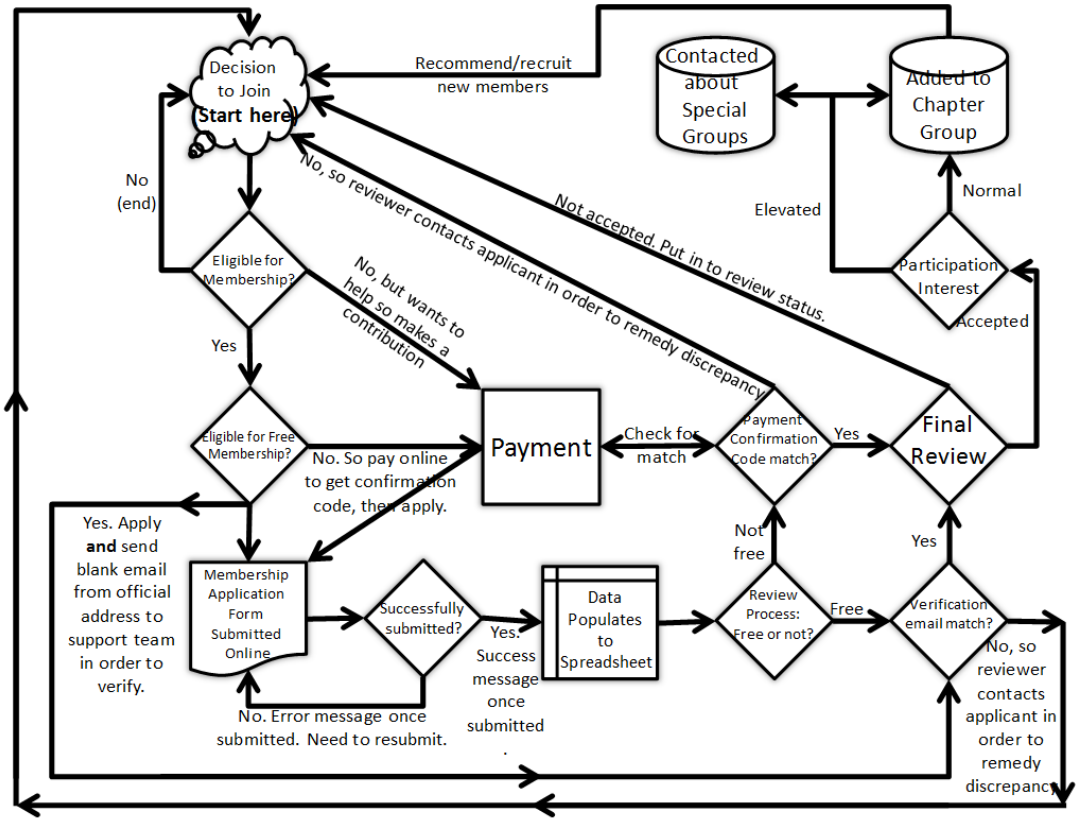

Figure 16. MCPA membership application process feedback loop.[46]

In addition to a website, the author determined that members expected a presence on Facebook and LinkedIn, proceeding to establish such venues. On Facebook, the fan page allows people to "Like" the MCPA. Additionally, a Facebook discussion group accommodates the subset of members that are already very comfortable interacting on that venue. The author considered numerous factors in the decision to establish a Facebook discussion group. One factor was the desire to herd discussions to a common venue to allow for the type of critical mass that can prove a powerful communitysourcing environment. This accommodation risked disconnect of discussions across multiple venues.

[46] Military Cyber Professionals Association, "MCPA Membership Application Process," (n.d.), https://sites.google.com/a/milcyber.org/about/join.

However, lowering the bar to as many members connecting weighed heavier in the author's decision. Since being established, the Facebook discussion site had proved a popular venue for members to connect. It is worth noting that the Facebook discussion group was established as invisible to the public, unless one was invited into it. These secret groups, as Facebook calls them, support a desire for a private and secure environment.

The author also established a LinkedIn company page and LinkedIn group. The LinkedIn group allows members to display their MCPA affiliation and other actions, if desired, which is commonplace for a wide range of military and non-military professional associations. The Facebook and LinkedIn MCPA pages helped this new organization with exposure.

D. ORGANIZATIONAL STRUCTURE

The role of the National staff and leadership is scoped to providing effective organizational leadership and management of various administrative processes in support of the MCPA mission. MCPA policy control will remain with a small board of directors, complimented by a more inclusive board of advisors. Maintaining policy control with a small board is intended to safeguard against mission creep and ensure an enduring Cyberist vision. The organizational structure is provided for the reader's orientation (see Figure 17).

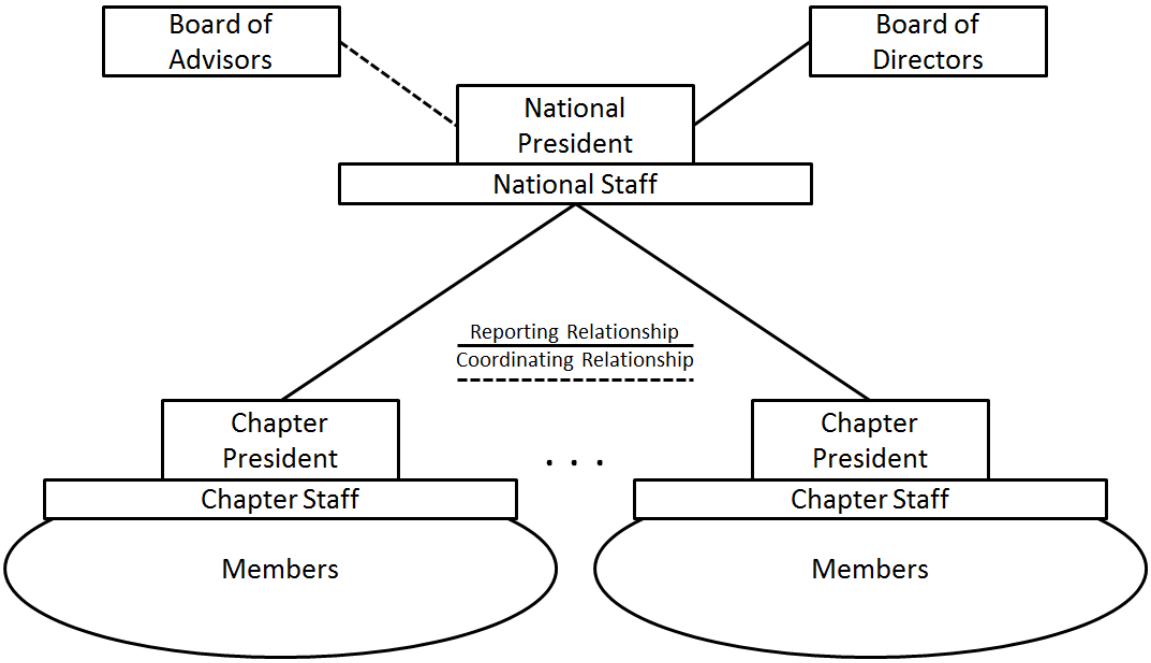

Figure 17. MCPA organizational chart.[47]

Chapters should be established wherever there is potential for enough members to support the mission of the association. There is not a hard number requirement as each community is different. Applications for the establishment of a new chapter by an appropriate leader willing to take responsibility for building the chapter are centrally approved as a means of quality control and coordination. An example of such a decision was whether to preposition the web infrastructure for a single chapter for the National Capital Region (NCR) or split it between three high military cyber professional concentration areas (Fort Meade, the Pentagon, and Fort Belvoir). The decision was made to start off with a unified NCR chapter to encourage collaboration and the type of critical mass needed for self-sustaining growth.

The basic functions of a chapter include organizing local events of both professional and social flavor. Local symposia, conferences, bar calls, barbecues, and balls are all examples of such events. Chapter leaders are

[47] Military Cyber Professionals Association, "Organizational chart," (n.d.), https://sites.google.com/a/milcyber.org/about/faq.

charged with building the chapter and assist with ensuring the recognition and STEM programs are executed in accordance with the intent of the association. By trusting in local leaders to take initiative in their own communities in pursuit of the MCPA mission and vision, the MCPA is able to unleash the power of local communities. With local chapters as the primary interface with a member, the MCPA can develop a distributed, flatter, and highly resilient organization.

E. JOURNAL

More than just a glorified newsletter that is a service expected by the target audience, journals have the potential to play a more powerful role in shaping the public discussion of their given area of focus. In military circles, there are incentives to publish, but those are ancillary when compared to the central role that publishing plays to many academics. Academics, particularly those seeking tenure, are under pressure to publish in well-respected journals in their field, or as the old adage goes, publish or perish. With an understanding of such an incentive structure, a journal can be developed into an influential tool in the development of the American military cyber profession.

Once criteria and a school of thought are established, one can understand that those seeking publication will design their research goals to fit that of the journal. In this case, the journal must be a tool of cyberists in promoting and amplifying cyberist thought and developing the paradigm for theorists and practitioners. Given time, such a process has the ability to change widely held perceptions about the given topic. In this case, there is much need to develop cyberspace as a domain from a military perspective. Characteristics of this journal should include relevance to military matters and an earned respect by academia.

F. RECOGNITION PROGRAM

Some means used to recognize behavior in line with the goals of the association are common across the plethora of military focused professional

association. This way of incentivizing excellence includes coins, certificates, plaques, and medals.

As the author explains on the association website, military associations typically have medals that are symbolically named after some inspirational character from history, mythology, or sacred texts. Some examples include the Order of Mercury from the Signal Corps Regimental Association and the Order of the Archangel from the Military Strategist Association. This association's medal was named in honor of Thor because he is a mythical warrior that operates in and through the clouds.[48] A rendering of the medal is found below (see Figure 18).

