The Politics of Social Media in the Department of Defense;

How DoD's Status Changed from Friend to Defriend to Friend Again

Claire E. Cuccio

Dissertation submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

In

Science and Technology Studies

Janet Abbate
Chair
Barbara Allen
Beverly Bunch-Lyons
Saul Halfon

October 8, 2014

Falls Church, VA

Keywords: Social Networking, Department of Defense Policy, DoD Policy, Military

The Politics of Social Media in the Department of Defense;

How DoD's Status Changed from Friend to Defriend to Friend Again

Claire E. Cuccio

ABSTRACT

The introduction of social media presented a significant challenge to the often secretive culture of the U.S. military. DoD struggled with publishing a social media policy forcing the armed services to develop their own policies, which were all inconsistent. When DoD finally established a social media policy in 2007, certain social media sites were banned from the Services' networks for a variety of reasons—the one most often quoted was risk. In February 2010, DoD completely reversed its policy and embraced social media. The new policy required the military to allow open access on the networks to social media for all employees, despite much resistance from internal stakeholders. In this dissertation, I research three significant events during the development of the DoD Social Media Policy: (1) the pre-policy environment, including actions to restrict social media on the DoD networks (2) coming to closure on the current policy and how DoD made its decision to open the networks to social media, and (3) the post-closure period and its ongoing and new tensions. This research project is a qualitative study of the evolution of social media (pre- and post a formal policy) within the DoD through the lens of social construction of technology (SCOT) and a discourse analysis of the policy formulation. My findings indicated that references to security and privacy risk, sociotechnological inevitability, responsible online behavior and youth were particularly important to the military discourse on social media. The study concludes the risk is worth to benefit to service members who want to use social media. Service members accept the sociotechnological inevitability of social media and feel they are responsible enough to use it wisely. The issue of youth was found to be not really a concern and leadership emerged as a discourse and is often referenced to solve any issue that may arise from the use of social media within the military environment.

ACKNOWLEDGEMENTS

Colonel (retired) Barry Hensley, United States Army, mentor and friend, provided the initial inspiration for this dissertation. It originated from a text message I sent him asking advice on a contentious topic to write a National War College paper on. Colonel Hensley immediately called me and suggested this topic. He also provided me introductions to some of the senior DoD leaders I interviewed for this work. Janet Abbate, dissertation advisor and mentor, provided much inspiration and contributions to this work. Every time I hit a roadblock, Janet helped me navigate through the barrier so I could continue on my way. I am grateful to Barbara Allen for grounding me in STS theory and ensuring this work correctly represented the field. Beverly Bunch-Lyons inspired me to use discourse analysis as a method in her Oral History class. Thanks to Saul Halfon who early on gave me guidance that completely reshaped the direction this work was heading and I drew upon his initial thoughts throughout the research process. I'd like to thank the United States Army not only for employing me for the past twenty-five years, but for introducing me to great Americans like Colonel Linda Jantzen, Colonel Dawnlee Walton and all of the other people that agreed to be interviewed for this work. I could not have produced this work without you agreeing to share your stories and experiences. I am indebted to you and I appreciate all the sacrifices you have made for our country. I would also like to thank my running buddies Commander (retired) Terry Waldbeesser, United States Navy, Lieutenant Colonel (retired) Yellixa Cruz, United States Air Force and Kirsten Knapp who have all listened to sections of my dissertation that I was trying to work through while we were out on the running trails at Burke Lake. Thanks to Lieutenant Colonel John Giordano, United States Army, for peer reviews and constructive criticism and to John Garstka who not only provided peer review but allowed me to build on his framework for military capability development. I would like to acknowledge my family: parents, Mike and Mary Cuccio, my sisters Annemarie and Caye, my brother, Colonel Mike Cuccio, USMC, Kevin McLaughlin and Yoly Cuccio for all their love and support over the five years of this journey. Lastly, I would like to thank my husband Lieutenant Colonel Richard Abelkis, who agreed to complete his Masters degree so we could have similar weekend schedules. Richard was always up for a debate and never let on if he was tired of talking about social media. It took a village to complete this work and I am thankful you are all part of my village.

CONTENTS

ABSTRACT……ii

ACKNOWLEDGEMENTS……iii

TABLE OF CONTENTS……....iv

LIST OF FIGURES AND TABLES…….vii

LIST OF ABBREVIATIONS……..viii

MILITARY RANK STRUCTURE……...…..x

CHAPTER 1: INTRODUCTION……...1

1.1 Definition of the Problem…….1

1.2 Research Questions……...2

1.3 Conceptual Framework…….2

1.4 Contributions to Knowledge……4

1.5 Theoretical Framework…….5

1.6 Research Approach and Methodology……14

1.7 Summary of Chapter Contents……15

CHAPTER 2: THE HISTORY OF THE DECISION TO OPEN THE DOD NETWORKS TO SOCIAL MEDIA……...18

2.1 Organization and Structure of the Networks……..19

2.2 Debates and Policy Actions Regarding Social Media……23

2.3 SCOT Analysis……...41

2.4 Relevant Social Groups……..42

2.5 Stabilization, Destabilization, Stabilization……52

CHAPTER 3: A DISCOURSE ANALYSIS OF FACTORS THAT IMPACTED THE SOCIAL MEDIA DECISION……...55

3.1 Discourse and Why We Study It……..55

3.2 RISK ……..59

3.2.1 STS Frameworks for Analyzing the Concept of Risk…….60

3.2.2 Department of Defense Views on Risk……62

3.2.3 Service Members' Views on Risk – Security……..64

3.2.4 Service Members' Views on Risk – Privacy……...75
3.3 SOCIOTECHNOLOGICAL INEVITABILITY……84
3.3.1 STS Frameworks for Analyzing the Concept of Sociotechnological Inevitability…….85
3.3.2 Department of Defense Views on Sociotechnological Inevitability……87
3.3.3 Service Members' Views on Sociotechnological Inevitability……91
3.4 RESPONSIBLE ONLINE BEHAVIOR……...106
3.4.1 Social Science Frameworks for Analyzing Responsible Behavior……108
3.4.2 Department of Defense Views on Responsible Behavior ……110
3.4.3 Service Members' Views on Responsible Online Behavior……..112
3.5 YOUTH……126
3.5.1 Social Science Frameworks for Analyzing Youth……128
3.5.2 Department of Defense Views on Youth……...130
3.5.3 Service Members' Views on Youth……...132
3.6 Chapter Conclusion……...142
CHAPTER 4: A POST POLICY ANALYSIS OF THE EFFECTS OF THE SOCIAL MEDIA POLICY ON THE DEPARTMENT OF DEFENSE……...144
4.1 Changes to the Social Media Policy from Feb 2010 to Sept 2012……...144
4.2 Service Post Policy Actions……..149
4.2.1 Air Force……149
4.2.2 Army……..151
4.2.3 Marine Corps…….155
4.2.4 Navy……...160
4.2.5 Service Comparison……...163
4.3 A Conceptual Framework for Innovative Technology…….165
4.4 A Proposal to Expand Garstka's Model to Include Policy as an Element……170
4.5 Chapter Conclusion……..176
CHAPTER 5: CONCLUSION……...178
APPENDIX A: SERVICE MEMBER INTERVIEW QUESTIONS…….183
APPENDIX B: POLICY MAKER INTERVIEW QUESTIONS……...185

BIBLIOGRAPHY……186

LIST OF FIGURES AND TABLES

FIGURES

Figure 2.1: Organization and Structure of the DoD Networks 2010……22

Figure 4.1: Garstka's Revised Four Element Model……..…166

Figure 4.2: Technology Innovation Leading……..…168

Figure 4.3: Process Links Up With Technology…….....169

Figure 4.4: Initial Operating Capability……..…169

Figure 4.5: Absence of Policy Blocks Progress to Organization and Process……170

Figure 4.6: Expanded Five Element Model……171

Figure 4.7 Policy Holds Back Process and Organization……...……172

Figure 4.8 Social Media in DoD at Stabilization/Closure……..176

TABLES

Table 4.1 Changes in DoD Social Media Policy from Feb 2010 to Sept 2012……...…...146

LIST OF ABBREVIATIONS

AFCENT	Air Force Central Command
ANT	Actor Network Theory
AOR	Area of Responsibility
ARNG	Army National Guard
ASD	Assistant Secretary of Defense
ATM	Automated Teller Machine
CG	Commanding General
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CNO	Chief of Naval Operations
CNO	Computer Network Operations
COC	Command Operations Center
COCOM	Combatant Command
COMSEC	Communications Security
CONUS	Continental United States
CSTC-A	Combined Security Transition Command-Afghanistan
DARPA	Defense Advanced Research Projects Agency
DASD	Deputy Assistant Secretary of Defense
DEPSECDEF	Deputy Secretary of Defense
DHS	Department of Homeland Security
DTM	Directive Type Memorandum
DISA	Defense Information Systems Agency
DoD	Department of Defense
DODI	Department of Defense Instruction
FOB	Forward Operating Base
FRG	Family Readiness Group
G3	General Staff Operations Officer
GIG	Global Information Grid
GPS	Global Positioning System
IA	Information Assurance
IAP	Internet Access Point
IC	Intelligence Community
IED	Inprovised Explosive Device
IRB	Institution Review Board
ISP	Internet Service Provider
IT	Information Technology
JCS	Joint Chiefs of Staff
JNCC-A	Joint Network Command Center-Afghanistan
JTF-CND	Joint Task Force-Computer Network Defense
JTF-CNO	Joint Task Force-Computer Network Operations
JTF-GNO	Joint Task Force-Global Network Operations
KIA	Killed In Action
LOL	Laugh Out Loud
MARADMIN	Marine Administrative

MCEN	Marine Corps Enterprise Network
MIT	Massachusetts Institute of Technology
MRAP	Mine Resistant Ambush Protected
MTV	Music Television
MWR	Morale, Welfare and Recreation
NDAA	National Defense Authorization Act
NII	Networks and Information Infrastructure
NIPRNET	Non-secure Internet Protocol Router Network
NOC	Network Operations Center
NOSC	Network Operations and Security Center
NSA	National Security Agency
OCS	Officer Candidate School
ODM	Operational Directive Memorandum
OPFOR	Opposing Force
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OUSD(AT&L)	Office of the Undersecretary of Defense (Acquisition, Technology, & Logistics
PA	Public Affairs
PAO	Public Affairs Officer
PSA	Principal Staff Assistant
RC	Regional Command
ROTC	Reserve Officers Training Corps
SES	Senior Executive Service
SMS	Short Message Service
TOC	Tactical Operations Center
TTP	Tactics, Techniques and Procedures
SASC	Senate Armed Services Committee
SCOT	Social Construction of Technology
SECDEF	Secretary of Defense
SNS	Social Networking Services
STS	Science and Technology Studies
SWA-TNOSC	Southwest Asia-Theater Network Operations and Service Center
TNOSC	Theater Network Operations and Security Center
UCMJ	Uniform Code of Military Justice
USCYBERCOM	United States Cyber Command
USMC	United States Marine Corps
USSTRATCOM	United States Strategic Command
VPN	Virtual Private Network
VTC	Video Teleconference

MILITARY RANK STRUCTURE
(from lowest to highest)

OFFICER (U.S. Army, U.S. Air Force, U.S. Marine Corps/Navy)

Cadet/Midshipman (Reserve Officer Training Corps (ROTC) or Service Academy)
Second Lieutenant/Ensign
First Lieutenant/Lieutenant Junior Grade
Captain/Lieutenant
----------separation between company grade and field grade officer----------
Major/Lieutenant Commander
Lieutenant Colonel/Commander
Colonel/Captain
Brigadier General/Rear Admiral Lower Half
Major General/Rear Admiral Upper Half
Lieutenant General/Vice Admiral
General/Admiral

ENLISTED (U.S. Army/U.S. Air Force/Navy/U.S. Marine Corps)

Private/Airman Basic/Seaman Recruit/Private
Private E2/Airman /Seaman Apprentice/Private First Class
Private First Class/Airman First Class/Seaman/Lance Corporal
Specialist, Corporal/Senior Airman/Petty Officer Third Class/Corporal
Sergeant/Staff Sergeant/Petty Officer Second Class/Sergeant
Staff Sergeant/Technical Sergeant/Petty Officer First Class/Staff Sergeant
-----separation between junior noncommissioned officer and senior noncommissioned officer-----
Sergeant First Class/Master Sergeant/Chief Petty Officer/Gunnery Sergeant
Master Sergeant/Senior Master Sergeant/Senior Chief Petty Officer/Master Sergeant
Sergeant Major/Chief Master Sergeant/Master Chief Petty Officer/Master Gunnery Sergeant

CHAPTER 1

INTRODUCTION

The introduction of social media presented a significant challenge to the often secretive culture of the U.S. military. The public nature of social media presented a new openness to the military and its members struggled with the terms of social media use in the absence of policy. There was much debate regarding its use and value within a military environment. At first, no social media policy existed at the DoD level and the armed services developed their own independent policies, which were completely dissimilar. When DoD finally established a restrictive social media policy in 2007, certain social media sites were banned from the Services' networks for a variety of reasons—the one most often quoted was risk. In February 2010, DoD completely reversed its policy and embraced social media, an event that was a surprise to many service members. The new policy required the military to allow open access on the unclassified networks to social media for all employees, despite much resistance from internal stakeholders any many top general officers.