Figure 18. Bronze Order of Thor medal.[49]

Further symbolism is covered above in the discussion of the MCPA logo. Options other than Thor included the Catholic Saint Isidore of Seville, patron saint of the Internet. The founder decided upon Thor for the appealing symbolism

[48] Military Cyber Professionals Association, "Frequently Asked Questions," (n.d.), https://sites.google.com/a/milcyber.org/about/faq,under "Why is your medal called the Order of Thor and when can I wear it?."

[49] Military Cyber Professionals Association, "Recognition Program," (n.d.), https://sites.google.com/a/milcyber.org/about/recognition, under "Bronze Order of Thor Medal."

discussed above and popularity among the target membership base due to the recent films featuring the character.[50] While home watching the 2011 film, Thor, the author was struck by the parallels between the film's description of the qualities of Thor's hammer and that of the cyber domain. Those qualities, the power to build and the power to destroy, have become the motto of the MCPA and the binary translation adorns the logo and Thor medal. The binary from the medal is provided below, along with the translation.

> 01010000011011110111011101100101011100100010000001110
> 10001101111001000000110001001110101011010010110110001
> 100100.01010000011011110111011101100101011100100010000
> 00111010001101111001000000110010001100101011100110111
> 01000111001001101111101111001.01000001011101110110000010
> 11100100110010001100101011001000010000001100110011011
> 11011100100010000001110011011100000110010101100011011
> 01001011000010110110000100000011000110110111101101110
> 01110100011100100110100101100010011101010111010001101
> 00101101111011010111001110011
>
> Or
>
> Power to build
>
> Power to destroy
>
> Awarded for special contributions[49]

G. STEM OUTREACH

A widely discussed problem with the American economy is the lack of personnel qualified for work in the Science, Technology, Engineering, and Mathematics (STEM) fields. The MCP in this case is a subset of the U.S. economy. Based upon observation and experience, the author has determined that the talent required to defend the nation in cyberspace cannot be developed once an individual joins the military in their late teens or older. A long-term approach toward growing Americans will a deep understanding in STEM areas would have to begin at a much earlier age, regardless of which sector of the

[50] Brian Kelly, "Patron Saint for the Internet, Isidore of Seville," Catholicism.org, January 8, 2010, http://catholicism.org/patron-saint-for-the-Internet-isidore-of-seville.html.

economy they will eventually contribute to. For these reasons, the MCPA would incentivize its STEM savvy members to volunteer in STEM outreach initiatives in their local communities. An ideal initiative would hypothetically combine cyber with Cub Scout like activities.

After this conclusion concerning STEM outreach was made, the author had discussed the logic with an instructor. The instructor referred the author to a local Institute that was developing a STEM outreach program called Cyber Adventures, which shared many characteristics and intent of what the author had envisioned as an ideal receiver for MCPA STEM outreach volunteers. The head of the Institute agreed to participate as thesis advisor for a case study about the innovation of the MCPA, providing the author time to deliberately design, plan, and execute.

An early opportunity in support of STEM outreach came with the *Ideas of March* event. The event was organized by the Institute for Innovation and Economic Development (IIED), part of nearby California State University – Monterey Bay (CSUMB), which is on the site of the former Fort Ord. This event connected the app concepts of local nonprofit and small business leaders with teams of student Android app developers. After conveying the need and vision for a fun game app that taught binary and hexadecimal conversion, the MCPA founder was armed with a team of student volunteers that selected the project. After an intense weekend of work, the game was produced, presented, and won an award for technical merit. At the time of this study, a presentation about the Conversion Cruncher app can be found on YouTube and a beta version of the Android mobile app could be downloaded using the below visual QR (quick response) code (see Figure 19).[51]

[51] IIED CSUMB, “Conversion Cruncher App,” http://www.youtube.com/watch?v=jDx8DXtMWg4, 2013.

Figure 19. Conversion Cruncher app, beta, QR code.[52]

H. BUSINESS PLAN

In order to support the services described above and the future goals of the organization, it was apparent that the MCPA needed a solid business plan. The author benefitted from advice from multiple sources and participated in a demanding weekend long business development workshop called *Startup Weekend*. Like the *Ideas of March*, this event was organized by the CSUMB IIED.

Of the thirty-two business concepts pitched to the audience, the MCPA was one of only ten selected for development over the weekend. It was the only non-profit business concept pitched. A team of strangers from diverse background swarmed upon the concept, many of whom attested to the worth of the organization's intent. They proceeded to help clarify and add to the MCPA concept. Elevating the significance of regular social events is an example of a

[52] Military Cyber Professionals Association, "QR code," (n.d.), https://sites.google.com/a/milcyber.org/stem/.

finding during the market research process. Another critical benefit was the help in articulating the value membership and sponsorship brings.

Over the course of the weekend, the team attempted to establish a site with basic functionality using WordPress, but was derailed by technical difficulties. The author's experience with WordPress at this event was a contributing factor to deciding upon other website solutions. The culmination of the weekend long event, the author presented the MCPA concept to an audience and panel of judges, some of whom were angle investors. At the time of this study's publication, the final presentation can still be viewed on YouTube.[53] Although there was a competitive aspect to this event, it remained ancillary to the author, whose intent had been met by garnering assistance in developing a solid business plan.

As part of a business plan that sought to keep overhead costs to a minimum while still meeting the basic expectations of the community, the author invested significant effort in researching cloud based merchandise solutions. By essentially outsourcing inventory management to a cloud solution, the author was free to focus on core business operations. After comparing numerous businesses that offered online designing of specific types American made products, like shirts, the author found Zazzle to be the best fit. Zazzle is a business that enables custom, on demand products, that a user can organize in an online shop for free. During this study, the author has maintained possession of recognition program items, like medals and coins until a more permanent solution is developed. The author invested considerable effort in procuring such American made items, which was a demonstration of loyalty to the American people, one of the MCPA values. A simplified overview of the MCPA business concept is provided for the reader's orientation (see Figure 20).

[53] IIED CSUMB, "Startup Weekend, Military Cyber Professionals Association," http://www.youtube.com/watch?v=kzdJ_p_5Azg, 2013.

Figure 20. MCPA business concept.[54]

Part of the business plan included setting quantifiable goals, one of which was recruiting a realistic percentage of members from the target market. Meeting the intent and mission of the MCPA would not necessarily require a large share of the market, but meeting the logistical needs in support of those unquantifiable goals necessitated such a calculation. An approximation of the market size can be derived based upon the number of personnel in cyber related occupations in the DoD. Out of that total number of personnel, not all would be expected to join such a professional association due to their own individual lack of interest or investment in their professional area.

The derivative target population is only a fraction of the total population in question, enough to ensure a Cyberist influence or the consideration of Cyberist perspectives in any important discussion concerning the development of cyber in the DoD. With the intent of keeping this work free from distribution restrictions, hard numbers will not be provided. Using the classic Rogers model of innovation diffusion as a guide and consideration of the rate of growth during the time of this

[54] Military Cyber Professionals Association, "Business concept," (n.d.), https://sites.google.com/a/milcyber.org/about/faq.

study, the MCPA membership goals are expected to take years to achieve. The Rogers model is provided for the reader's orientation (see Figure 21).

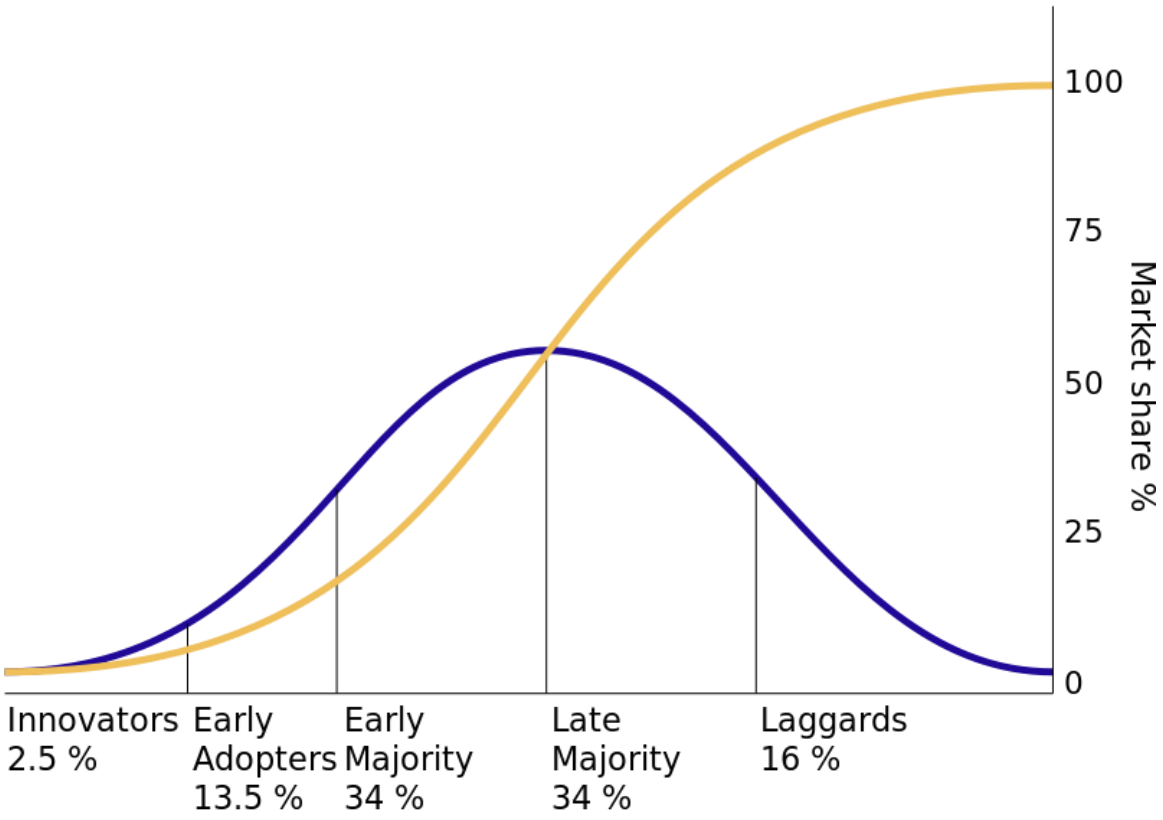

Figure 21. The Rogers model of innovation diffusion.[55]

55 Everett M. Rogers, "Adopter Categorization on the Basis of Innovativeness," *Diffusion of Innovations* (2003): 281, quoted in Wikipedia, "Diffusion of innovations," (n.d.) https://en.wikipedia.org/wiki/File:Diffusion_of_ideas.svg, under "image."