1.1 Definition of the Problem

The reasons for the sudden policy shift are the basis of this dissertation. Because of the reversal in policy, the use of social media in the military has increased dramatically over the past several years, but the controversy has not dissipated. Some service members believe social media is a powerful technology that cannot be stopped and liken its introduction into society and the military to a tsunami.[1] Others believe social media is a danger to our troops and it will only take one significant incident for the military to restrict its future use on military networks.[2] I

[1] Interview with Army Colonel, November 8, 2011.
[2] Interview with USMC Lieutenant Colonel, October 27, 2011.

believe the discourse surrounding the policy debate significantly affected the outcome of the policy decision to both restrict and then allow social media on the DoD networks.

1.2 Research Questions

In this project I researched three significant events, (1) the pre-policy environment, including actions to restrict social media on the DoD networks (2) coming to closure on the current policy and how DoD made its decision to open the networks to social media, and (3) the post-closure period and its ongoing and new tensions. The central research questions for this dissertation apply to all of these events in an effort to ascertain how the four major discourses I have identified, surrounding military social media, shaped the current policy. The questions were:

(1) How have the initial and post-policy debates on social media and the military been shaped by competing discourses of security and privacy risk, sociotechnological inevitability, responsible online behavior and youth?

(2) What are the relationships among the discourses and how do they affect views of policy?

1.3 Conceptual Framework

This research project is a qualitative study of the evolution of social media (pre- and post a formal policy) within the DoD through the lens of social construction of technology (SCOT)[3] and a discourse analysis of the policy formulation. My research indicated that references to security and privacy risk, sociotechnological inevitability, responsible online behavior and youth were particularly important to the military discourse on social media. DoD's social media policy completely reversed over the course of three years. In this dissertation, I analyzed the reasons for the policy reversal by examining the discourse of STS and social science scholars, DoD

[3] SCOT is a theory started by Pinch and Bijker under the theory that "society is an environment where technologies develop."
Langdon Winner. "Social Constructivism, Opening the Black Box and Finding It Empty," Conference Proceedings, Biennial Conference of the Society for Philosophy and Technology, Mayaguez, Puerto Rico, March 1991 435.

publications, and service member interviews. I concentrated my research on how the DoD came to closure on the decision to first restrict the use of social media on DoD networks; the decision to mandate opening the networks to social media; and finally the debate within the post-closure period over the sufficiency of the policy. I also propose a framework for social media capability development and show how absence of policy impeded the development and acceptance of a social media capability for the DoD. I integrated SCOT with discourse analysis to discover the underlying assumptions surrounding the social media debate and portrayed how these beliefs limited policy actions.

Since I started this project, the social media policy enacted in February 2010 has been amended twice. The policy seems to be in a current state of closure, and the number of military members using social media is ever increasing. There are many different ways service members use social media: personal use- e.g. keeping in touch with their families while deployed; official use- e.g. recruiting or public affairs information sites; and a blend of off-duty and on-duty use, e.g. official military unit sites where they can obtain current events information or keep in touch with old friends. Yet, even though some senior leaders embrace it, there is a concern by others that the risk of using the technology is not worth the benefit. This dissertation provides a better understanding of how most military members accepted and use social media while also explaining the ongoing tensions over tradeoffs between openness and security. As the use of social media by service members evolves, this study will strengthen the knowledge base to inform future policy decisions by the Department of Defense.

My research is informed by my expertise and experience from twenty five years of working in network security jobs in the United States Army. The advent of internet use and the DoD's subsequent dependence on the network evolved during my entire career. I have worked at

various levels of the network. As a young officer in Germany in 1989, my job was providing communications services, including the newly minted internet to customers on a military base. At that time, there was no security on the unclassified networks and no social media existed. I also worked at the Defense Information Systems Agency (DISA) and Joint Task Force Global Network Operations (JTF-GNO) in 2004, where my role was at the supervisory and policy level. In my last job at the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)) in 2014, I researched and recommended the acquisition of cyber technologies and provided input to DoD level cyber policy based on evaluating the risks presented to the networks. One of the policies I reviewed was the 2012 (most current) social media policy. Currently, I am back to operating and defending Army networks as the Senior Operations Officer for the 311th Signal Command in Hawaii, where I am responsible for the operations and security of Army networks in Hawaii, Alaska, Japan, Korea and Guam.

1.4 Contributions to Knowledge

I chose a qualitative study because a gap existed in the research on social media, especially as it pertains to the military. In 2010, social media was a new technology for DoD with emerging policy issues. Most scholarship on social media at the time did not address the military experience, while the majority of the existing work was focused on the need for a consistent policy throughout the DoD. The DoD released an initial social media policy in February of 2010 and two subsequent updates on July 15, 2012 and September 11, 2012. The events that occurred leading up to the release of the social media policy has never been documented until now and there still exists a debate about the security and privacy of social media, and the usefulness of social media to military operations. As the DoD policy evolved, service members temporarily had to develop their own standards of conduct while using social media. My interviews identify

the dominant discourses in this debate and assist in showing how the discourse framed social media policy choices.

My study of military use of social media is unique in that it provides evidence of the underlying, continuing tensions (e.g. through discursive inconsistencies and contradictions) that show that the initial closure of the social media policy was not stable. These tensions undermined the initial restrictive policy, and ultimately led to reversing the policy to one where the use of social media on the DoD networks was mandated. Studying the social media policy decisions in the DoD broadens Science and Technology Studies (STS) scholarship on social media by examining discourses of risk, identity (youth), and personal agency (responsible behavior) within a military rather than commercial or recreational environment.

1.5 Theoretical Framework

My intent for this dissertation was to integrate SCOT with discourse analysis to show how the DoD's social media policy achieved closure and especially how the stability of that closure was undermined by continuing tensions and contradictions. I examined the discourse surrounding the debate to open the military networks to social media in several areas: risk to security and privacy, sociotechnological inevitability, responsible online behavior and youth. I explored the conditions surrounding the pre- and post-policy decisions of opening the military networks to social media from the STS perspective of social construction.

In SCOT, relevant social groups shape the direction of invention. Pinch and Bijker describe the result as a multi-directional model in which some variants "die out" and others "survive."[4] In the next two chapters, I will show the relevant social groups headed by military generals "die

[4] Trevor J. Pinch and Wiebe E. Bijker. "The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other," in *The Social Construction of Technological Systems*, ed. Weibe E. Bijker, Trevor Pinch, and Thomas P. Hughes. Cambridge, MA: MIT Press, 1987, pp. 17-50.

out" as they lose their battle for restriction of social media on DoD networks. The social groups headed by DoD civilians will "survive" as they emerge victorious from their battle with the generals for allowing social media on military networks. Interpretive flexibility means not only that people have different ways of perceiving social media, but also that there were multiple options for a final solution. Peoples' positions on the topic were clearly based on their job responsibilities. Those responsible for operating and defending the networks wanted to ban social media use while those who did not have direct responsibility for network operations were supporters of the use of social media. In fact, in the beginning, the generals were able to restrict social media on military networks and were aiming for a more stringent policy. But not all generals agreed with that approach; two of the Service leads (Air Force and Navy) charged their organizations with figuring out how to utilize social media effectively. The decision to open the networks could have been either permissive or more restrictive. The discourse surrounding the debate influenced arriving at stabilization and a signed social media policy. SCOT is also a methodology and provides a framework in which to study the acceptance or rejection of a technology by society. I started with Pinch and Bijker's framework in chapter 2, The History of the Decision to Open the DoD Networks to Social Media, to study the history of social media in the military using the interpretive flexibility of the possible courses of action, the relevant social groups involved and explored the conflicts that arose. Unlike Pinch and Bijker, I did not conclude my analysis at stabilization and closure. As Langdon Winner points out, the social construction approach is too narrow and the studies rarely explore the consequences of technical choice on society.[5] My study looks beyond the closure of publishing the new social media policy in 2010 and explains how the social media has transformed service members' personal

[5] Winner, 438.

conduct and social relations in the years since the decision was made. This analysis helps to frame the context for the development of future DoD social media policy.

In applying the SCOT notion of closure to the DoD social media decision, I borrowed from actor network theory (ANT) the idea of "normalization," in which the stability of the system is "achieved by standardizing and constraining actors and intermediaries."[6] The military uses orders and policies to enforce control over service member behavior. In 2007, the generals ordered the network operators to restrict access to many social media sites in order to constrain the use of social media. Normalization is similar to Pinch and Bijker's closure, but it allows for what Callon calls "retranslation," which is the possibility of the network to destabilize and restabilize as something else based on the conflict and discord of the actors.[7] When I first started researching social media in the military in 2010, DoD was revisiting the social media policy based on two relevant incidents. The Staff Judge Advocate of the U.S. Marine Corps sent a request to Congressman Duncan Hunter (R-CA) to amend the social media directive after a Marine was punished for a negative posting about President Obama.[8] In the other incident, a military dating site was hacked exposing the usernames and passwords of subscribers with ".mil" email addresses.[9] The actor-network was unstable at that time and the policy was under review by many of the same actors involved in the decision. At such a time of uncertainty, there was a possibility the actor-network could transform and restabilize into a different policy, which it did rather quickly, despite fierce opposition from senior general officers.

---

[6] Michel Callon"Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fisherman of St. Brieuc Bay, in J. Law, *Power, Action, and Belief: A New Sociology of Knowledge?*, London, Routledge, 1986, p.151.
[7] Callon, 150.
[8] Gina Harkins, "Marines Seek Guidance on Social Media After Anti-Obama Posts," *Marine Corps Times*, April 7, 2012.
[9] Kevin McCaney, "Pentagon To Update Rules for Using Commercial Social Media Sites," *Government Computer News*, May 29, 2012.

I also drew from systems theory the concept of technological momentum. Social media in the military is currently progressing from mostly social uses to some operational functions. It is becoming not only accepted, but relied upon, for intelligence uses. Social media has a current momentum that may not allow a radical solution such as banning it from military networks. The momentum of social media in DoD helps explain why the discourse of sociotechnological inevitability is so common. In front of Congress, the DoD CIO, Mrs. Teri Takai, said information sharing was an expectation,[10] rather than a benefit. Reknown counter-insurgency expert Lieutenant Colonel (retired) John Nagl claims military officers who embrace social media will have success.[11] The great forward momentum of social media in society influenced the desire of the members of the military to utilize social media. It is important to study the discourse surrounding the social media debate to discover why people who just started using social media quickly developed a dependence on it.

There is a fascinating gap between what people say about their conduct on social media and what they actually do. This can highlight internal conflict and create subsets within a social group or even individual dissent from the group position. One way to explore these tensions and inconsistencies is through discourse analysis. The author of *A Closed World* and an expert in discourse analysis, Paul Edwards, claims discourse is the "act of conversation, as distinguished from the language itself."[12] In my research, four themes clearly emerged from the discourse of social scholars, DoD publications, and service members: the risk to security and privacy, sociotechnological inevitability, responsible online behavior and youth. Edwards also said, the

[10] Takai, Teresa M. "Improving Management and Acquisition of Information Technology Systems in the Department of Defense," *Statement for the Record, House Armed Services Committee on Emerging Threats and Capabilities*, Washington, DC, April 6, 2011.
[11] Gordon Lubold. "Military Brass Joins Wired Troops." *Christian Science Monitor*, Boston, MA, January 21, 2009.
[12] Paul N. Edwards, Paul N. *The Closed World: Computers and the Politics of Discourse in Cold War America.* Cambridge, MA: MIT Press, 1997, 34.

analytic term "discourse analysis" descends from the sociological studies of speech.[13] I interpret this to mean, a discourse analysis examines how people construct their ideas and experiences using language. Dr. Eamon Fulcher, a cognitive behavioral psychologist at the University of the West in England, believes, it is based on the assumption that peoples' views are affected by culture and society and conclusions can be drawn by studying the themes which emerge in them.[14] You will see in the next two chapters how social media acceptance in society directly influenced the discourse and acceptance of social media by the DoD. Common features studied in discourse analysis can include: recurring themes, inconsistencies, assigning blame, and references by many people to a single event. Fulcher concludes social constructionists regularly use discourse analysis to portray a particular reality to the best extent possible.[15] I believe the discourse surrounding the DoD social media debate will help reveal how the social media policy came to closure.

There are two different types of interviewees in my dissertation—policy makers and service members. I used different questions and modes of analysis for each group. University of Western Ontario Professor Bernd Frohmann's research methods in library and information science were useful when looking at the speech patterns of policy makers,[16] while Tampere University's Professor Sanna Talja's methods were useful for analyzing both policy makers' and service members' statements. Frohmann states that rhetoric about technology does not describe the actual technology, but how it came to be in its current form and how people understand and use it.[17] I would add to Frohmann's statement that the rhetoric not only shapes the technology,

[13] Edwards, 34.
[14] Dr. Eamon Fulcher. "What is Discourse Analysis?" eamonfulcher.com, 2012.
[15] Ibid.
[16] Bernd Frohmann. "Discourse Analysis as a Research Method in Library and Information Science." Library and Information Science Research 16 (1994): 119-138.
[17] Baym, Nancy K. *Personal Connections in the Digital Age*. Malden, MA: Polity Press, 2010, 43.

but how society changes because of peoples' reaction to the technology. Rather than trying to argue that participants in the social media debate are right or wrong, a matter that will never be settled, Frohmann encourages analysts to focus on the existence of the dialogues of the debate and discern the politics and motivations involved in the arguments.[18] Frohmann focuses on institutional platforms and professional or corporate talk as major influencers in the construction of policy. He believes that the ideas within policy makers' speech "gain autonomy by passing an institutional test"[19] and are therefore more readily accepted by the affiliated society. I studied the statements made by DoD policy makers, in person and in existing publications, to identify general characteristics of DoD institutional discourse and then explored if these themes emerged in their discussion of social media. There are many select word choices that associate social media issues with the DoD such as, "securing the perimeter,"[20] "the enemy is watching,"[21] or as the President said, "a [potential] weapon of mass destruction."[22] By referring to security in familiar military terms, some policy makers tried to make their arguments against the use of social media more persuasive.

For all of the interviews conducted, I used the approach described by Talja to compile themes concerning the unresolved tensions with the current policy. Talja provided a useful framework for qualitative interviews where she says not to focus on individual thoughts about a subject, but rather on broad regularities in participants' accounts of a subject.

[18] Palmquist, Ruth. University of Texas at Austin, Graduate School of Library and Information Science, Author's webpage. Accessed 6 May 2012 at: http://www.ischool.utexas.edu/~palmquis/courses/discourse.htm.
[19] Frohmann, 120.
[20] Joe Gould. "Army Expands Warnings on Social Networking," Army Times, September 26, 2011.
[21] Cheryl Rodewig. "Social Media Misuse Punishable Under UCMJ," U.S. Army, Ft Benning, GA, Feb 9, 2012.
[22] The White House. "Remarks By the President on Securing Our Nation's Cyber Infrastructure," Office of the Press Security, May 29, 2009.

Talja suggested three possible approaches for analyzing discourse.[23] First, a researcher must search for inconsistencies and internal contradictions in one interviewee's statement. Second, to identify repeatable explanations and arguments across interviewees' statements, and lastly, find the basic assumptions and starting points underlying the select arguments. My interviews contained many examples of Talja's first approach of exploring inconsistencies. Most of the interviewees said they were concerned about security, but not one had ever read the privacy statements on social media sites and most were truly not aware of exactly what data a particular social media site collected and distributed about them. As an example, a Marine Lieutenant Colonel started the interview with a completely negative view of social media and stated how it is of no use to him. He spent the rest of the interview telling me how useful Facebook was as a tool when he was a Battalion Commander in Afghanistan.[24] There were similar contradictions in many of my other interviews. This suggests there were underlying conflicts of interest or conflicts between norms and desires, and the service member's discourse was an attempt to reconcile or explain away those conflicts.

There is a shared discourse including background and terminology that most everyone in a given social group adheres to even if they disagree on some specific points. This shared, unquestioned set of beliefs facilitates peoples' central understanding of a subject, it makes it easier for people to relate to each other, but also limits the terms of the debate.[25] I used Talja's second approach to find the commonalities across the interviews. Statements such as, "I do (or do not) need social media to keep in touch with my friends" and "Every piece of information that you put online is no longer private," were common declarations. Talja's third approach was to

[23] Sanna Talja. "Analyzing Qualitative Interview Data: The Discourse Analytic Method," University of Tampere, Finland, 9.
[24] Marine Lieutenant Colonel, interview by author, Washington, DC, October 27, 2011.
[25] Edwards, 34.

find the assumptions underlying the arguments such as, "Service members want to use social media" or "Youth are irresponsible." The commonalities and underlying assumptions can show why some policy choices are favored while others are unimaginable or difficult. They also can define the boundaries within the discourse and possibly narrow the argument. Understanding how the present discourses function can help policy makers decide if DoD needs to change the discourse in order to become more consistent and arrive at a more acceptable policy.

Talja believes a discourse analysis is meant to derive the macrosociological interpretations of a topic.[26] As such, the results of qualitative interviews can be triangulated amongst other research materials, publications and institutional artifacts to discover consistencies in the formation of knowledge.[27] I used this method in my dissertation by exploring common statements found in social science publications, DoD publications and the media regarding the understanding of security and privacy risk, socioinevitability of the technology, what it means to be responsible online, and the characteristics of youth in regards to social media. I analyzed these sources for each of the four discourses and correlated them with service members' discourses on the same topics. Recurring views on the understanding of security and privacy risk can be characterized by some generalizations as well. On one extreme, social media "has future operating challenges of a traditional, irregular, catastrophic or disruptive nature" and "has ramifications for U.S. national security."[28] There is said to be a central problem of anonymity—people cannot trust other people to be who they say they are.[29] Security is often cited as a reason to assert strict hierarchy and control[30] and it is suggested there may be a possible justification for

[26] Talja, 13.
[27] Talja, 14.
[28] Linton Wells II and Mark Drapeau. Social Software and National Security, An Initial Net Assessment, Washington, DC: National Defense University, April 2009, 1.
[29] Baym, 32.
[30] Milton L. Mueller. Networks and States; the Global Politics of Internet Governance. Cambridge, MA: MIT Press, 2010, 159.

the suspension of civil liberties.[31] There are also people who are not as concerned about security. They believe nothing on the internet is secure and ask why bother trying to control it?[32] These are examples of how risk is assumed to be more important than communication or civil liberties; and, also of how claims about sociotechnological inevitability can disrupt arguments about the need for more security. The risk discourse became weaker over time as the generals traded it for social media as a waste of time or a bandwidth waster.

Common views on the inevitability of social media technology are that the [U.S] "government ignores social media at its peril"[33] and "failure to adopt [social media] tools may reduce an organization's capabilities over time."[34] Another view is that people just accept the digital footprint social media can leave behind and people are tracked everyday electronically by technology such as passport readers, ATM machines, sensors and bar codes-they barely notice it anymore.[35] Such statements exemplify the discourse of sociotechnological inevitability. The military discourse was significantly more focused on security risk than the civilian discourse, which leaned towards sociotechnological inevitability.

The statements centering around youth often overlap those of responsible online behavior and focus on the inability of youth to be responsible. Baym believes the fear about youth arises from a parental anxiety of losing control over children and that concerns about safeguarding children are coming in the wake of any new communication medium.[36] This apprehension is often transferred to the technology, not associated with the people and may explain why policy makers focus on limiting technological access rather than educating users on the "responsible" use of

[31] Mueller, 160.
[32] Marine Lieutenant Colonel, interview by author, Washington, DC, October 27, 2011.
[33] Wells and Drapeau, 1.
[34] Wells and Drapeau, 1.
[35] David Lyon. "Surveillance Technology and Surveillance Society," in Modernity and Technology, ed. Thomas J. Misa, Philip Brey, and Andrew Feenberg. Cambridge, MA: MIT Press, 2003. Print, p. 172.
[36] Baym, 43.

technology. Youth are seen as more likely to be irresponsible with spending by running up a large phone bill or losing their mobile handset.[37] Another argument that reveals the assumption that young people are a unique, problematic, social group is that social media is something youth will not live without. There is a stated fear that young people will not work for the government if the government does not adopt modern methods like social networking.[38] I consistently found themes of security and privacy risk, sociotechnological inevitability, responsible online behavior and youth woven into my interviews and the larger social media discourse found in other sources.

1.6 Research Approach and Methodology

As mentioned previously, to explore the use of social media in the military, I used qualitative interviews conducted with members of the military and DoD officials in positions to influence policy. I interviewed approximately sixty people total from the DoD, Army, Navy, Air Force and Marines in all different military specialties, i.e. pilots, infantry, surface warfare officers, intelligence, communications, etc. Some of the policy makers were DoD civilians as well. I classified youth as thirty years of age and younger. I chose thirty years old as the cutoff point because that is about the time a soldier transitions from a junior to a senior noncommissioned officer or a company grade officer to field grade officer. Senior noncommissioned officers and field grade officers are place in positions of greatly increased responsibility for personnel, property and operations. I varied the interviewees based on age and rank. Since I am currently on active duty in the military and worked at the Pentagon during the research phase of this project, I had access to service members in all branches of the military. Most of the Pentagon

[37] Jack Linchuan Qiu. Working Class Network Society: Communication Technology and the Have-Less in Urban China. Cambridge, MA: MIT Press, 2009, 133-134.
[38] Jim Garamone. "Lynn Discusses Social Media at Facebook Headquarters," American Forces Press Service, April 28, 2010.

employees were senior leaders. To capture the youth view, I went to Fort Belvoir, VA; Joint Base Myer-Henderson Hall, VA; Fort Lewis, WA; and Fort Shafter, Hawaii. I also conducted three phone interviews with deployed service members in Afghanistan and one with a soldier deployed to Iraq. The questions I asked revolved around their personal use of social media and how they make decisions on sharing or restricting different types of information.[39] Service members remained anonymous throughout the study and are referred to by their rank and specialty, unless I am quoting a statement from a public source or they otherwise gave me permission.

Of the sixty people interviewed, nineteen were senior officials involved in DoD policy at the time the social media policy was debated and signed and seven were from the 2014 post-policy environment. I questioned the subjects on how the social media policy was created, what the debate was in the DoD at the time, and what the future held for social media policy.

1.7 Summary of Chapter Contents

In this project I researched three significant events during the development of the DoD Social Media Policy: (1) the pre-policy environment, including actions to restrict social media on the DoD networks (2) coming to closure on the current policy and how DoD made its decision to open the networks to social media, and (3) the post-closure period and its ongoing and new tensions. Chapter two, the History of the Decision to Open the DoD Networks to Social Media, focuses on SCOT and a history of the pre-policy environment. It begins with the organization and structure of the DoD networks, which is necessary in order to understand the relevant social groups and their positions in the social media debate. I explore the initial position of the Services in the debate and the process the DoD used in order to come to the initial closure of

[39] Questions appear in Appendix A.

banning most social media sites from DoD networks. Next, I focus on the actual debate and the concerns of the various social groups from their viewpoints. Chapter two wraps up with the destabilization or the restrictive policy and the timeline to closure of the final policy which is exactly opposite the initial policy. Chapter three, a Discourse Analysis of Factors that Impacted the Social Media Decision, explores the discursive threads involved in this project, surrounding security and privacy risk, sociotechnological inevitability, responsible online behavior and youth. I research different viewpoints on each thread: social and STS scholar publications, DoD publications, and service member interviews. Chapter three uses discourse analysis to portray the concern over security and the perceived risks involved with using social media. It showcases the struggle between security and keeping up with the civilian sector and how service members struggle with responsible online behavior in their official and personal roles. The youth discourse is completely inconsistent, yet youth are widely considered the reason for DoD changing the social media policy to be more permissive. Chapter three shows how the discourses interrelate and compete with each other for dominance to support each social group's official position. Chapter four, a Post-Policy Analysis of the Effects of the Social Media Policy on the DoD, examines the changes to the social media policy over time and the current social media status on each Service's networks. It shows that social media use is thriving within the DoD and leaders are advocating an even larger role for social media use with in DoD. I propose an amendment to an existing conceptual framework for DoD capability development that includes policy as one of its pillars. This dissertation shows the absence of policy hindered the organization and processes associated with social media use within the DoD. The final chapter concludes the risk is worth to benefit to service members who want to use social media and how the risk discourse loses prominence as an argument over time. Service members accept the

sociotechnological inevitability of social media and feel they are responsible enough online to use it wisely. The issue of youth was found to be not really a concern and leadership is relied on to solve any issue that may arise from the use of social media.

CHAPTER 2

THE HISTORY OF THE DECISION TO OPEN THE DOD NETWORKS TO SOCIAL MEDIA

Before we can understand the effects of social media on the DoD's networks, it is important to understand the context and the organizations responsible for operating and defending the networks and some of the issues associated with the use of social media. This chapter will introduce the organization and structure of DoD networks, describe debates and policy actions involving social media (pre-policy), and present a SCOT analysis and a systems analysis of the DoD social media policy debate. The time period covered in this chapter is from 2006 to February 2010. Social media is a relatively new form of communication that includes mobile and web-based technologies that utilize the internet to provide a forum for personal interaction. Leading social media scholars, Ellison and Boyd, define social networking sites as, "A networked communication platform in which participants 1) have uniquely identifiable profiles that consist of user-supplied content, content provided by other users, and/or system-provided data; 2) can publicly articulate connections that can be viewed and traversed by others; and 3) can consume, produce, and/or interact with streams of user generated content provided by their connections on the site."[40] Social media offers users the ability to communicate one-to-many in which one posting can be read and commented on by many people.

The push for social media originated at the top of the U.S. government. On his first day in office in 2009, President Barack Obama released a memorandum that said, "My Administration is committed to creating an unprecedented level of openness in Government. We will work together to ensure the public trust and establish a system of transparency, public participation,

[4040] Nicole Ellison and Danah Boyd. "Sociology Through Social Networking Sites," in Dutton, W.H., *The Oxford Handbook of Internet Studies*, Oxford: the Oxford University Press, pp. 158.

and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in Government."[41] Through the Open Government Initiative, Departments and Agencies were directed to explore technologies to allow public participation and feedback on government policy.[42] The Obama Administration's goals on open government are transparency, public participation, and collaboration. In regard to transparency, Departments and Agencies were directed to make unclassified information available on operations and decisions and solicit input from the citizens. Collaboration is meant for Departments and Agencies to collaborate with other government Agencies, nonprofit organizations, businesses, and individuals in the private sector.[43] Federal Departments and Agencies quickly embraced commercial social networking sites because the infrastructure was already existing, use of the commercial sites incurred no additional monetary investment or support, and these social networking sites were an easy way to disseminate information, involve the public, and collaborate amongst different entities in compliance with President Obama's Open Government Initiative.