IV. THE MAIN WORK OF ADOPTION

Denning and Dunham describe each innovation as being adopted three times. The first is in the mind when offering the concept and people commit to consider the idea. The second is in the hand when adopters commit to the trial. The third is in the body when adopters commit to sustaining the innovation over time.[56] This chapter discusses each of the three stages of adoption of the MCPA.

The offer for MCPA was promulgated primarily through the website and public relations (PR) activities. The response was measured primarily by people joining the organization, but also by observing other factors such as website view statistics and the reposting of articles.

A. OFFERING

After having developed the web mechanisms to process membership applications and some local activities, it was time to offer membership in the new organization and remain vigilant in responding to feedback. From the author's perspective, the more impactful practice of offering came with the publishing of an article about the MCPA.

1. Press

The article, published by the NPS Public Affairs Office (PAO), articulates the MCPA concept vividly and made a powerful contextual case for it. Included with the article is a picture that featured the MCPA founder meeting with the President-elect of the Association of Old Crows (AOC) at the NPS Cyber for Cyber Warfare (CCW). During the discussion, the AOC President-elect, an Electronicist, conveyed recognition and respect for the niche that the MCPA intended to fill, being that cyber is not the primary interest of the AOC. The symbolic value of the picture is tremendous, demonstrating cooperation and

[56] Peter J. Denning and Roberts Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010), 187.

respect between the different communities, in accordance with the MCPA vision. The photo is provided (see Figure 22).

Figure 22. Picture of Billingsley and Shaw featured in an NPS article.

First published on the NPS website in early April 2013, the article organically propagated across the web.[57] Shortly after the NPS article was published, the MCPA founder was approached by a writer for *Associations Now*, a magazine of the Center for Association Leadership. The resulting article was published in the magazine's Leadership section. At the time of this study, the article can be found online.[58] This second article was more focused on the business aspects of the MCPA effort. Increased exposure about the offer resulted, partially measured by recorded views of the MCPA site (see Figure 23).

[57] Kenneth A. Stewart, "Cyber Warriors Professionals Association Another Sign of Evolving Battlefield,"NPS, April 8, 2013, http://www.nps.edu/About/News/Cyber-Warriors-Professional-Association-Another-Sign-of-Evolving-Battlefield.html.

[58] Rob Scott, "New Cyber Warfare Association Will Address Evolving Military Needs," *Associations Now*, April 12,2013, http://associationsnow.com/2013/04/new-cyber-warfare-association-will-address-evolving-military-needs/.

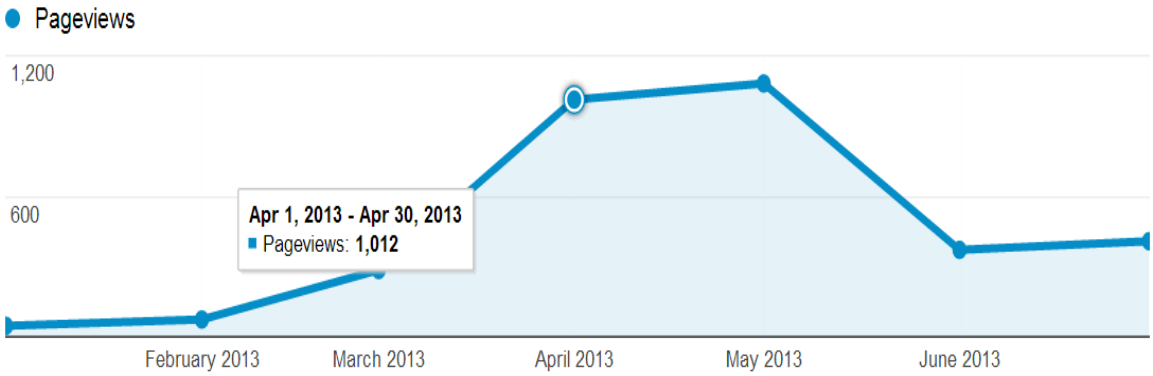

Figure 23. Page views of the MCPA homepage, produced using Google Analytics.

Some of the sites or services that reposted the above articles include: Navy.mil, DoDLive.mil, DVids.net, Journal of Law and Cyber Warfare, legalpronews.findlaw.com, patriotfiles.com, information-operations.com, gala-global.org, highbeam.com, institute-for-operations-research.rsspump.com, newsle.com, newsle.com, asktostudy.com, cyberwar.einnews.com, worldcyberfacts.blogspot.com, silobreaker.com, associationuniverse.com, securnews.com, rediff.com, de.cyclopaedia.net, and numerous public and private Facebook.com, LinkedIn.com and Twitter.com accounts. A simple Google search was used to find the aforementioned links.

2. Feedback

The author avoided some potential breakdowns by cultivating an environment of unfettered feedback with the PAO. The founder engaged some social hubs who had displayed an interest in the MCP and their efforts helped to spread the word further and provided added social validity to the initiative. Some others provided feedback as to why they would not yet adopt. Intuition and the warnings of the IW framework used vigilance in responding to feedback. The site and membership form were even modified to encourage feedback. Not surprisingly, zero complaints were received about the price of membership. Conscious of keeping barriers to adoption low, membership fees were waived for all employees of the USG and the States, encouraging integration of those like

state Nation Guards. Feedback responded to by leveraging U.S. military tradition, namely naval, when conveying all early adopters with the title of *plank holder*. A plank holder or owner is a title of prestige for a crewmember that sailed on the first voyage of a ship or was part of a unit when it was first established.[59]

B. ADOPTION

The articles mentioned above that reverberated across the web helped to get the word out to those interested enough in the subject to conduct web searches of news articles covering the development of the MCPA. The result was a diverse body of adopters from various occupations, organizations, and locations. As discussed in the first chapter of this work, conceptual diversity and a range of expertise was sought to support communitysourcing efforts.[45] From this perspective, the more diverse the membership base, the more potential for effective problem solving. Membership applications included information such as occupation, organization, location, and recommender (if any), allowing for precise tracking of adoption.

Samplings of the plank holders reveal their diversity. They come from the Pentagon, Air Force, Army, Navy, Marines, Senate, DIA, DISA, DHS, NSA, DOE, GAO, allied nations, Silicon Valley, and the citizenry. They are Active Duty uniformed service members, USG civilian employees, contractors, Reservists, members of State National Guards, veterans, businesspeople, and students. The rank of adopters range from flag officer to junior enlisted. They are located in the U.S., as well as overseas. They come from a wide range of communities, some of which include warfighters, intelligence personnel, communicators, academics, attorneys, foreign area officers, strategists, and information scientists.

One of the most notable clusters of adopters includes members of the office responsible for cyber policy in the Office of the Secretary of Defense, the first of which was a former DARPA employee. The MCPA concept was built

[59] Karen E. Riecks, "Plank Owner, Plank Holder," Nautical Dictionary, (n.d.), http://www.seatalk.info/cgi-bin/nautical-marine-sailing-dictionary/db.cgi?db=db&uid=default&FirstLetter=p&sb=Term&view_records=View&nh=4.

around the strategic priorities of the DoD concerning cyber, so adoption by this particular cluster can be interpreted as evidence suggesting the strategic validity and value of the concept. The author here notes the interesting parallels between the propagation of well-designed concepts in the wilds of cyberspace until (and after) it hits its target and that of the reported spread of Stuxnet.

1. Measurement

In this case innovation adoption was operationalized, or measured, by members joining the organization and those non-members providing observable support such as sponsorship. Following the aforementioned three-part criteria, the idea was considered when the potential adopter visited the site. The willingness to start the application process can be considered the initial trial. For the purposes of operationalizing *adoption* for this study, completion of the application process through to validation, which includes providing personally identifiable information (PII), is a demonstration of enduring commitment by an adopter. Sharing of one's PII in this online environment is considered to meet the adoption criteria because members of this particular community are much more sensitive than most to the vulnerabilities inherent to such sharing. Adoption statistics are displayed below (see Figure 24).