2.1 Organization and Structure of the Networks

The Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD NII/DoD CIO) is the SecDef's Principal Staff Assistant (PSA) for the policy and oversight of information resources management, to include matters related to information technology (IT), network defense, and network operations.[44] U.S. Strategic Command (USSTRATCOM), a functional Combatant Command (COCOM), is

[41] The White House. "Transparency and Open Government." *Memorandum from President Barack Obama*. Jan. 21, 2010.
[42] Wendy R. Ginsberg. *The Obama Administration's Open Government Initiative: Issues for Congres*s. Washington, DC: Congressional Research Service, August 17, 2010.
[43] Ibid, 8.
[44] www.disa.mil

responsible for the operation and defense of the DoD Global Information Grid (GIG)[45] which consists of all the DoD networks. Both the ASD NII/DoD CIO and the Commander, USSTRATCOM report to the SecDef. The ASD NII/DoD CIO is responsible for IT policy, while USSTRATCOM is responsible for operations and defense on the DoD networks. Both organizations supervise the Defense Information Systems Agency (DISA), who actually operates and maintains the backbone of the GIG, under different areas of U.S. Code; the ASD NII/DoD CIO under Title 40 (Public Buildings, Property and Works) U.S Code and USSTRATCOM, under Title 10 (Armed Forces). Sometimes these roles overlap.

DISA is a Combat Support Agency headquartered at Fort Meade, MD which provides the enterprise information infrastructure necessary to operate and maintain the DoD's networks.[46] DISA has a presence all over the globe and is at the top of a hierarchical wide area network connecting U.S. military in various countries around the world. It also connects the DoD to the rest of the internet. The four military Services (Army, Navy, Air Force, and Marine Corps), regional Combatant Commands and other subordinate organizations like the U.S. Army Corp of Engineers or U.S. Army Medical Command all operate their own networks below the DISA backbone. Even though DISA is above the Service and Agency networks in a hierarchical structure, DISA has little physical and technical control over how the independent networks conduct operations.

While DoD originated the Internet and had been using it for almost three decades, the advent of the world wide web and social media in the 1990s created new security risks for which DoD was not prepared. Previously, DoD's main concern was penetrations by external, unauthorized

[45] Chairman of the Joint Chiefs of Staff Memorandum, "Distribution of the Unified Command Plan 2008 (UCP 08)," Washington, DC, Dec. 23, 2008.
[46] www.disa.mil

users; the new media introduced another concern, risky behavior by DoD's own authorized users. The DoD decided to create an organization to meet the need using a standing Joint Task Force (JTF). The Department created the JTF – Computer Network Defense (JTF-CND) in 1998 to merge the network experts with DoD law enforcement and intelligence communities to direct the defense of the networks as a single entity.[47] Over the next five years, the organization matured and changed its name to JTF-Computer Network Operations (JTF-CNO) and then JTF-Global Network Operations (JTF-GNO) representing an evolution in roles and responsibilities of network defense. JTF-GNO was the relevant military organization responsible for defending the DoD's network infrastructure during the debate and at the time of social media decision in 2010. The JTF-GNO directs operations across the DoD networks using a series of electronic operational messages which contain instructions and directions to Department network providers at all levels. JTF-GNO conducts both offensive and defensive operations.[48]

Operational responsibility for DoD networks is split among the individual Services and Agencies, which operate their own local area networks, and DISA, whose global backbone connects the Service networks to each other and to the rest of the Internet. Overall policy for operation of these networks is set by ASD NII/DoD CIO, while direction for operation and defense of the networks is provided by DISA and JTF-GNO. DISA and JTF-GNO are separate, independent organizations that share a Commanding Officer. The Commander of DISA is dual hatted as the Commander of JTF-GNO but each role has a different higher headquarters. As DISA Commander s/he reports to the both the ASD NII/DoD CIO and USSTRATCOM, while in the JTF-GNO role, the Commander reports only to USSTRATCOM.

[47] Michael J. Carden. "Cyber Task Force Passes Mission to Cyber Command," *American Forces Press Service*, Sept 7, 2010.
[48] Ibid.

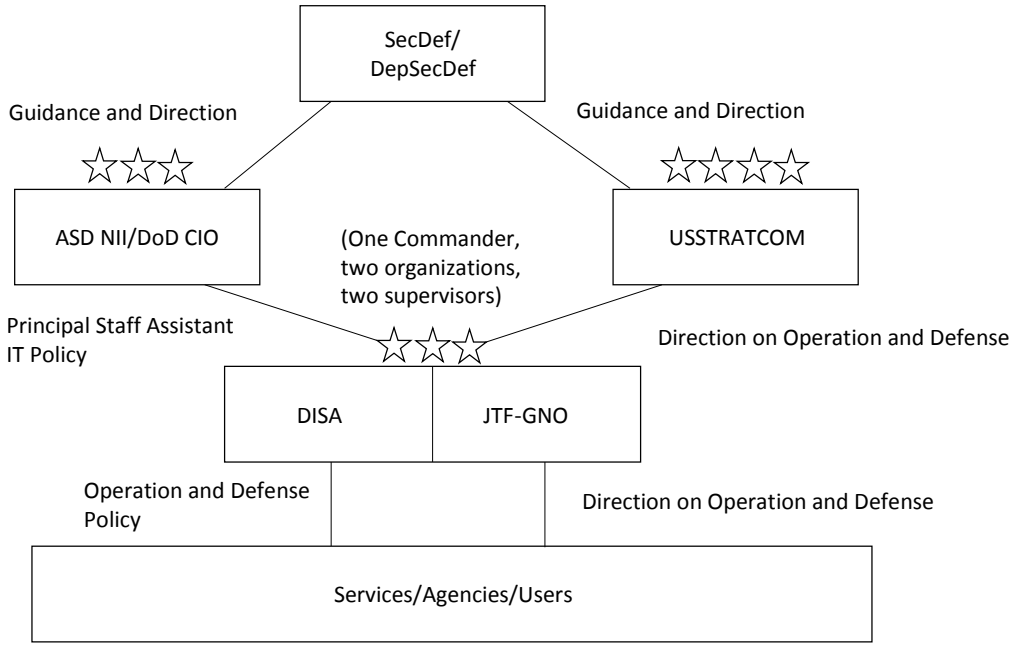

Figure 2.1 Organization and Structure of the DoD Network 2010

There are some challenges with a dual-hatted governance structure. From 2006 to 2010, DISA and JTF-GNO had separate network operations centers (NOCs) in the same headquarters building in Arlington, VA. The NOCs had similar network displays on large screens and each had its own watch floor, where action officers monitored and responded to network actions. There were overlapping displays and functions that have since restructured and today are combined into a single watch floor and NOC. Despite the same Commander and co-located NOCs, there was often conflicting guidance disseminated to the Services, leaving the Services in a position to choose which guidance to follow.[49] In the case of social media, the ASD NII/DoD CIO failed to develop a policy early enough, so the JTF-GNO filled the void with their campaign to block social media on DoD networks. The Services also developed their own independent social media policies which were not consistent among themselves. Both DISA and JTF-GNO favored blocking social media, but for different reasons. JTF-GNO was concerned with security

[49] Interview with Army Colonel who previously worked at JTF-GNO, February 6, 2012.

and privacy issues that exist with social media, while DISA was in support of the cost savings associated with reduced bandwidth usage.

2.2 Debates and Policy Actions Regarding Social Media

In a three year period, DoD issued two major, contradictory decisions on social media use in the military. In May 2007, the JTF-GNO ordered the restriction of recreational and social media websites at all DoD internet access points. In February 2010, the Office of the Deputy Secretary of Defense reversed that decision and directed DoD service providers to completely open their networks to social media use. Both policies generated debate from within and outside the military and led to a heated battle within the walls of the Pentagon. That battle is far from over, but is temporarily stabilized at the moment with the use of social media allowed on all DoD networks.

In 2005-2006, the DoD was facing "a continuous set of intrusions. There was always a base or organization being compromised and a complete lack of consistent discipline in network management."[50] The leaders at DISA decided to take a holistic view of the network and try to solve some of these problems. One of DISA's remedial actions was to start monitoring and reporting top internet domains that were sending traffic to DoD.[51] These internet traffic surveys proved that DoD employees were spending a significant amount of time on social media sites during the workday.[52] It was an unintentional discovery that would spark a contentious debate among many different social groups within the Department, on Capitol Hill and in the media.

[50] Interview with Operations Officer JTF-GNO, Feb 28, 2013.
[51] Department of Defense. "Department of Defense Personnel Access to the Internet," *Report to Congress* in response to request on page 323 of Senate Armed Services Committee Report Number 110-77, Sept 2007, p. D-1.
[52] Interview with retired Army Colonel, Feb 10, 2013.

Also at this time, the Services were all using social media differently and there were various applicable policies, but no standard for the Department. The Navy and the Marine Corps had definitive policies, though they conflicted with each other. The Navy officially endorsed social media on October 28, 2008 when it released a memorandum signed by the Navy Chief Information Officer (CIO) with the subject line, "Web 2.0 – Utilizing New Web Tools." It stated, "The Department endorses the secure use of Web 2.0 tools to enhance communication, collaboration, and information exchange; streamline processes; and faster productivity improvements."[53] The Marine Corps released an order on August 3, 2009 entitled, "Immediate Ban of Internet Social Networking Sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPRNET." This order stated, "Access is hereby prohibited to internet SNS from the MCEN NIPRNET, including over virtual private network (VPN) connections."[54] This is significant because the Marine Corps is a subordinate part of the U.S. Navy. The Army's policy allowed for some social media blocking according to the guidelines of JTF-GNO. It released an order on August 14, 2009 entitled, "Public Announcement on the Army's Guidance on Accessing Social Networking Sites (SNS)." The policy stated, "Current Army guidance permits mission use access to internet social networking sites (SNS), unless specifically prohibited by Joint Task Force Global Network Operations (JTF-GNO)…The Army is currently reviewing its policies on SNS. While waiting for this review to be completed, there is no Department of the Army directive that prohibits users from accessing social networking sites."[55] The Air Force did not publish a separate social media policy. However, in November 2009, the Air Force Public

[53] Department of Defense. "The Use of Web 2.0 in the Department of Defense," *DoD CIO and Joint Staff J6*, Washington, DC, July 2009, p. 4.
[54] United States Marine Corps. "Immediate Ban of Internet Social Networking Sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPRNET," *MARADMIN* 0458/09, Washington, DC, August 3, 2009.
[55] United States Army. "Public Announcement on the Army's Guidance on Accessing Social Networking Sites (SNS)," *ALARACT 228/2009*, Washington, DC, August 14, 2009.

Affairs Agency published a booklet entitled *Social Media and the Air Force.* Within this booklet is a statement commenting on the lack of policy, "Until now, the Air Force has not had an official stance on engaging bloggers, social media and Web 2.0 initiatives."[56] The booklet also urges members of the Air Force to use social media, "All Airmen are encouraged to use social media to communicate about topics within their areas of expertise, or their interests."[57] The Air Force Public Affairs office also provided links to the Air Force's official YouTube, Facebook and Flickr sites within the booklet.

The Deputy Secretary of Defense William J. Lynn, III, who would eventually sign the new policy allowing social media use on DoD networks, was a supporter from the beginning. As one of his staff recalled, "Deputy Secretary Lynn saw the value of social media and wanted the DoD to be able to use it safely."[58] The DISA/JTF-GNO Commander thought otherwise. As he later argued, "I can tell you, the people who approved this policy have never run or tried to protect a network."[59] So how does a contentious issue get resolved if people at the highest levels of the Department disagree?

The Department of Defense has a process to debate contentious topics at the most senior military levels called the Joint Chiefs of Staff (JCS) Tank. Officially the room where the meetings are held is called the JCS Conference Room; unofficially, by insiders, it is called the "tank."[60] The Chairman of the Joint Chiefs of Staff (CJCS) regularly[61] meets with the Military Service Chiefs and their three star operations deputies in the tank to discuss national security

---

[56] United States Air Force Public Affairs Agency. *Social Media and the Air Force*, Washington, DC, November, 2009, p. 23.
[57] Ibid, p. 1.
[58] Interview with Acting DoD CIO, January 20, 2011.
[59] Interview with 3 star general (retired), February 13, 2013. Incidentally, JTF-GNO has morphed again under a different name but at the time period in this chapter it is called JTF-GNO.
[60] Bernard E. Trainor. "Washington Talk: Joint Chiefs of Staff; Inside the 'Tank': Bowls of Candy and Big Brass," *New York Times*, Jan 11, 1988.
[61] Approximately three times per week.

issues and resolve disputes among the Services. The CJCS is a four star general and the nation's highest ranking military officer. The Service Chiefs are all four star generals and the top ranking individuals within the Army, Navy, Air Force, Marines and the National Guard. Topics may include national strategy, topics with Congressional interest, or topics with irreconcilable and unresolved differences from the Services. Tank sessions are private and comments made inside the room cannot be attributed to their originator when the meeting is over.[62]

Tank sessions are very structured. The room is locked and late arrivals and early departures are not allowed for any reason. The briefings follow a specific format which presents background information, identifies the issue, presents COCOM, Service, Agency, and Joint Staff positions, and then presents several solutions including a recommended solution. There is candid discussion, and the principle attendee is the only one allowed to speak for each COCOM, Service or Agency.[63] The use of social media on DoD networks was the subject of at least two tank sessions in 2007.

In Feb 2007 and on May 25, 2007, the senior leaders of JTF-GNO briefed the tank on the Services' use of bandwidth, with the intention of gaining concurrence to restrict web content on DoD networks.[64] The argument used in the tank was first about limiting access to recreational websites by government employees during the workday, not as much about network security.[65] I spoke with the then Commander of DISA and JTF-GNO about his experience back then and he stated, "We could monitor network statistics and we found that 75% of the NIPR[66] bandwidth

[62] Interview with 3 star general, February 3, 2013.
[63] Chairman of the Joint Chiefs of Staff Instruction, "Meetings in the JCS Conference Room," CJCSI 5002.01, Washington, DC, 13 Dec 2010.
[64] Department of Defense. "Department of Defense Personnel Access to the Internet," *Report to Congress* in response to request on page 323 of Senate Armed Services Committee Report Number 110-77, Sept 2007, D-1.
[65] Interview with 3 star general, February 3, 2013.
[66] The NIPRNET (Non-secure Internet Protocol Routing Network) is the DoD's unclassified network.

was going to things like March Madness,[67] financial sites, and dating services. It was costing the government a lot of money for a lot of non-government work. Service members were on these [social media] sites and it was costing the government a significant amount of money. It's misuse of government funds. By blocking these websites to save money, we could also improve our cyber security."[68]

The operations officer of the JTF-GNO backed up the general's statement. "Our opposition to social media wasn't about OPSEC [operations security]—we were not trying to solve that problem, that came up later…we did run network analysis tests to see what we were allowing access to on the government networks. We were able to show a significant amount of non-mission essential traffic during normal duty hours. We keep paying for bandwidth to support non mission essential traffic. Does that pass the sanity test?"[69] The ASD/NII for DoD stated, "It wasn't that much of a security issue, it was more about stopping employees from goofing off. It was not about bad behavior; the statistics didn't show that."[70]

The JTF-GNO, in their defense role, should have been focused on the threats to the network from social media, but they seemed to be side tracked by a desire to ensure that government employees were not surfing the internet during duty hours. I believe they thought it would be easier to convince operational commanders by using a productivity example instead of using network threats and technical jargon the operational commanders would not be familiar with. This would prove to be a severe miscalculation on JTF-GNO's part.

A bandwidth study conducted in July 2006 on DoD networks showed that 90 percent of inbound internet traffic was due to commercial web browsing, with as much as two thirds proven

[67] A Division 1 college basketball tournament usually held annually in March.
[68] Interview with 3 star general, February 3, 2013.
[69] Interview with Army Colonel (retired), February 28, 2013.
[70] Interview with Acting DoD CIO, January 20, 2011.

to be for recreational use during main duty hours.[71] The network access points were saturated during any major news event. As one operations officer recalled, "I lived through the Michael Jackson death. It was the single most consumption of DoD bandwidth up to that point."[72] The evidence provided by the bandwidth study was compelling enough and the tank's decision was to allow certain websites to be blocked at the internet access points.

The JTF-GNO released warning order 07-003 on February 6, 2007 entitled "Blocking Recreational Traffic at the Internet Access Points (IAP)." It was released to the OSD, the Joint Staff, Combatant Commands, Military Services and DoD Agencies and warned them that an order was forthcoming to block certain network sites. The ASD for Public Affairs said, "When General Chilton put out that warning order it, it was a shot across the bow."[73] The civilian leadership in DoD were preaching open communications and touting the use of social media across DoD and here was a military subordinate command warning the Department it was about to restrict all access to social media. There was immediate conflict.

On May 15, 2007, the JTF-GNO issued an Operational Directive Message (ODM) 059-07 with the subject, "IAP Access Control List (ACL) Security Filter Update" which directed DoD service providers to block certain recreational websites, many of them social media sites.[74] There were thirteen websites on the block list: You Tube (www.youtube.com), 1.FM (www.1.fm), Pandora (www.pandora.com), Photo Bucket (www.photobucket.com), MySpace (www.myspace.com), Live365 (www.live365.com), Hi5 (www.hi5.com), Metacafe (www.metacafe.com), MTV (www.mtv.com), I-Film (www.ifilm.com), Black Planet (www.blackplanet.com), Stupid Videos (www.stupidvideos.com) and File Cabi

[71] Department of Defense. "Department of Defense Personnel Access to the Internet, p. 5.
[72] Interview with COL (retired) U.S. Army, April 5, 2013.
[73] Interview with ASD for PA, May 29, 2013.
[74] Department of Defense. "Department of Defense Personnel Access to the Internet,", p. 7.

(www.filecabi.com). DoD stated that once the block was in place, there was an immediate, measureable effect of 140 Mbps freed up for operational use.[75]

From 2007 to 2009, the only policies in effect were many messages from JTF-GNO updating the prescribed block list for websites, constantly adding more sites to block. Service members were unable to access most social networking sites from government computers. Written policies were inconsistent across DoD, ranging from no Air Force policy, an Army policy to partially block social media in accordance with JTF-GNO guidance, to the Marine Corps banning social networking entirely from its official networks,[76] despite a Navy policy encouraging Navy/Marine use of Web 2.0 technology.[77] The DoD lacked a comprehensive strategy to address social networking from a Department level standpoint. The Marine Corps IA Manager captured the situation in 2009 perfectly in an interview, noting, "Right now, the [Defense Department] has yet to come up with a policy on this. So we are just maintaining what has been the policy since 2007."[78]

In September 2007, the Department of Defense responded to a congressional request in the 2008 National Defense Authorization Act asking for a report on the effects of blocking social media on DoD networks. The Department announced that the blocking of websites in the future was likely to become even more constricting than it already was. The report said, "Recreational web browsing cannot be left unchecked in DoD systems and available to be exploited by hostile actors. As DoD continues to assess its network vulnerabilities, more filtering may be required to

[75] Department of Defense. "Department of Defense Personnel Access to the Internet,", p. 7.
[76] Lubold.
[77] Department of the Navy. *Web 2.0-Utilizing New Web Tools*. Chief Information Officer, United States Navy. Washington, DC, October 20, 2008. This is significant because the Marine Corps is part of the Department of the Navy and they share one network, the Navy-Marine Corps Internet (NMCI).
[78] John J. Kruzel. "Officials Look to Solve Social Network Risks Without Ban," *American Forces Press Service*, Washington, DC, August 6, 2009.

tamp the ever-increasing demand for bandwidth and to mitigate the security vulnerabilities introduced by certain web technologies and entities."[79]

Previous to the 2010 policy, the Service and Agency network providers had the prerogative to block additional sites to the ones mandated by JTF-GNO. Additionally, there was no standardization of what was blocked across the Army networks; it was entirely up to the local network service provider. For example, in 2008-2009, while I was in Southwest Asia, I was Director of the Theater Network Operations and Security Center (TNOSC), which operated the wide area network in Afghanistan, Kuwait, Qatar, Bahrain and the intrusion detection sensor grid in Iraq. While we generally conformed our restrictions to the websites JTF-GNO directed we block, we also blocked sites based on bandwidth constraints. At that time, in Afghanistan and Iraq, Army networks traveled over primarily satellite links, and to conserve bandwidth, we blocked all streaming video. In Kuwait, Bahrain and Qatar, we were more liberal with the restricted website list because there were primarily fiber links and bandwidth was not an issue. We did block several of the more popular sports sites and internet based email like Gmail and Hotmail. In fact, after seeing the results of the DISA bandwidth studies, we conducted our own survey of what people were surfing in our area of operations (AOR) and decided to block some of the "top talkers" [a slang term for the most visited websites]. But we first tried to ascertain if there was a legitimate use for the site. For example, the number four most visited site was 'manorama.com' which none of us could identify. It turned out to be an Indian social media site which raised the immediate question 'Who on duty in Kuwait is surfing Indian social media sites on the Army network and why?' We discovered that many of the third country nationals working for the United States in Kuwait were from India and they were utilizing our unclassified

[79] Department of Defense. "Department of Defense Personnel Access to the Internet."

network in performance of their duties. Right after that network test, I was in the travel office where four people from India worked. I was the only person in the office when I walked in and from the center of the room I could see all four computer screens which all had manorama.com open on the desktop.

The lack of a clear policy also led to misunderstandings and conflicts between network operators and commanders. During my time in Southwest Asia, I was also approached by a Major General in the dining facility who demanded to know why FoxSports.com was blocked. He wanted to know if there was a specific policy in place blocking it or if the TNOSC was making arbitrary decisions to block websites. We originally blocked it because JTF-GNO informed us by official message that hackers embedded malware in links associated with Foxsports.com's Fantasy sports league websites, which was also well publicized in the media.[80] The general's perception was that in the absence of an official policy I, as the TNOSC Director, was making subjective decisions to ensure deployed personnel were not using the official network for personal business.

Meanwhile, the debate continued in the Department and in the press over security risk versus recognized benefit and responsibility of service members. One of the Colonels who worked at JTF-GNO thought back then the Public Affairs Offices (both military and civilian) (PAOs) had been overly influential in the social media argument because of their relationship with the press.[81] He brought to my attention that a notable figure in the press was Mr. Price Floyd, the Deputy Assistant Secretary of Defense (DASD) for Public Affairs, who was in favor of social media. Mr. Floyd gave many interviews during this time period and the following are representative samples of statements he made in his media interviews:

[80] Threat Center Live Blog. "Foxsports.com Used to Serve Malware," October, 2, 2009.
[81] Interview with Army Colonel (retired) April 5, 2013.

- "The [Defense Department] is, in that sense no different than any big company in America. What we can't do is let security concerns trump doing business. We have to do business."[82]
- "The key to understand is that most of your people already have joined the social media revolution. It's time for you to suit up and join the battle."[83]
- "There also were the tried-and-not-true claims that social media drained productivity."[84]
- "OPSEC needs to catch up with this stuff. This is the modern equivalent of sending a letter home from the front lines."[85]
- "In fact, they talk about the ability for their kids to do homework with their parent who's at war in real time—and that kind of morale boost that happens when you are able to do that is immeasurable."[86]

I tracked down Mr. Floyd in his new position, and asked him about this period of time while the social media debate was raging. He confided that he had felt very strongly on the issue and that it was his duty to support the issue in public. "It was a long time until they rescinded the order [restricting social media on DoD networks]. I felt I had a lot of work to do to publicize this issue to make sure it got the attention it deserved."[87] It is possible that statements by high ranking government officials in the press influenced decisions and policies of DoD by creating a climate of public opinion in favor of an open network policy and by convincing the SecDef/DepSecDef that the DoD needed to keep up with the new technology of the day.

[82] Kruzel. "Pentagon Weighs."
[83] Price Floyd. "In Defense of Social Media," *The Washington Times*, March 21, 2011.
[84] Ibid.
[85] Kruzel. "Pentagon Weighs."
[86] American Forces Press Service. "Social Media Sites Provide Morale Boost, Official Says," *Armed Forces Press Service*, Washington, DC, March 17, 2010.
[87] Interview with Mr. Price Floyd, former ASD PA, May 29, 2013.

The Services and Agencies knew from the newspapers and the chatter within the walls of the Pentagon that a new policy was being developed, but they were not sure what it was going to say and they state they weren't consulted at the network operations level for input. The Air Force Lieutenant Colonel who ran the Air Force Service level Network Operation and Services Center (NOSC) at the time told me, "I didn't have any insight into the DoD level policy as it was being written. We knew it was coming in 1st quarter of 2010, but we didn't know what it was going to say."[88] While I was the TNOSC Director, I was never contacted by either my Service or by JTF-GNO for my input on the social media policy for my recommendations from my experience at the network level. Neither were the Marines, who said, "As far as we knew, DoD was developing a restricting policy. We had already come to that conclusion for the internal Marine Corps networks in August 2009."[89] Had the Marine Corps known the intent of the ASD NII/DoD CIO to open the networks to social media, they may have reworded the title of a directive that generated much debate in the press.

As mentioned earlier, on August 3, 2009 the Marine Corps released a message [called a MARADMIN] with the subject, "Immediate Ban of Internet Social Networking Sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPRNET," which required Marine network providers to block social media sites. The reason given in the message is as follows, "These internet sites in general are a proven haven for malicious actors and content and are particularly high risk due to information exposure, and user generated content and targeting by adversaries. The very nature of SNS creates a larger attack and exploitation window, exposes unnecessary information to adversaries and provides an easy conduit for information leakage that puts OPSEC [operations security], COMSEC [communications security], and personnel and the

[88] Interview with Air Force Lieutenant Colonel NOSC Director, January 28, 2013.
[89] Interview with Marine Corps civilian, Mar 20, 2013.

MCEN at an elevated risk of compromise. Examples of internet SNS sites include Facebook, MySpace and Twitter." [90] Nowhere in the message does the Marine Corps mention conserving bandwidth or expressing concern for recreational use of the internet during duty hours. The message provides a waiver process should a unit deem it needed social media for mission critical work.