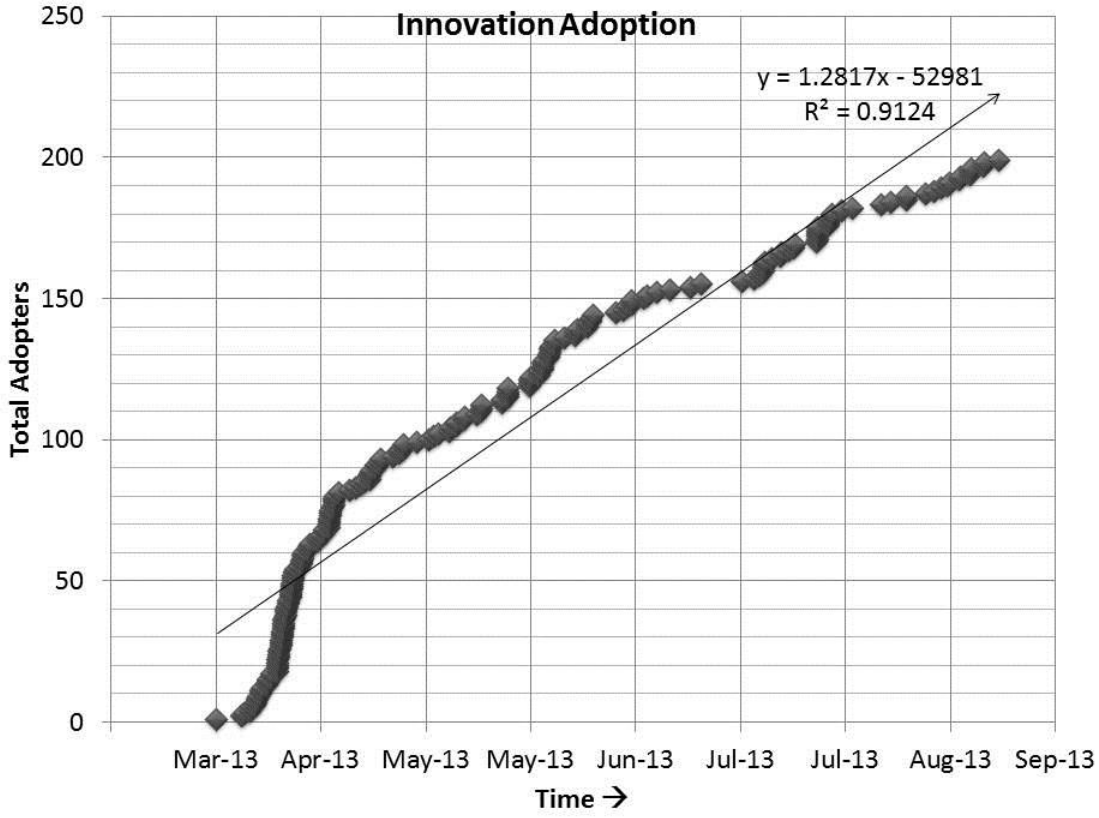

Figure 24. Total adopters over time from MCPA membership data.

2. Resistance

Various forms of resistance were encountered while seeking adoption. Some potential resisters were successfully transformed in to partners with the application of respect, humility, and providing a mutually beneficial vision of a shared future. Other resisters, be they active or passive, may remain unresolved. Armed with the IW framework, complimented with a healthy dose of insight from the works of Kuhn and Rogers, the author of this study concluded that patience is the only solution to overcome some resisters.

3. Breakdowns

Some characteristic breakdowns during this practice were anticipated and averted by the author of this study. Due to the lack of assigned subordinates

during duty as a student, the author found the easiest breakdown to avert to be the forcing of adoption through compulsion.

The author found initial difficulty in articulating the value derived from adopting, but overcame the challenge by seeking help and a crowdsourced solution during the Startup Weekend event. Yet another challenge was the initial lack of enabling tools and process for adoption, which was remedied with the refinement of the membership application process. Such are examples of characteristic breakdowns of this practice, identified by the IW framework, that the author took action toward remedying earlier on than if recognition of the breakdown had not occurred.

C. SUSTAINING

The anatomy of the sustaining practice involves the objectives of integrating, enabling, supporting, and dealing with ongoing resistance.[60] Manifestations of each objective found in this case are discussed below, none of which have been completed at the time of this study.

1. Integrating

By establishing a recognition program with artifacts that are very common throughout the culture of the target membership base, such as medals and coins, little rethinking was required for it to make sense. It is common for military communities to have aligned professional organizations, each with their own medal recognizing excellence in their given focus area and according to their own criteria. Such a move is an example of integrating within existing structures.

The STEM outreach program is another such example, in that MCPA members are volunteering in established STEM related programs in their local community, which also endears them with local community leaders. In this area,

[60] Peter J. Denning and Roberts Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010), 207.

the role of the MCPA chapter is limited to offering interested members with a list of local opportunities, tracking hours, and recognizing such contributions.

One potential breakdown cited in the framework is the lack of commitment to continue. Although the founder is committed, duty as an active duty officer may potentially overcome the ability to devote appropriate time to leading the effort. The solution has been found in integrating dependable leaders responsible for key functions. As time progresses and more resources are available to the growing organization, all functions of leading and managing the MCPA are planned to be handed over, with the founder retaining dominant policy influence at the head of a board of directors.

2. Enabling

Based upon observables, leaders cognizant of the effort have generally given passive or unspoken support for the initiative. Some have given active support, such as taking an official role in the organization, spreading the word, contributing their perspective as part of a video series on the development of the MCP, or playing a role in the thesis process which has enabled the author to have founded the MCPA. To date, no leaders have provided active and observable resistance.

The single greatest impediment to enabling growth through local chapter activities has been a lack of a finalized Charter. The need to establish such a document for local chapters to base their activities off of is apparent and has been dependent upon key organizational decisions. With such decisions recently having been made, such enabling documents will be published after appropriate legal counsel.

3. Supporting

Some important elements of a supportive environment include education and training customer service, tools, maintenance, emotional support, value,

accommodating adoption rates, and managing moods.[61] As a result of leveraging a relatively refined GAB infrastructure, many of these elements were nonissues for the MCPA. An initial difficulty with sharing forum postings in a regular consolidated digest e-mail, exacerbated by the founder's uncompromising efforts to keep all MCPA communications from public view, were solved. So, too, was the issue of mistaken URL. After observing numerous and understandable erroneous references to a milcyber.*com*, related potential security concerns were quelled with the purchase of milcyber.com and redirecting it to milcyber.*org*.

Dealing with resistance, be it actual or anticipated, needed to be addressed. Resistance by those who did not feel comfortable signing up for a Google account in order to join was addressed by policy update, tradeoffs, and accommodation. On the MCPA's GAB infrastructure, a member's Google account is used to control access to intranet pages because GAB does not provide such access functionality for non-Google accounts. The founder had decided upon a policy update that allowed applicants to provide a non-Google account (or Google-linked account) with the understanding that they would not have access to certain members-only benefits like the MCPA intranet. They would still be able to access the e-mail distribution list function. Such a trade-off was deemed acceptable, when considering that any other non-governmental credentialing solution would force maintenance of yet another username and password. More so, any other non-governmental credentialing solution would not have security investments on par with the GAB solution.

Alternative credentialing solutions were investigated. After observing DoD credentialing being leveraged by another NGE professional association for their portal access, the author found an organization that specializes in federated credentialing across governmental and NGEs. For a price, and having met

[61] Peter J. Denning and Roberts Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010), 209.

certain infrastructural standards, federated credentialing with DoD certificate authorities (CA) was determined a potential course of action, albeit not for the near term.

Real work has gone toward incorporating potential resisters as partners in an effort to neutralize resistance before it happens and further diversify the membership base. One example of partnership has been demonstrated by coordination with other associations interested in the MCP, one of which is the Air Force Command, Control, Communications, and Computers Association (AFC4A). The AFC4A has added a MCPA link to their list of suggested websites.[62] The MCPA is refining its message and mechanisms to create meaningful partnerships. Potential legal resistance to the initiative has been addressed by the development of an organic MCPA legal team.

[62] Air Force Command, Control, Communications, and Computers Association, "Suggested websites," (n.d.), http://afc4a.org/Hot%20Links.asp.

V. THE ENVIRONMENT FOR THE OTHER PRACTICES

A. EXECUTING

Executing refers to making and completing the commitments of the organization. Within the first few months of offering, some of the promised benefits to members had already been demonstrated. Some unexpected benefits had even emerged.

This chapter will examine anecdotal evidence of benefits that emerged, many of which from reducing the numerous degrees of separation between members of this community down to two. Degrees of separation between members, or hops, were reduced by utilizing weak ties. In this case, weak times refer to the ties between each member and the MCPA. In network theory, weak or unofficial ties are recognized as enabling introduction of new information, as those with strong ties most probably already have access to similar information and share a similar perspective.[63]

The below diagram illustrates the hops between individuals, depicted as A, A+1, etc. The solid arrows represent official relationships or strong ties, such as a chain of command. The dashed arrows represent weak or unofficial ties, such as those between an individual to the MCPA. In the below figure, if each of the hops were counted as one, then the number of official hops between individuals A and A+N would be four. In such a scenario, the four official hops are replaced by just two unofficial hops, saving a total of two total hops. Anybody familiar with the many levels of hierarchy of the U.S. military can easily imagine the dramatic number of hops and associated time that can be saved when considering a connection between an individual in the Pentagon and one in a platoon deployed in a combat zone (see Figure 25).

[63] Albert-Laszlo Barabási, *Linked* (Cambridge: Penguin Group, 2003), 43.

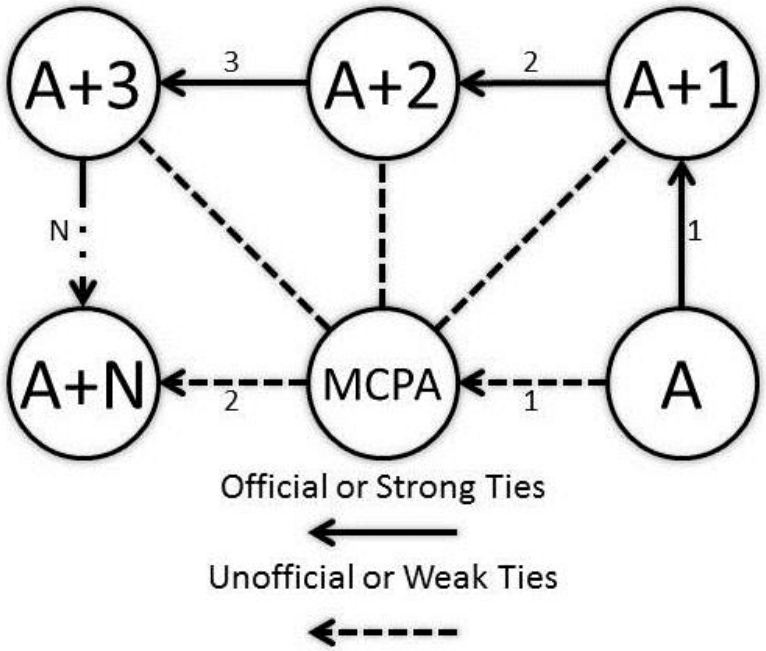

Figure 25. Reducing hops to two by leveraging the potential of weak ties.[64]

1. Task Related

Two exemplars of the potential inherent in the weak ties between members are discussed here. One was a top-down request for input. The other resulted in a bottom-up solution. Realizing such potential is sustained by a standard policy of recognition of quality contributors and reliance on the disposition toward cooperation inherent in the military community.