I asked the Information Assurance Manager for the Marine Corps about the release of the MARADMIN and he replied, "We unfortunately used the phrase 'Immediate ban on the use of social media.' We meant, unless you have a mission need to use it like recruiting or public affairs. It was misinterpreted by many to mean, lock it down. What we wanted to do was keep it in control and keep it mission focused. The Marine Corps Times got ahold of it and their report created a firestorm. I should have phrased it differently, like just 'use of social media'. There was a perception we were banning it all and we paid for it in the press."[91]

I asked Mr. Price Floyd about the Marines' situation and he said that incident changed the way he characterized his side of the debate. "I thought I would be cute on Twitter and tweeted, 'Lots in the media today about the Marine Corps blocking social media.' I was surprised by all of the comments I got back. Lots of people weighed in on why we should block access. They all supported the Marine Corps. The same arguments came back, 'Bad guys can find out where we are,' and 'Marines should be out there killing people, not hanging out on social media.' 'They'll use it for phishing.' I was surprised at the comments that came back against social media—on social media!"[92] Floyd said the overwhelming response in support of the safety of the Marines made him change is message to the public on the DoD social media policy. From then on he was

[90] United States Marine Corps. "Immediate Ban of Internet Social Networking Sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPRNET," *MARADMIN* 0458/09, Washington, DC, August 3, 2009.
[91] Interview with Marine Corps civilian, Mar 20, 2013.
[92] Interview with Mr. Price Floyd, former ASD for PA, May 29, 2013.

sure to say "Yes we need to use it, but we need to use it responsibly."[93] While an awkward situation, the Marine's public directive actually brought the two sides closer in terms of understanding each other's concerns.

Another angle of the debate was captured by the Senate Armed Services Committee (SASC) who were concerned that the block of recreational websites was affecting the morale of service members deployed to Iraq and Afghanistan. In 2007, The SASC requested a report on post policy bandwidth and security analysis to see the effects the JTF-GNO order blocking certain websites was having on the Department. The report introduction stated, "Those deployed in Iraq, Afghanistan, and elsewhere around the world, sometimes for more than a year, deserve every opportunity to connect with their friends and family on a frequent basis. Social networking web sites facilitate that communication for this generation, in the same way letters, phone calls and telegrams did for previous ones. The committee believes that access to the commercial internet can promote strong morale among personnel in the field as well as family members on the home front."[94] The network bandwidth study proved the bandwidth problem was not being exacerbated overseas by recreational website use. It found most of the use of recreational websites on DoD networks occurred within the Continental United States (CONUS) during typical duty hours, not in the war zones.[95]

The concern for deployed service members to be in constant contact with their families is a common theme in the media and around the Services. The operations officer for JTF-GNO said when they first blocked the thirteen sites, "We got a lot of pushback. 'You bastards, you are going to affect the warfighter.' But what we found out was there wasn't a lot of recreational use

[93] Ibid.
[94] Department of Defense. "Department of Defense Personnel Access to the Internet."
[95] Interview with retired COL, Feb 28, 2013.

deployed. And that was because we funded commercial internet cafes."[96] Where ever possible, the military sets up kiosks for commercial internet in order to keep personal traffic off the DoD network. They are called Morale, Recreation and Welfare (MWR) computers and operate on a network not connected to the NIPRNET.[97] The network studies showed that while there was some use in deployed theaters, it was minimal. There was a lack of a consistent social media policy and not every forward operating base in Iraq and Afghanistan had existing commercial internet available for off duty web surfing. In more austere locations, many base commanders decided to allow social media use for morale purposes. Even so, the amount of recreational website traffic was significantly higher in stateside locations.

I spoke with the government civilian at the Office of the Secretary of Defense (OSD) level who was the action officer responsible for penning the policy on opening the networks to social media and shepherding it through the approval process. He said, "At the time, the information gathering on both sides was skewed and irrelevant. They made it sound like putting it on the DoD networks was the only way for Service members to stay in contact with their families. However, as you know, there were standalone capabilities on MWR networks at most bases. They didn't have to use social media at work."[98] He also related it to his own military experience, "I was in the Navy in the 80's and 90's. We didn't need that much contact with our families."[99] Though he did admit the military's circumstances have changed significantly in past ten years because of the wars in Iraq and Afghanistan: "But then again the navy wasn't gone for

[96] Interview with retired COL, Feb 28, 2013.
[97] Interview with Marine Corps Civilian, Mar 20, 2013.
[98] Interview with DoD civilian policy writer, Dec 20, 2012.
[99] Ibid.

a year or two years on the extended deployments that are a large part of today's military culture."[100]

In response to the debate and requests for guidance from the Services and Agencies and the DoD Public Affairs Office, the Deputy Secretary of Defense directed the ASD NII/DoD CIO to produce a policy for use of social media. The ASD NII/DoD CIO assembled a small group of action officers from USSTRATCOM, DISA, JTF-GNO, and NSA to produce the document. The Services were not represented in the initial draft of the document, yet they were allowed to review and comment on it during the staffing process. It took about nine months[101] to complete *Directive Type Memorandum 09-026 – Responsible and Effective Use of Internet-based Capabilities,* which was signed by the Deputy Secretary of Defense on February 25, 2010.

The policy itself was a mere two pages with three attachments and succinctly states the new policy regarding user of social media. The policy applies to all of the Department of Defense and starts with a definition of a new term, *Internet-based Capabilities*. These are, "all publicly accessible information capabilities and applications available across the Internet in locations not owned, operated or controlled by the Department of Defense or the Federal Government. Internet-based Capabilities include collaborative tools such as SNS [social networking services], social media, user generated content, social software, email, instant messaging, and discussion forums (e.g. You Tube, Facebook, MySpace, Twitter, Google Apps)."[102] The small group of authors assembled by the ASD NII/DoD CIO, agonized over

[100] Ibid.
[101] Interview with DoD civilian policy writer, December 20, 2012.
[102] Deputy Secretary of Defense. *Directive Type Memorandum 09-026 – Responsible and Effective Use of Internet-based Capabilities*, Department of Defense, Washington, DC: Office of the Deputy Secretary of Defense, February 25, 2010.

every sentence and debated every word of the policy so nothing would be left to the interpretation of the individual Services and Components.[103]

The policy itself is as follows:

- The NIPRNET shall be configured to provide access to Internet-based Capabilities across all DoD Components.
- Commanders at all levels and Heads of DoD Components shall continue to defend against malicious activity affecting DoD networks, (e.g. distributed denial of service attacks, intrusion) and take immediate and commensurate actions, as required, to safeguard missions (e.g. temporarily limiting access to the Internet to preserve operations security or to address bandwidth constraints).
- Commanders at all levels and Heads of DoD Components shall continue to deny access to sites with prohibited content and to prohibit users from engaging in prohibited activity via social media sites (e.g. pornography, gambling, hate-crime related activities).[104]

The three attachments contain references, responsibilities of each staff section or component, and guidelines for use of internet based capabilities. The first bullet made clear the policy applies to everyone in the Department of Defense. The second bullet allows operational Commanders to block sites if there is malicious content on them that is affecting the mission or if those sites are utilizing excessive bandwidth. It was very important to policy makers to ensure the Commanders on the ground had the flexibility to make their own decisions based on threat or operational need.[105] Note the words in the second bullet, *temporarily limiting access to the internet*. This sentence was written specifically to prevent the Marines from making an

[103] Interview with Acting DoD CIO, January 20, 2011.
[104] DTM 09-026, *Responsible and Effective Use of Internet-based Capabilities*
[105] Interview with Army Major General, April 27, 2012.

overarching decision from their Commandant to permanently limit access to social media sites.[106] The third bullet reiterates the DoD policy for network providers to block prohibited activities such as pornography and hate crimes. This allows for the military to block social media sites that cater to such activities which are against the morals associated with the DoD. There are two appendixes to the policy which provide further guidance on having an official presence on a non-DoD site (e.g. The Commandant of the Marine Corps could have his own official Facebook page) and also states that individual Service members are not allowed to represent the Department of Defense on external social media sites. There is also a section containing roles and responsibilities of the DoD components, most notably the DoD Public Affairs Office is required to maintain a registry of all DoD official presences and the requirement for the individual Services and Agencies to register any official presence.

Attachment 2 to the policy provides guidelines for use of internet-based capabilities. It provides examples but does not limit what internet-based capabilities are (i.e. social networking sites, image and video hosting web services, blogs, etc.). It guides the creation of DoD official presences and official use of social media for DoD specific business. Lastly, this attachment permits employees to use social media on government time – on a non-interference basis with their jobs, cautions both official and non-official users about OPSEC, and states that employees "shall not represent the policies or official position of the "Department of Defense."[107] A general officer who previously worked in JTF-GNO thought these guidelines should have been in the main body of the policy. "The existing policy has no balance of risks and benefits. The risks are buried in the back of the document in an appendix!"[108]

[106] Interview with Acting DoD CIO, January 20, 2011 and Interview with Marine Civilian, Mar 20, 2013.
[107] DTM 09-026, *Responsible and Effective Use of Internet-based Capabilities.*
[108] Interview with Army Major General, Apr 27, 2012.

The civilian at the OSD level responsible for the policy was privy to the internal DoD debate between the DoD CIO, DISA, JTF-GNO, National Security Agency (NSA) and United States Strategic Command (USSTRATCOM. He was responsible for collecting and adjudicating the official comments from the Components on the policy. He recalled, "The policy was completed in about 9 months. It was very contentious. There were extremes to both of the options…there was a conflict of interest between openness and security."[109] The same Major General who thought the guidelines should have been in the main policy does believe the topic was sufficiently debated, "There wasn't a blind jump towards the technology. It was a slow and deliberate movement for the most part."[110] However, the topic was never taken back to the Tank, and the decision to restrict access to social media on DoD networks was reversed with the stroke of a pen.

It is unusual for an OSD level policy to be produced and signed in such a short period of time. On average it is about two years to develop and publish a policy.[111] It is also unusual to make such a large decision without the Service Chiefs conferring in the Tank. A retired Colonel who supported blocking social media claimed, "They took it to the Tank and the Chiefs agreed to block these sites."[112] The Colonel's view was the Tank is a decision making body that had the authority to make this decision. ASD for Public Affairs Price Floyd, a DoD civilian, had a different view of the Tank. "The problems with Tanks is there are just uniforms in the room – no civilians, they aren't based in reality."[113] After the Commander of USSTRATCOM published the order to block certain social media sites on the networks, Floyd said another high ranking

[109] Interview with DoD civilian policy writer, December 20, 2012.
[110] Interview with Army Major General, April 27, 2012.
[111] Interview with DoD civilian policy writer, December 20, 2012.
[112] Interview with Army Colonel (retired), January 17,, 2013.
[113] Interview with Mr. Price Floyd, former ASD PA, May 29, 2013.

civilian on the OSD staff asked in the SECDEF's weekly staff meeting, "Does he [the USSTRATCOM Commander] have the authority to do that?"[114] The question of his authority prompted the Commander of USSTRATCOM to advocate for adding their Unified Command Plan (UCP) role to the policy stating USSTRATCOM's responsibility to operate and defend the GIG to the final version of the policy.[115] The final decision to open the networks was made by the DepSecDef William J. Lynn, and the initial policy was written by a small group of action officers that initially did not include the Services. The seemingly-hasty decision fueled further debate on the topic and added to existing tensions between opposing sides.

2.3 SCOT Analysis

The social construction of technology (SCOT) provides useful concepts to analyze how the decision in the debate on social media on government networks was made. Starting with the traditional views of Pinch and Bijker, the situation can be broken down into artifacts, problems, solutions and social groups.[116] Clearly, the artifact would be social media under a traditional SCOT view. However, unlike Pinch and Bijker's case study of the bicycle, I am not examining various versions of social media to see which one becomes the mainstream technology. Pinch and Bijker use SCOT to explore how the technology itself changes due to social influences. I am interested in how the policy governing the technology of social media evolves due to the social influences within the DoD. For this use case, the artifact is the social media policy itself and whether to permit or restrict the use of social media on DoD networks.

[114] Interview with Mr. Price Floyd, former ASD for PA, May 29, 2013.
[115] Interview with Army Colonel, February 2011.
[116] Trevor Pinch and Weibe E. Bijker. "The Social Construction of Facts and Artifacts: Or How the Sociology of Science and Sociology of Technology Might Benefit Each Other," in *The Social Construction of Technological Systems*, ed. Weibe Bijker, Trevor Pinch, and Thomas P. Hughes, Cambridge, MA: MIT Press, 1987, p. 32.

One of the main concepts of SCOT is a multidirectional model in which some variants "die out" and others "survive."[117] Interpretative flexibility means that not only do people perceive the artifact differently, but there are multiple options for a final solution. In the case of the DoD social media policy, there were four possible outcomes that social groups could favor: (1) Allowing social media on DoD networks, (2) Not allowing social media on DoD networks, and (3) Partially allowing it on DoD networks by restricting some social media sites, and (4) Creating DoD only versions of social media for use behind a DoD firewall. Each one of these four solutions has been pursued at some time by various social groups.

2.4 Relevant Social Groups

In order to understand the problems and possible solutions associated with the artifact, we must first define the relevant social groups and the "problems" they were trying to solve. According to Pinch and Bijker, social groups are defined by problems. Each group has a common "problem" with the technology, though each group can also have multiple problems.[118] I have identified ten relevant social groups and their views on what problem they were trying to solve in the decision to open the DoD networks to social media.

(1) SecDef/DepSecDef: The SecDef Robert Gates and DepSecDef William J. Lynn were both early supporters of the use of social media on DoD networks.[119] Gates and Lynn believed the problems were the need to support users and the need to keep up with current technology. Gates believed the [pro-democracy] protestors in Iran in early 2009 were fueled by social media. "It's a huge win for freedom, around the world, because this monopoly of information is no longer in the hands of the government. Governments may be able to

[117] Trevor J. Pinch and Wiebe E. Bijker. "The Social Construction of Facts and Artifacts," p. 29.
[118] Ibid, 30.
[119] Interview with Mr. Price Floyd, former ASD for PA, May 29, 2013.

squelch some information channels but they just can't draw the net tight enough to stop everything. If you can't text, then you Twitter."[120] Secretary Gates charged the ASD for Public Affairs, Mr. Price Floyd, with introducing the DoD to social media and embracing its use throughout the Department. Floyd said, "When I did my interview' with Secretary Gates, we talked about social media. He understood in a dramatic way the importance of social media and challenged me to fully utilize it within the Department of Defense…he challenged me to bring social media to the men and women of the Armed Forces, and to 'go make it happen.'"[121] Gates told Floyd that while he was the President of Texas A&M, he encouraged students to email him directly. He wanted to be in touch with the students using the methods the students used to communicate.[122]

DepSecDef Lynn, was responsible for signing the social media policy. Lynn was a supporter of opening the DoD networks to social media, despite concerns from inside the Pentagon of security issues.[123] Early on, the Commander of USSTRATCOM submitted a proposed policy to Lynn which was 18 pages long and severely restricted the use of social media on DoD networks. The restrictive policy went against everything the SecDef and DepSecDef were doing to encourage the use of social media and the policy was rejected by the DepSecDef. Floyd remembers, "When he [Lynn] first saw the first attempt from STRATCOM at a social media policy, he looked at me and said, "What am I supposed to do with this?"[124] The Acting DoD CIO agreed with Floyd about Lynn's reaction and told me,

[120] Miles, Donna. "Gates, Mullen: Communications Technologies 'Strategic Asset' for United States," *American Forces Press Service*, Washington, DC, June 18, 2009.
[121] Interview with Mr. Price Floyd, former ASD for PA, May 29, 2013.
[122] Ibid.
[123] Burns, Robert. "William J. Lynn, Deputy Defense Secretary, Will Resign: Top Pentagon Official Plans to Quit by Early Fall," Huffington Post, July 7, 2011.
[124] Interview with Mr. Price Floyd, former ASD for PA, May 29, 2013

"Bill Lynn killed that policy."[125] Two years later, just after signing the DoD social media policy, Lynn went to Facebook headquarters on an industry visit to share DoD's new view on social media and told the workers there, "We [DoD] certainly see social media as a critical new avenue in how you communicate."[126] At the same venue, he stated that DoD's reasons for allowing social media on DoD networks were attracting youth to DoD, allowing deployed service members to communicate regularly with their families at home, and as a possible tool for information gathering.[127]

(2) US Strategic Command (USSTRATCOM) is responsible for the overall defense and operation of the DoD Global Information Grid (GIG). This is tasked by the President of the United States in his role as Commander in Chief of the Armed Forces in the Unified Command Plan (UCP). President Bush tasked USSTRATCOM with this role in UCP 2008; it was the first time Cyberspace Operations was mentioned in a UCP.[128] The Commander of USSTRATCOM was adamantly against opening the networks to social media because of the security risks involved.[129] General Chilton believed the problem was the security risk that social media could potentially introduce into the DoD networks. His philosophy was to block everything and only permit web access by exception (called whitelisting) as opposed to allowing everything and blocking known or suspected websites (called blacklisting).[130] Blacklisting was then and still is the common practice on the DoD networks. An Army officer responsible for securing DoD

[125] Interview with Mr. Dave Wennergren, Acting ASD NII/DoD CIO, Jan 20, 2011.
[126] Jim Garamone. "Lynn Discusses Social Media at Facebook Headquarters," *American Forces Press Service*, Apr. 28, 2010.
[127] Ibid.
[128] Chairman of the Joint Chiefs of Staff Memorandum, "Distribution of the Unified Command Plan 2008 (UCP 08)," Washington, DC, Dec. 23, 2008.
[129] Interview with Acting DoD CIO, Jan 20, 2011.
[130] Robert Ackerman and Rita Boland. "Army Programs Face Daunting Challenges," *Signal*, Nov 2008.

networks at the time commented, "We had the Cold War, bunker in, keep everything out mentality at the time-especially from STRATCOM."[131]

(3) Intelligence Community and National Security Agency (NSA): The NSA is responsible for preventing foreign adversaries from gaining access to sensitive or classified national security information on DoD's networks. NSA also enables Network Warfare operations to defeat terrorists and their organizations at home and abroad.[132] The Commander of NSA, General Keith Alexander, was exploring the problem social media poses on DoD networks because of the perceived security threat.[133] The NSA recognized the need to address the threat and was exploring hybrid options to block certain social media sites. NSA was not an advocate of banning social media entirely without studying the problem. The NSA staff visited JTF-GNO in 2007 to discuss this issue. According to one JTF-GNO staffer, "NSA gave a briefing saying social media is a big threat vector...They are phishing grounds for advanced threats. General Alexander's staff wanted to start a conversation with us at JTF-GNO to attack this problem together."[134]

(4) Service Providers: The Service Providers are DISA and JTF-GNO, responsible for operating and defending the Department's networks. Since both organizations had the same Commander, they were united in their position favoring a hybrid solution where certain social media sites are blocked. The Service Provides were torn between their desire to provide access to social media services to support what users want and the desire to protect users from outside threats. A strong factor in their position was their higher headquarters, USSTRATCOM, was adamantly against allowing social media on DoD networks. Another factor was cost. As service providers, it is

[131] Interview with Army Colonel, Apr 5, 2013.
[132] http://www.nsa.gov/about/mission/index.shtml
[133] Interview with Army Colonel (retired), Feb 28, 2013.
[134] Ibid.

more cost effective to block something completely from the network, than it is to develop tools to combat a threat. A former Operations Officer told me, "At JTF-GNO, we conducted bandwidth studies of what was happing on the networks. We found we could go two years without increasing bandwidth. We would save a lot of money by blocking these sites."[135] As stewards of the public trust, their interest was in operating and defending the DoD networks in a safe and cost effective manner.

The Commander of DISA and JTF-GNO at the time said, "We at DISA wanted to selectively block content based on people's jobs. We could monitor network statistics and we found that 75% of the NIPR bandwidth was going to things like March Madness, financial sites, and dating services. It was costing the government a lot of money for a lot of non-government work..."[136] DISA also explored creating a social media site for DoD behind the Department's firewalls. "We offered to create a social network within the dot mil but it wasn't successful and service members did not want to use it."[137] Service members wanted to use social media not only to keep in touch with each other, but to keep in touch with their families while they were deployed. A service behind the firewall would not be available to all of the people service members want to keep in touch with which was the big flaw in this course of action.

(5) Military Services/Agencies: This includes Service Chiefs and also the network providers for the Army, Navy, Air Force, Marines, other DoD Agencies and activities. (The Coast Guard is not included in Military Services because they are governed by the Department of Homeland Security (DHS) and are not subject to the same network rules as the DoD.)[138] There was initial conflict within this social group on their issues with social media. Like the service providers, the

[135] Interview with retired Army Colonel, Feb 10, 2013.
[136] Interview with former Commander of DISA and JTF-GNO, Feb 13, 2013.
[137] Ibid.
[138] http://www.uscg.mil/top/missions/

Services were torn between wanting to support users who desired use of social media and the security risks of social media. While some believed it could be an effective and necessary tool in recruiting and public affairs, there was always the question of operations security and the safety of military personnel that caused doubt about the social media technology. In discussing the tank sessions on social media with me, the Commander of DISA and JTF-GNO said, "The Services were split in their positions on social media. One of the reasons given were 'young people expected to use the military networks like they would their home networks' not, 'we need it for the mission.' Another was 'there was a high demand for it.' The belief that it [social media] was a competitive technology and we needed a lollipop to entice people to work for us."[139]

An Army Lieutenant Colonel tied the social media security problem to the Taliban—the military's foe in Afghanistan. "Overall it's probably too early to talk about trends, but I would say the Taliban, just like the rest of the world, are trying to use social media to achieve their aims. The Taliban have proven to be an adaptable enemy and are now using cyberspace as a new battlefield. The Taliban use social media to provide information, including false and misleading 'disinformation' to various audiences, both domestically and internationally."[140]

To solve this problem, the Services also looked at creating their own social media sites behind firewalls but discarded those plans as infeasible due to user feedback. An Army Colonel stated, "My sense is that the military tends to be clumsier about adopting commercially available technologies and we tend to try to build our own—which typically fall short of the touch and feel of commercially available products."[141] Anther Army officer commented, "Should we build our

[139] Interview with the former Commander of DISA and JTF-GNO, Feb 13, 2013.
[140] Bill Gertz. "Inside the Ring: Taliban Infiltrate Social Media," The Washington Times, Washington, DC, August 22, 2012.
[141] Interview with Army Colonel, Feb 6, 2012.

own sites? I don't think so. People just want to use what everybody else is using."[142] At periods of time, the members of this social group did not agree on the position of accepting or rejecting social media, they had the same opportunity to present their argument to the tank. And ultimately, their reaction to the policy shift united them as they all had to proceed together to implement the policy.

(6) ASD NII/DoD CIO is the Principal Staff Assistant (PSA) responsible for architecture and defense of the DoD networks and all IT related policy.[143] The Acting ASD NII/DoD CIO, Mr. David Wennergren, was a supporter of opening the networks to social media because he believed social media tools were essential to the future of DoD, they would help service members perform their jobs better, and they would attract the youth in the Millennial or Net Generation to work at DoD.[144] "Not only are service members using these tools to communicate with their friends and family, but people are also using them to do their jobs better and even to collaborate with mission partners and people outside the organization,"[145] Wennergren said in an interview at the time. When I spoke with Wennergren in 2011, he said, "The millennial workforce expects to use social media. We want the Department of Defense to be the employer of choice for the "Net Generation."[146]

Wennergren also believed social media would support deployed service members in contacting home, though he did make a point of stating the need to achieve a balance between information sharing and security,[147] a point he also made to me in our 2011 interview.

---

[142] Interview with Army Lieutenant Colonel, Jan 17, 2013.
[143] Department of Defense. "Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)/DoD CIO)," *DoD Directive number 5144.1*, Washington, DC, May 2, 2005.
[144] Department of the Navy. "A Conversation with David M. Wennergren, DoD Assistant Deputy Chief Management Officer, *CHIPS Magazine*, Jan-Mar 2011.
[145] J. Nicholas Hoover. "DoD Loosens Social Media Restrictions," *Information Week*, Feb 26, 2010.
[146] Interview with Mr. Dave Wennergren, Acting ASD NII/DoD CIO, Jan 20, 2011.
[147] Donna Miles. "New Policy Authorizes Social Media Use With Caveats," *Armed Forces Press Service*, Washington, DC, Feb 26, 2010.

(7) Public Affairs Offices (PAO): The PAO provides DoD information to the public, Congress and the media.[148] Price Floyd said he didn't really understand why USSTRATCOM, DISA, JTF-GNO, and NSA were fighting so hard to restrict the use of social media when the SecDef had already decided the outcome. "I wasn't trying to convince anyone because the decision had already been made by Secretary Gates. You have to be careful when you start a fight, you can lose it. I had the advantage in that I knew where the end was going to be, but I didn't understand the visceral fear of the results of opening access to everyone."[149]

Besides my interview with Price Floyd and his positive comments on social media in the press, I spoke to two Public Affairs officers in the Army. They were very enthusiastic about the introduction of social media to their jobs and both felt it was necessary to use social media and it was the IT community's job to figure out how to secure it.[150] In fact, the Army PAO created a new office to handle social media and their chief told me, "People don't have time to read emails but they have time to scan a quick tweet that comes up on their computer and if they have a link, they can follow it easily rather than opening up emails. There's no time for email...This is like instant information straight to your brain. It enhances everything we do by elevating it to a greater reach."[151] I include in this social group any other specialty that clearly benefits from the legitimate, work related use of social media to connect with the public in their everyday jobs, (e.g. recruiters, base commanders, etc.) As stated previously, Floyd, as the PAO at the Office of Secretary of Defense level, was extremely influential in the decision to open the networks to social media.[152]

[148] http://www.defense.gov/pubs/almanac/asdpa.aspx
[149] Interview with Mr. Price Floyd, ASD for PA, May 29, 2013.
[150] Interview with Army Public Affairs Officers, 26 Nov 2012 and 14 Dec 2012.
[151] Interview with Army Chief of Social Media, 26 Nov 2012.
[152] Interview with Chief of Staff, JTF-GNO, Apr 5 2013.