The top-down instance was a request for input and ideas concerning educating the military cyber workforce. The requestor was a member in the Pentagon working on an official document. The call for input from the MCPA community provided a real opportunity for members across the force to provide direct input into a document that would directly affect their profession. A number of recommendations were provided by a diverse set of members.

[64] Military Cyber Professionals Association, "Networking," (n.d.), https://sites.google.com/a/milcyber.org/about/join, under "Some benefits include."

The bottom-up example was a call for input by a member that was responsible for developing a discussion for his organization concerning certain aspects of cyber operations in the military. He received numerous replies, both directly e-mailed to him and accessible to the community. One of the responses available to the community came from a highly qualified subject matter expert in the Pentagon. The requestor expressed enthusiastic feedback to MCPA leadership about the feedback and about significant potential for leveraging unofficial stakeholders in developing this emerging area.

2. Business Related

Without encouraging a brain drain of talented members of the MCP out of government service, business networking has been encouraged, especially in support of veterans, those transitioning to retirement from government service, members from industry, and collaborative opportunities. Examples of business related connections can be found with the successful pairing of partners via MCPA venues. Venues include both cloud based and physical gatherings. Fruitful gatherings of MCPA members even emerged among the backdrop of DEFCON and Blackhat, the annual cyber related conferences in Las Vegas.

3. Professional Development

Some manifestations of the MCPA commitment to developing the profession can be found in the MCPA video series, database, and other artifacts. A video series dedicated to developing the MCP had been established on YouTube, which includes videos of military cyber theorists.[65] Within the MCPA Intranet, a database of cyber related degrees, courses, certifications, centers, and conferences is being built by member input. Also fueled by member input are regular postings of news articles of interest that directly apply to the MCP. Plans for MCPA chapters include at least one professional development event per quarter, although such activities have yet to be realized at the time of this study's publish.

[65] John Arquilla, "Cyber Warfare in a Historical Context," *Military Cyber Professionals Association*, July 2013, http://www.youtube.com/milcyberorg.

With the intend of complimenting or informing current and future innovation processes, especially those within DoD and cyber related, the MCPA encourages the use of effective practices, such as those of the IW framework.[66] Further encouraging innovation related professional development, an innovators discussion group has been established within the organization's Intranet.

In addition to the medal discussed earlier, American made challenge coins have been produced and presented as a means of recognizing excellence and contributions to the profession. Such items are regularly utilized by leaders to encourage and recognize excellence. At the time of this study, there are over forty other items designed to encourage excellence and a sense of esprit d'corps, made available to order on the MCPA online shop.

B. LEADING

Denning and Dunham list seven principles of innovation leadership, many of which had peppered the preceding practices as depicted in Figure 3. The IW leadership principles are:

- Leaders look for opportunities to take care and produce value.
- Leaders encourage other with new narratives for the future.
- Leaders make offers, take stands for their offers, and engage with disagreement and resistance to their efforts.
- Leaders inspire followers to make and sustain commitments; in doing so they build power for themselves and others.
- Leaders initiate actions and conversations, accept the risks, and learn from consequences.
- Leaders build a presence, a voice, and identity to have their offerings heard and accepted.
- Leaders are continually learning and sharpening their own skills.[67]

[66] Military Cyber Professionals Association, "What's Different About Your Organization Compared to Others?," (n.d.), https://sites.google.com/a/milcyber.org/about/faq.

[67] Peter J. Denning and Roberts Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010), 244.

1. Inspiring

Conceptual inspiration came by a strong message, well grounded in the values of the American military. At the ground level, a new organization full of national and local positions of high visibility provided numerous leaders an opportunity to shine while contributing to the development of this national security priority. In designing a relatively flat and distributed organization that entrusts local leadership and focuses on the mission, the founder appears to have tapped in to enormous potential for action. In this case, effective innovation leadership by a junior level military officer was demonstrated by a wide range of followers, including military offers of significantly higher rank. In an effort to encourage an environment of recruiting new followers, a recruiting officer was established as a baseline requirement for each chapter. Taking care as a leader and producing value demanded attention and follow through. One example of taking care was the use of a MCPA discussion group for the coordination of needed care packages for a member deployed to a combat zone.

2. Risk Taking

Accepting risks associated with actions initiated can take many forms. One example is the founder taking on all initial financial risks associated with the establishment of the MCPA, as opposed to seeking partners with which to spread the risk and therefore control. Taking on such risk was balanced with an effective accounting system to monitor funding flows in the organization. At the time of this study, steady progress has been made toward establishing a reliable revenue stream, including purchases from the MCPA shop, paid membership, and maturation of the sponsorship program.

3. Breakdowns

A less successful example of risk taking came in the form of entrusting other personnel to execute tasks which they had agreed to, resulting in months of delays. Some lessons were derived from such delays, including a stop to requests of those who had not clearly and convincingly volunteered themselves for such service.

The ability to maintain focus on the innovation process proved challenging at times for the founder, while simultaneously serving as an active duty Army officer enrolled in Masters, Doctoral, and Joint Professional Military Education programs. Taking risks of credibility and career, including publically associating with the innovation, proved an effective motivator in maintaining focus. With such an insight in mind, one may assume that a study of a less public nature would be coupled with more risk. Where enough focus was not mustered, help was requested or goals appropriately delayed. Pushing back some milestones until after the completion of the study was determined to be an acceptable means of coping with this common breakdown.

C. EMBODYING

1. Somatics

Embodying refers to developing a practice in which one is able to act automatically and skillfully. Applying this as a practice means the innovator needs to embody the eight practices in order for the community to embody the proposed new practice. As part of embodying, the IW framework discusses somatics, or the unity of mind, emotion, and body. Somatics involve maintaining harmony between one's thoughts, body language, and other actions in the pursuit of successful innovation, not personal development goals.[68] The coming together of all other practices and the heart of somatic skill is the process of *blending*, in which one holds their center as choosing to align with another for the sake of opening a shared future.[69] The below image helps to convey the environmental aspect of somatics (see Figure 26).

[68] Peter J. Denning and Roberts Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010), 258.

[69] Peter J. Denning and Roberts Dunham, *The Innovator's Way: Essential Practices for Successful Innovation* (Cambridge, Massachusetts: The MIT Press, 2010), 282.

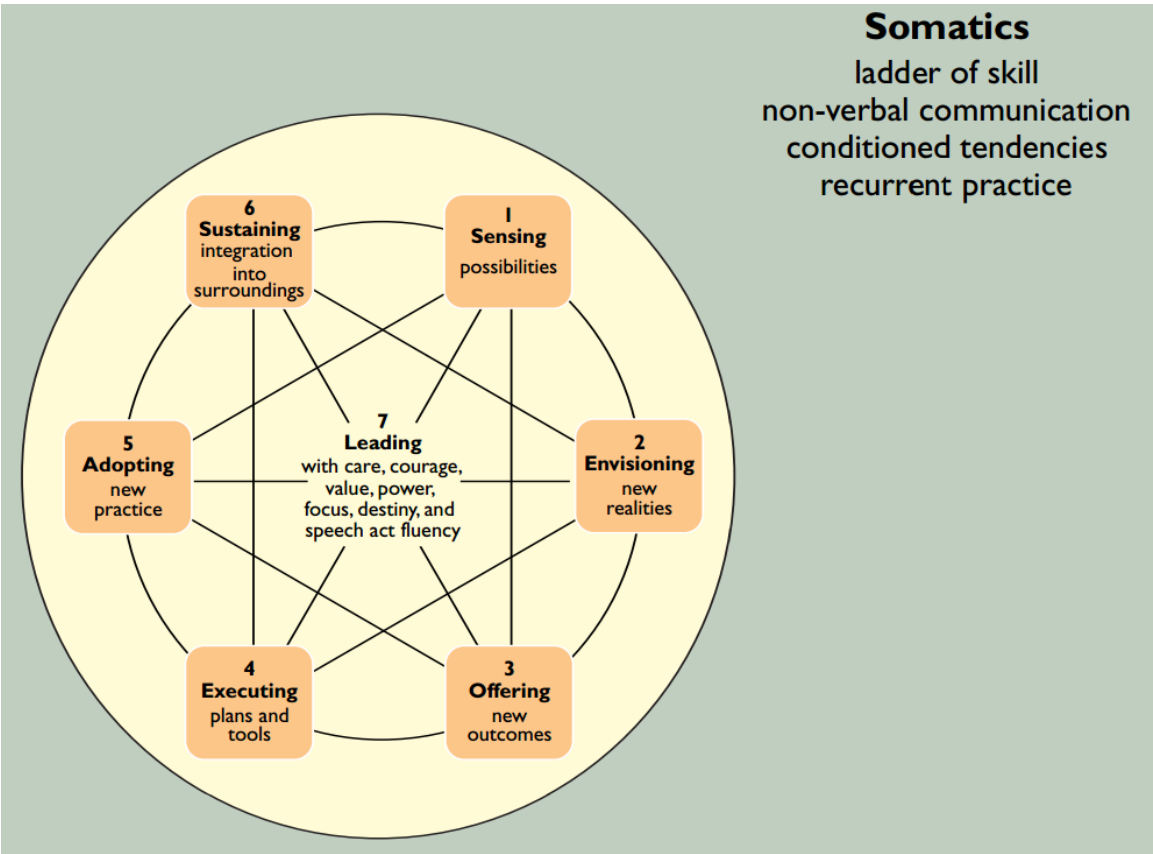

Figure 26. Somatic practices surround others.[70]

Somatic development during prior duty assignments in service as Platoon Leader and Company Commander contributed toward the author avoiding most common breakdowns of this practice, including the inability to read and respond to body language, or failing to appreciate differing levels of skill. The military service demands the ability to lead and communicate, lest lives be lost needlessly. The practice of blending plays a central role in both leading and communicating. Elements of the practice of embodying include producing trust and developing an open and inviting presence. Trust in the innovation builds upon trust in the innovators, both may take years to cultivate and maintain. Having a more permanent office space will encourage an open and inviting

[70] Peter J. Denning and Dennis J. Frailey, *"Innovation as Language Action," Communications of the Association for Computing Machinery*, Volume 49 Issue 5, May 2006, http://web.eecs.umich.edu/~imarkov/Innovation.pdf.

presence, which is planned for the near future. Again, such aspirations are expected to be accomplished in years, not months.

2. Blending

Over the course of this case study, the author aligned with the stated vision of the DoD, articulated by the first Commander (CDR) of USCYBERCOM. Although such alignment had geographically been from afar, an opportunity for face to face dialogue presented itself during a visit by the CDR. While breaking bread, blending occurred between the author and the CDR. During this encounter, the CDR offered his vivid vision for the future of the military cyber profession, as the founder offered the MCPA to compliment and support the CDR's vision. The founder aligned to support the CDR's cyberist vision, some of which went beyond the founder's initial expectations. When presented with the MCPA concept, the CDR provided positive feedback. The below image captures a moment in an instance of blending, during which the founder articulated how the MCPA innovation can support the CDR's vision (see Figure 27).

Figure 27. The author speaking with USCYBERCOM Commander.[71]

Although the above discussed act of blending was the most notable, blending had occurred numerous times throughout this process of innovation. Another notable instance was between the founder and the President-elect of the AOC, previously discussed in this work and visually captured in Figure 22. During that meeting, the two discussed some of the conceptual and physical differences and similarities between EW and cyber, concluding with mutual respect and encouragement of each other's role in support of national defense.

Other examples of blending occurred while building the team that supports MCPA operations and when direct feedback resulted in adjustments to orientation and policy. The earliest case of blending in this innovation process occurring during the first purposeful offer, which was to who would become the advisor for this thesis. In this discussion, a vision for a new organization was articulated, one which could simultaneously gain from and support the interests of the advisor.

[71] Military Cyber Professionals Association, "MCPA Founder, Joe Billingsley (left) breaking bread with USCYBERCOM Commander, Gen. Alexander (right)," (n.d.), https://sites.google.com/a/milcyber.org/about/.

A case of blending based upon feedback was recounted earlier in this work, resulting in the policy update to accept non-Google accounts during membership application. The app development process, also previously documented in this work, can be considered an act of blending, as the author and development team both presented offers that resulted in a shared outcome. In blending, social skills were found to be paramount, including the ability to read and present beyond language.

VI. CONCLUSIONS

The main research objective of this work was to answer each of the research questions in meaningful case study. The objective has been met.

The IW framework has been validated for this innovation process. The successful results of this yearlong process include both conceptual and physical elements. This case study contributes to the body of knowledge about innovation and the MCP. The tangible output of this process is observable online and across numerous DoD installations worldwide.

The IW framework works for both social and technical innovations. The complexity inherent in social systems resulted in an elongated process of invention using social components. The methods provided in the framework for navigating and addressing typical breakdowns, especially in the social domain, proved their value by saving time and reducing needless risk.

A thriving young organization resulting from the IW framework has resulted in increased interest in innovation among members of the defense community, which has been met with encouraged with resources. The wide range of innovations that the IW framework can handle has been demonstrated and is expected to help other aspiring innovators within the MCP and beyond.

The author has concluded that the IW model was well fit and valid for this social innovation, as demonstrated by what was produced. The product of this process is the MCPA and a case study which enriches the body of knowledge about innovation and cyber. Future evidence of the generalizability of the IW model is expected, as the author of this study has been approached by other military officers that have expressed an interest in learning how to develop their own defense related community of interest. If assessment of a theoretical model was based upon its usefulness in understanding and further progress in its given area of interest, then the author has a favorable assessment of this generative framework presented by Denning and Dunham.

Before taking the time to learn the IW framework of practices, some successful professionals will undoubtedly believe their vision and plan is sound, based upon their own experiences and observations. As true as such an initial assumption may be, great risk in the process of innovation can be mitigated by considering the guidance distilled in the IW framework. The wisdom found in the pages of the IW book is a product of years of thoughtful contemplation of experiences and analysis of cases of adoption. Unarmed with the understanding that innovation includes invention through past adoption, inexperienced innovators may be ill equipped without consideration of the breakdowns that typify various practices.

The author of this study has found much deeper insights in the text of IW after having actually gone through en entire deliberate process of innovation. Armed with the undeniable understanding that comes with firsthand experience, a rereading of the IW framework has led the author to conclude that, like with so many other endeavors, practice makes perfect.

A. FUTURE WORK

1. Innovation

This case study demonstrated the opportunity to investigate the nuances of innovation adoption. Recommended future work includes more case studies of innovation generation and emergence in complex systems. Such studies will fuel development and refinement of understandings about innovation and complexity.

More opportunities will arise to investigate new phenomenon as technology evolves and human behavior coevolves. An example of such an opportunity may present itself in a systematic analysis of an innovation adoption, written about from the innovator’s unfettered perspective, as most innovation studies appear to be based on the limited data of the observer, be it secondhand or historical. As discussed by the IW authors, much of the framework was based upon case studies and observations, which are inherently limited. Over the course of this study, a pattern of bursts of innovation adoption was observed, warranting further study to dissect and fundamentally understand the phenomenon.

As other professionals within the government learn of this study and seek to replicate the success in their own area of interest, they will learn the IW framework. Like any model, the more usage it receives, and studies published using it, will lead to further refinement and an enriched body of knowledge. Such a body has yet to be established, but in which those facing challenges can find assistance in the best practices of previous innovators.

2. The Profession and Association

Building upon contributions of this study, further work is warranted on mapping the entire military cyber domain, one component of which is the military cyber profession and those communities with which there is significant overlap. Specifically, an investigation of the pros and cons associated with jointly aligning cyber occupations is warranted. Such work will increase DoD situational awareness, informing decision makers in support of determining the most effective and efficient way ahead. Worse than too few planners across the DoD understanding cyber is the lack of cyber understanding among the cyber profession itself, hence the calls for innovative approaches to development.

Instead of an end goal, establishing the MCPA was merely a first step in addressing the national priority of developing the profession, which itself is a decades-long campaign of tasks. A skillfully angled journal and well executed high visibility events are still yet to have been realized, but the author is confident that such work will be addressed in the near future due to the timeliness and interest in this national security concern.

At the conclusion of this study that resulted in establishing an enduring engine of development of the people who do cyber for the DoD, great comfort can be found in a reminder by the first Commander of ARCYBER, in that the key to cyber is not technology, but people.[72] Today, there is an organization dedicated to developing this profession which avails itself as a test bed for appropriate innovation studies.

---

[72] Rhett Hernandez, "Transforming Cyberspace While at War…Can't Afford Not To!," *Association of the U.S. Army*, 11 October 2011, http://www.ausa.org/meetings/2011/annual/Documents/Presentation_CMF%20LandWarNet%20Hernandez.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. 2011 CYBER OPERATIONS-RELATED MILITARY OCCUPATIONS[73]

Specialty Code	Specialty Title
Air Force	
Enlisted	
3DXXX	Cyberspace Support Career Profession (Cyber Systems)
1B4X1	On-Net Operations
3DX72	Cyber Transport Systems Craftsman (Cyber Systems Operations)
3DX52	Cyber Transport Systems Journeyman (Cyber Systems Operations)
3DX73	RF Transmission Systems Craftsman (Cyber Surety)
3DX90	Cyber Operations Superintendent OR Cyber Systems Superintendent (Cyber Systems Operations)
Officer	
17DXA	Cyber Warfare Operator (Control)
17DXB	Cyberspace Operations (Defense)
Army	
Enlisted	
25B	Information Technology Specialist
25C	Radio Operator
25E	Electromagnetic Spectrum Manager (Grade E6 – E9)
25F	Network Switching Systems Operator - Maintainer
25L	Cable Systems Installer
25M	Multimedia Illustrator
25N	Nodal Network Systems Operator – Maintainer
25P	Microwave Systems Operator – Maintainer
25Q	Multichannel Transmission Systems Operator – Maintainer
25R	Visual Information Equipment Operator - Maintainer
25U	Signal Support Systems Specialist

[73] Department of Defense, "Cyber Operations Personnel Report," (n.d.), http://www.nsci-va.org/CyberReferenceLib/2011–04-Cyber%20Ops%20Personnel.pdf, under "Appendix A – Cyber Operations-related Military Occupations."

Specialty Code	Specialty Title
25S	Satellite Communications Systems Operator – Maintainer
25T	Satellite/Microwave Systems Chief (Grade E8)
25B	Information Technology Specialist
25C	Radio Operator
25E	Electromagnetic Spectrum Manager (Grade E6 – E9)
25F	Network Switching Systems Operator - Maintainer
25L	Cable Systems Installer
25M	Multimedia Illustrator
25N	Nodal Network Systems Operator – Maintainer
25P	Microwave Systems Operator – Maintainer
25Q	Multichannel Transmission Systems Operator – Maintainer
25R	Visual Information Equipment Operator - Maintainer
25U	Signal Support Systems Specialist
25S	Satellite Communications Systems Operator – Maintainer
25T	Satellite/Microwave Systems Chief (Grade E8)
25V	Combat Documentation/Production Specialist
25W	Telecommunications Operations Chief (Grades E7 and E8)
25X	Senior Signal Sergeant (Grade E9)
25Z	Visual Information Operations Chief (Grades E7 – E9)
35H	Common Ground Station (CGS) Analyst
35N	Signals Intelligence Analyst
35P	Cryptologic Linguist
35S	Signals Collector / Analyst
35T	Military Intelligence (MI) Systems Maintainer/Integrator
35Z	Signal Intelligence Senior Sergeant
94E	Radio & Communications Security (COMSEC) Repairer
25V	Combat Documentation/Production Specialist
25W	Telecommunications Operations Chief (Grades E7 and E8)
25X	Senior Signal Sergeant (Grade E9)
Officer	

Specialty Code	Specialty Title
25A	Signal Officer
24A	Telecommunications Systems Engineer
53A	Information Systems Manager
35G	Signal Intelligence/Electronic Warfare (SIGINT/EW) Officer
Warrant Officer	
255A	Information Services Technical (Previous 251A and 254A)
255N	Network Management Technician (Previous 250N)
255S	Information Protection Technician
255Z	Senior Network Operations Technician
Navy	
Enlisted	
IT-2709	Joint Force Air Component Commander (JFACC) System Administrator
IT-2720	Global and Command Control System-Maritime (GCCS-M) System Administrator
IT-2730	Naval Tactical Command Support System (NTCSS) System Administrator
IT-2735	Information Systems Administrator
IT-2779	Information Systems Security Manager
IT- 2780	Network Security Vulnerability Technician
IT-2781	Advanced Network Analyst
IT-2782	Defense Message System (DMS) System Administrator
Officer	
1600	Information Professional
1610	Information Warfare (Information Warfare specialty)
Limited Duty Officers	
6420	Communications and Information Systems
Chief Warrant Officers	
7420	Communications and Information Systems
7430	Chief Warrant Officers (Cyber Warfare)
Marine Corps	
Enlisted	
0212	Technical Surveillance Countermeasures (TSCM) Specialist

Specialty Code	Specialty Title
0551	Information Operations Specialist
0619	Wire Chief
0629	Radio Chief
0651	Data Network Specialist
0659	Data Chief
0689	Information Assurance Technician
0699	Communications Chief
2611	Cryptologic Digital Network Technician/Analyst
2629	Signals Intelligence Analyst
2651	Special Intelligence System Administrator/Communicator
Officer	
0206	Signals Intelligence/Ground Electronic Warfare Officer
0215	Technical Surveillance Countermeasures Trained Counterintelligence/HUMINT Officer
0515	Information Operations Staff Officer
0602	Communications Officer
0640	Strategic Spectrum Planner
0650	Network Operations and Systems Officer
2602	Intelligence/Electronic Warfare Officer
8834	Technical Information Operations Officer

APPENDIX B. BENEFIT TO DOD AND ORGANIZATIONAL SUMMARY

A. APPLICABILITY AND BENEFIT TO DOD

The recipients of the benefits of this work are wide ranging and can be found at every echelon of both the public and private sectors. Those benefiting, based upon an interest in innovation study, have already been discussed.

As for the benefits derived from the organizational product of the innovation study, the seeds of this decades long approach are expected to continue blossoming, becoming ever more observable. The below organizes the current and anticipated benefits according to echelons familiar to those versed in American defense doctrine. It is worth noting that this study used no taxpayer dollars or government support, besides the time allocated to the author and those who advised him.

1. Grand Strategic

At the grand strategic level, the enduring national interests of sustainable prosperity and security are addressed by the output of this study.[74] The MCPA contribution to such national interests is demonstrated by its educational activities focusing on young Americans, a commitment to which is codified with applicable wording in the MCPA mission statement.

2. Strategic

At the strategic level, the MCPA contributes to each of the initiatives listed in the DoD Strategy for Securing Cyberspace. Each is discussed below.[2]

74 Whitehouse, "National Security Strategy" Washington, DC: Whitehouse, 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

a. Strategic Initiative 1

Strategic Initiative 1 reads: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential. This initiative is addressed by establishing an organization of such a broad scope that distinguishes itself by using an understanding of cyberspace as an operational domain as a theoretical point of departure.

b. Strategic Initiative 2

Strategic Initiative 2 reads: Employ new defense operating concepts to protect DoD networks and systems. Discussion forums and journal lend themselves to developing new concepts and ease employment by increased communication between members of this profession network.

c. Strategic Initiative 3

Strategic Initiative 3 reads: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy. Although focused on DoD, the MCPA sets an inclusive tone by inviting partners interested in this area. Members and partners come from across the Federal government, numerous State governments, and the private sector.

d. Strategic Initiative 4

Strategic Initiative 4 reads: Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity. Although focused on the American situation, the MCPA welcomes such partners. For example, shared strength comes from comparing models between partners and collaborative events at chapters located in places like Germany, Japan, and South Korea.

e. Strategic Initiative 5

Strategic Initiative 5: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation. As enshrined in the MCPA mission statement, the organization is dedicated to developing this population. As a product of a purposeful process of innovation, the study is of great value to those interested in a model of successful innovation, especially within government and military.

In support and as a reminder of the aforementioned DoD Strategy for Operating in Cyberspace, from which this work has drawn great inspiration and grounding, a word cloud of the text of the strategy document has been produced and adorns some esprit d'corps items. Word clouds are useful for identifying the most popular words contained in a selection of text (see Figure 28).

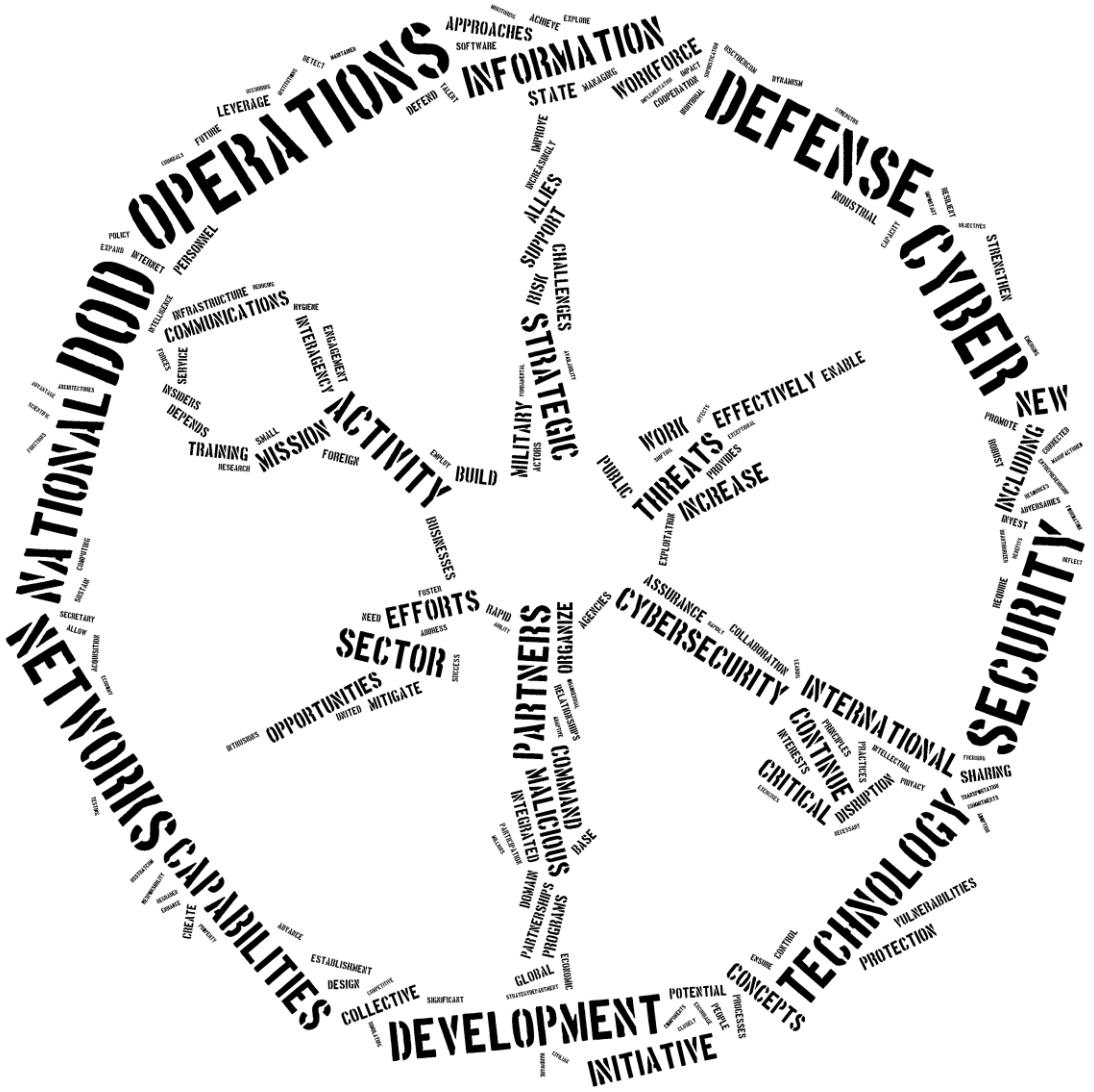

Figure 28. Author produced word cloud of the 2011 DoD Strategy for Operating in Cyberspace, shaped to the MCPA seal.

3. Operational

Numerous operational units and organizations are gaining a more networked workforce. Such an asset can easily leverage expert knowledge and assets from outside of their own organization to accomplish tasks that would otherwise prove more formidable. Such an increase in cross talk channels is expected to reduce duplication of effort on projects, minimizing waste of

organizational budgets and taxpayer dollars. Such benefits have been demonstrated and are discussed in the body of this work.

4. Tactical

Individual members gain tremendously from the opportunity to network with mentors and colleagues from across the joint force. The communitysourced resources have created a repository of professional development, training, and educational opportunities. Tactical applicability has been exemplified by tangible support received by service members deployed to combat zones, resulting from discussions that emerged in MCPA venues.

B. ORGANIZATION SUMMARY

Although components of the MCPA are discussed in the context of each specific practice, a summary of the organization and components is gathered here for the reader's situational awareness.

Founded in Monterey, California during the 2013 fiscal year, the MCPA is a not for profit professional association that is pursuing 501(c)(6) status with the government at the time of this study. The MCPA is dedicated to developing the American MCP and investing in America's future through STEM outreach. Although focused on the American situation, the MCPA is global in nature, with chapters having been seeded wherever a sufficient concentration of DoD personnel are found. Leveraging a cloud based infrastructure, national leadership is highly distributed. The organization is thoroughly joint (Army, Navy, etc.) and interdisciplinary (warfighters, technologists, intelligence personnel, etc.) as such a diverse perspective is needed to understand an entire domain of activity. Components include the following.

1. Members

Members are the strength of the MCPA, fueling activities and connecting to form a new network of professionals. At the conclusion of this study, there were over two hundred members. MCPA members can be found from the

foxhole to the Pentagon, from Afghanistan to Kansas, from junior enlisted service members to flag officers, from each of the military services, from USCYBERCOM, Senate, DHS, allied nations, national laboratories, NSA, State governments, and others.

2. Web Presence

The organization's domain, https://milcyber.org, is the gateway for all subsequent activity. The domain publically communicates the mission, values, goals, and story of the MCPA. It houses member and sponsor processes, online shop, and an Intranet. The Intranet provides an environment conducive to communitysourcing various areas of focus, including a database of professional development opportunities, discussion forum, and projects like developing a Code of Ethics for the profession.

Outside of the MCPA domain, there are other online assets. There is a LinkedIn company page and group, which allows validated members to publically display their affiliation, as is commonplace on the LinkedIn professional network. There is a Facebook fan page and discussion group, allowing for a comfortable venue that is not publically accessible. There is a Zazzle online shop, providing a wide range of customizable esprit d'corps items. There is also a YouTube channel that provides public access to promotional and educational videos.

3. Recognition Program

A critical aspect of focusing and encouraging development of the MCP is the use of incentives, realized in the recognition program. Artifacts familiar to the target population, such as challenge coins and medals, are used to recognize excellence and contributions to the profession, being presented by local leaders.

4. Education Program

The MCPA education program encompasses efforts focused for both internal and external audiences. The efforts for internal consumption include the aforementioned Intranet database, a video series on the development of the

profession, an Android app game encouraging binary and hexadecimal fluency, and resources that inspire innovation like a special interest group for innovators.

The STEM outreach program is a long-term contribution to strengthening the nation's prosperity and security by sparking an interest in STEM topics among K-12 students. The program integrates the recognition program to encourage technically savvy MCPA members to focus their volunteer activities on STEM outreach program in their local community.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

5th Signal Command. “European Cyber Ball commercial.” Accessed July 1, 2013. http://www.youtube.com/watch?v=qOhY-gea0ow, 2011.

Air Force Command, Control, Communications, and Computers Association.“Suggested websites.” Accessed June 1, 2013. http://afc4a.org/Hot%20Links.asp.

Armed Forces Communications and Electronics Association. “Mission Statement.” Accessed January 1, 2013. http://www.afcea.org/mvc.asp.

Association of the U.S. Army, “General Hernandez discusses transforming cyberspace while at war…can’t afford not to.” Accessed June 1, 2013. http://www.ausa.org/meetings/2011/annual/Documents/Presentation_CMF%20LandWarNet%20Hernandez.pdf.

Association of Old Crows. “Mission Statement.” Accessed January 1, 2013. http://www.crows.org/about/mission-a-history.html.

Barabási, Albert-Laszlo. *Linked.* Cambridge, MA: Penguin, 2009.

Bergson, Jr., Arthur W., “The Birth of Armored Forces.” Last modified March 26, 2007. http://www.army.mil/article/2413/.

Capra, Fritjof. *The Web of Life.* New York: Anchor Books, 1996.

Catholicism.org. “Patron Saint for the Internet, Isidore of Seville.” Accessed July 1, 2013. http://catholicism.org/patron-saint-for-the-Internet-isidore-of-seville.html.

Denning, Peter J. and Robert Dunham. *The Innovator’s Way: Essential Practices for Successful Innovation.* Cambridge,MA: The MIT Press, 2010.

Denning, Peter J., and Dennis J. Frailey, *“*The Profession of IT: Who Are We - Now?” *Communications of the Association for Computing Machinery*, 54, no. 6, (June 2011), http://mags.acm.org/communications/201106/?pg=27#pg25.

Department of Defense. “Cyber Operations Personnel Report.” Accessed February 1 2013. http://www.nsci-va.org/CyberReferenceLib/2011–04-Cyber%20Ops%20Personnel.pdf.

Department of Defense. “JP 1–02 Dictionary of Military and Associated Terms.” Accessed August 1, 2013. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Department of Defense, “USCYBERCOM seal.” Accessed February 1, 2013. http://www.defense.gov/home/features/2010/0410_cybersec/images/cybercom_seal_large1.jpg.

Ford, Gary and Normal E. Gibbs, *A Mature Profession of Software Engineering* Software Engineering Institute, Technical Report CMU/SEI-96-TR-004, 1996. http://www.sei.cmu.edu/library/abstracts/reports/96tr004.cfm.

Fort Bliss, “1AD History.” Accessed May 1, 2013. https://www.bliss.army.mil/1AD/.

Hender, Jill. *Innovation Leadership: Roles and Key Imperatives.* London: Grist, 2003.

Hollis, David, “Cyberwar Case Study: Georgia 2008,” *Small Wars Journal*, January 6, 2011. http://smallwarsjournal.com/blog/2011/01/cyberwar-case-study-georgia-20/.

IIED CSUMB,. “Conversion Cruncher App.” Accessed June 1, 2013. http://www.youtube.com/watch?v=jDx8DXtMWg4, 2013.

IIED CSUMB. “Startup Weekend, Military Cyber Professionals Association.” Accessed June 1, 2013. http://www.youtube.com/watch?v=kzdJ_p_5Azg, 2013.

Internal Revenue Service. “Tax-Exempt Status for Your Organization.” Accessed March 1, 2013. http://www.irs.gov/pub/irs-pdf/p557.pdf.

Institute of Heraldry. “101 Military Intelligence Battalion.” Accessed June 1, 2013. http://www.tioh.hqda.pentagon.mil/Heraldry/ArmyDUISSICOA/ArmyHeraldryUnit.aspx?u=3832.

Institute of Heraldry. “1 Armored Division.” Accessed June 1, 2013. http://www.tioh.hqda.pentagon.mil/Heraldry/ArmyDUISSICOA/ArmyHeraldryUnit.aspx?u=3006.

Kuhn, Thomas S. *The Structure of Scientific Revolutions.* Chicago: University of Chicago Press, 1970.

Mills, John R. “The Key Terrain of Cyber,” *Georgetown Journal of International Affairs*, March 2013. http://journal.georgetown.edu/2013/03/23/the-key-terrain-of-cyber-by-john-r-mills/.

Military Cyber Professionals Association. “About.” Accessed March 1,2013. https://milcyber.org.

National Archives. “General Records of the Chief Signal Officer, 1914–18.” Accessed August 1, 2013. http://www.archives.gov/research/guide-fed-records/groups/018.html#18.2.

Nielsen, Michael A., *Reinventing Discovery: The New Era of Networked Science.* Princeton, NJ: Princeton University Press, 2012.

Pellerin, Cheryl, “Critical Cyber Needs Include People, Partners General Says,” *Armed Forces Press Service*, July 2, 2013. http://www.defense.gov/news/newsarticle.aspx?id=120402.

Pentagon. “JP 3–0, Joint Operations.” Accessed June 1, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

Pentagon, “Department of Defense Strategy for Operating in Cyberspace.” Accessed January 1, 2013. http://www.defense.gov/news/d20110714cyber.pdf.

Pentagon. “2012 Army Strategic Planning Guidance.” Accessed December 1 January, 2013. http://www.army.mil/standto/archive/issue.php?issue=2012–04–27.

Pentagon. “2013 Army Strategic Planning Guidance.” Accessed August 1, 2013. http://www.army.mil/standto/archive_2013–02–07/.

Secretary of Defense. “Joint Ethics Regulation.” Accessed January 1, 2013. http://www.dtic.mil/whs/directives/corres/pdf/550007r.pdf.

Stewart, Kenneth A., “Cyber Warriors Professionals Association Another Sign of Evolving Battlefield.” *NPS PAO*, April 8, 2013. http://www.nps.edu/About/News/Cyber-Warriors-Professional-Association-Another-Sign-of-Evolving-Battlefield.html.

Saltzer, Jerome, and Michael Schroeder. 1975. “Protection of Information Computer Systems.” *Proceedings of the IEEE 63*, 9 (September).

Scott, Robert, “New Cyber Warfare Association Will Address Evolving Military Needs,” *Associations Now*, April 12,2013,

http://associationsnow.com/2013/04/new-cyber-warfare-association-will-address-evolving-military-needs/.

U.S. Army Signal Center of Excellence. “Signal Corps Regimental History.” Accessed May 1, 2013. http://signal.army.mil/history/00_wig_wag.html.

Voigts, Scott A., “Organizational Use of a Framework for Innovation Adoption.” Mather’s thesis, Naval Postgraduate School, 2011.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California