(8) Congress: Congress was a cautious supporter of social media and its Members consistently mention the need to balance security with openness. Senators and Congressmen desire to support their constituents, especially those serving in the Armed Forces and deployed and their families living back in the district. In the *National Defense Authorization Act for Fiscal Year 2008 Report*, Congress required DoD to provide a report after the restriction of the networks to social media in 2007.[153] They acknowledged DoD's need to preserve bandwidth and ensure operations security for military operations, but were concerned with the morale of the deployed troops and their ability to communication with their families while deployed. The Senate Armed Services Committee (SASC) asked DoD to report on the effect the web content restrictions have on the network and how DoD provided service members access to the commercial internet in deployed locations.[154]

(9) Media: The media does not have a single position on social media. Instead, journalists produce content that appeals to consumers in their market.[155] Journalists' sensationalist headlines influenced the public, service members', and policy makers' perceptions of social media. Headlines such as, "Social Media Sites Provide Morale Boost, Official Says,"[156] "U.S. Employees Set to be Forced to Give Bosses Their Facebook PASSWORDS," [157] "Taliban Infiltrate Social Media,"[158] "Air Force Seeks Fake Online Social Media Identities,"[159] and

[153] Senate Armed Services Committee. "National Defense Authorization Act for Fiscal Year 2008," U.S. Government Printing Office, Washington, DC, June 5, 2007.
[154] Department of Defense. "Department of Defense Personnel Access to the Internet."
[155] Gentzkow and Shapiro provide empirical evidence of this and that news content can have significant effects on the political attitudes and outcomes. Matthew Gentzkow and Jesse M. Shapiro. "What Drives Media Slant? Evidence from U.S. Daily Newspapers," *Econometrica*, Vol. 78, No. 1, Jan 2010, pp 35-71.
[156] American Forces Press Service. "Social Media Sites Provide Morale Boost, Official Says," *Armed Forces Press Service*, Washington, DC, March 17, 2010.
[157] Steve Nolan. "U.S. employees set to be forced to give bosses their Facebook PASSWORDS," *Daily Mail Online*, United Kingdom, April 23, 2013.
[158] Bill Gertz. "Inside the Ring: Taliban Infiltrate Social Media," The Washington Times, Washington, DC, August 22, 2012.
[159] Techweb. "Air Force Seeks Fake Online Social Media Identities," *TECHWEB*, Feb 22, 2011.

"Marines Social Media Ban is Bad for Morale,"[160] are examples of media headlines that could possibly have affected a service member's or policy maker's beliefs.

(10) Users: Military and civilian employees of the DoD. This group has many subgroups that have different issues with social media. DoD employees want to use social media for legitimate uses as well as recreational uses. A Marine Corps pilot told me that on his deployment, "Facebook was an absolute must. That's the way the younger generation communicates and that's also the way my younger Marines communicate with their parents and that's the way their parents communicate with us."[161] They want to use current technology and they want the ability to contact all of their friends and family members, not just the ones that can get access to a firewall. An Army Lieutenant deployed to Afghanistan during the interview said, "There were many times I contemplated deleting my Facebook account, but I didn't because I am in Afghanistan and it is my lifeline."[162]

Users also face the problem of proper conduct and the consequences that come with negligent use. Service Members are subject to military laws and punishment if they violate the trust their Commander has in them. In the absence of a specific social media policy at this time, users had to choose how to act on social media. When asked about choices, a young ROTC Cadet said, "It's making good decisions in whatever ways you are doing that, like throughout any aspect of your life. I would say with Facebook, it's the same thing. You don't put anything on there that's inappropriate or disrespectful. I just don't get why people post pictures of themselves doing illegal things on there." [163] Users are also concerned with security and privacy. Staff Sergeant Sweetnam, from the Army's social media office, points out that the enemy is not necessarily

[160] Bronk, Chris. "Marines' Social-Media Ban is Bad for Morale," *Federal Computer Week,* Sept. 17, 2009.
[161] Interview with USMC Lieutenant Colonel, Harrier Pilot, Nov 27, 2011.
[162] Interview with Army First Lieutenant, Afghanistan, Mar 4, 2013.
[163] Interview with ROTC Cadet #1, Oct 20, 2012.

nameless and faceless. It could be someone you just met. "Honestly, it's pretty scary how much an acquaintance that becomes a Facebook 'friend' can find out about your routines and habits. Make sure you are careful who you let into your social media circle."[164] Deployed users have different needs than stateside users. Deployed users do not always have easy access to alternate means of communications such as a personal computer or cell phone. There is also a subgroup of youth as its own social group and another group for high profile users who have an official presence which both have their unique challenges. Most of the service members I talked to wanted the ability to access social media at work on the military provided network. As DepSecDef Lynn argued, the military user wants to use the technology he/she has at home on commercial systems, at work.[165] Users are also united because they are subject to the policies of the DoD and have to abide by whatever policy is chosen at the top of the hierarchy.

As you can see, in 2009 there was a disparate collection of relevant social groups facing some shared and some unique problems and multiple proposed solutions to the issue of whether or not to allow social media on DoD networks. Back then, it was not predictable as to what direction the policy would go. Opinions on the final outcome were based on whatever organization the individual was from and its perceived gain or loss in the struggle. There were two different stabilizations where the DoD decided as a whole what the policy was on allowing social media on its networks.

2.5 Stabilization, Destablization, Stabilization

Pinch and Bijker define stabilization of an artifact as closing out a technology "controversy."[166] On May 15, 2007, there was a first stabilization and closure of the social

[164] Cheryl Rodewig. "Geotagging Poses Security Risks," *US Army*, Ft Benning, GA, March 7, 2012.
[165] Jim Garamone. "Lynn Discusses Social Media at Facebook Headquarters."
[166] Ibid.

media policy with the publication of the USSTRATCOM order to allow blocking the thirteen websites. In the military, there tend to be a lot of debate on open topics, but when an order is signed, it is permanent and the debate usually shifts to how to implement the new policy. As predicted by DoD's report to the SASC mentioned earlier, the JTF-GNO continued to restrict the policy over the next two years by increasing the number of websites on the blocked list. In actor network theory, Callon calls this stabilized state, "normalization."[167] Stability is achieved by standardizing and constraining actors and intermediaries. The JTF-GNO issued a standard order to all DoD network providers to block certain social media sites and all of the actors had to comply. The situation seemed like it was at closure.

However, Callon allows for "retranslation" which is for the network to destabilize and restabilize as something else based on the conflict and discord of the actors (or relevant social groups), which is exactly what happened. In late 2009, the DepSecDef directed the ASD NII/DoD CIO to develop a social media policy while communicating his intent to open the networks and allow DoD to use social media tools.[168] The first effort to write a policy was led by USSTRATCOM who developed an extensive, 18 page, hybrid policy that contained a structured process to allow and restrict certain websites. The DepSecDef and ASD NII/DoD CIO did not agree with the restrictive content, rejected the draft and directed them to develop a policy that was more permissive.[169]

During this timeframe, the Public Affairs Offices lobbied the DepSecDef and ASD NII/DoD CIO heavily for a more permissive policy. JTF-GNO, NSA, DISA and the Services were also favoring a hybrid solution involving blocking only certain sites and were contributing at the

[167] Callon, 151.
[168] Interview with Acting DoD CIO, January 20, 2011.
[169] Ibid.

headquarters level to the STRATCOM's version of the policy. The Congress was leaning toward a more permissive policy to support their deployed constituents and the media continued to publish sensationalist headlines framing the debate. Congress and the Media also thought the DoD should adapt to new social media tools along with the rest of the federal government. For the most part, the users were in favor of allowing access to social media at work as evidenced by the positive stories in the press about their use of Facebook and similar sites while deployed. The JTF-GNO had not yet ordered Facebook blocked and many users-service members and their families-were using it by the end of 2009 to stay connected during the twelve to fifteen month deployments.

The second stabilization and closure occurred on February 25, 2010 when DepSecDef Lynn signed the Directive Type Memorandum 09-026, "Responsible and Effective Use of Internet-based Capabilities" (also known as the social media policy). Unlike the first stabilization, the Service Chiefs were not briefed in the tank on the upcoming policy. The final content was debated by several relevant social groups: the DepSecDef, ASD NII/DoD CIO, USSTRATCOM, NSA, DISA, and JTF-GNO and the Services. By now, the use of social media was increasing rapidly on the commercial networks and was considered an innovative way to disseminate information quickly to a worldwide audience. Additionally, the ASD for Public Affairs had private meetings on the matter with the DepSecDef to communicate his position.[170] The relevant social groups containing the OSD civilian leaders used the discourse surrounding sociotechnological inevitability, youth and responsible online behavior to their advantage, while downplaying the security and privacy risks to convince the DepSecDef to direct a policy change. The discourse analysis supporting the policy change is covered in the next chapter.

[170] Interview with Mr. Price Floyd, ASD PA, May 29, 2013.

CHAPTER 3

A DISCOURSE ANALYSIS OF FACTORS THAT IMPACTED THE SOCIAL MEDIA DECISION

In this chapter, I will analyze the discourse of DoD personnel to explore how it affected the development of the policy to first block social media on military networks and then the sudden change to policy which openly allows and encourages the use of social media. The four discourses I will explore are risk to security and privacy, sociotechnological inevitability, responsible online behavior and youth—all centered on social media and the military. These four themes appeared the most frequently in the media and in the interviews I conducted with service members.

Within these discourses I will examine how STS and social science scholars have analyzed them, what the military institution says about them, and the view of the service members that I interviewed. I was inspired by Nancy Baym's use of discourse analysis in her book, *Personal Connections in the Digital Age*, where she states, "Rhetoric tells us little about the technology, but provides insight into how the technology came to be and how they came to be understood and used."[171] I adopted Baym's method of featuring the actual words of her interviewees to support the main points I will make in this dissertation. In this chapter, I will not analyze social media technology itself, but how the discourse affected the policy decision to allow social media on military networks.

3.1 Discourse and Why We Study It

"Discourse is the act of conversation (as diminished from language itself)…the analytical term descends from sociological studies of speech."[172] In *Leviathan and the Air Pump*, Shapin

[171] Baym, 43.
[172] Edwards, p. 34.

and Shaffer offer that discourse "produces power and knowledge: individual and institutional behavior, facts, logic and the authority that reinforces it."[173] Another author who inspired me to use discourse analysis as a method was Paul Edwards. In *The Closed World,* Edwards states competing discourses "vie with each other for dominance."[174] At some point, a dominant discourse wins out and stabilizes an object's development, at least temporarily in this case, and influences policy. The use of dominant discourse on the benefits of social media had the power to completely reverse the social media policy in the DoD from being completely restrictive to being completely permissive. In her study of digital communications, Baym said, "The choices that designers and developers make as they develop technology are dependent on their social context, in part shaped by communication"[175] and the final outcome is "usually a matter of compromise."[176] Though one of the leading STS scholars, Michel Callon warns us that, "the sociological explanation of scientific and technical controversies is as debatable as the knowledge and objects it accounts for."[177] Qualitative analysis is not an exact science, but we can extract many important insights from its use and applications.

Discourse analysis is particularly useful for understanding the decisions behind technology design and deployment and how these decisions reflect the local subculture. Langdon Winner believes we need to "study origins of technology" and also need to "study the consequences on society and how technology transforms personal experience and social socially constructed and society shaping."[178] In the case of social media and the military, I studied the origins of social media on the DoD networks and am now following with the consequences of the technology on

[173] Steven Shapin and Simon Schaffer. Leviathan and the Air Pump: Hobbes, Boyle and the Experimental Life. Princeton, NJ: Princeton University Press, 1985, p. 40.
[174] Edwards, Paul p. 38.
[175] Baym, Nancy p. 39
[176] Baym, p. 40.
[177] Callon, p. 3.
[178] Hughes, p. 51.

military society as seen through the perspective of service members. If we study how people perceive technology and the policy related to that technology throughout its development, we can understand how the technology arrived at stabilization and closure. Studying the discourse surrounding the decision to allow social media on DoD networks will allow me to discern why the sudden policy change from a network closed to social media to a network where it is openly allowed. Paul Edwards states, "Tools and uses form an integral part of human discourse and shape material reality…Tools shape discourse, but discourse also shapes tools."[179] In the case of social media in the military, the tools shaped the discourse. Words such as "friended," "pinned," "tweeted," and "Facebooked" came directly from social media and are already in wide spread use in service members' jargon. Conversely, senior service members' discourse on security and the concern for responsible online behavior initially led to limiting the use of social media tools on military networks. Shirky, who has studied DoD, adds a military perspective to the discussion by stating, "Organizational values and culture can similarly impede a military organization's ability to pursue certain types of innovation."[180] I believe Shirky is correct and that the military has a unique environment with its own values and prejudices that affect the discourse. What I explore in this chapter is how the discourse surrounding the DoD's social media decision was instrumental in shaping the outcome of the policy.

There are many techniques of discourse analysis. Discourse analysis examines how rhetoric can produce descriptions of a concept that appear factual and independent of the orator.[181] Edwards describes discourse as "a way of knowledge, a background of assumptions and agreements about how reality is to be interpreted and expressed, supported by paradigmatic

[179] Edwards, p. 28.
[180] Shirky, p. 50.
[181] Jonathan Potter. *Representing Reality: Discourse, Rhetoric and Social Construction*, Thousand Oaks, CA: SAGE Publications, 1996.

metaphors, techniques, and technologies and potentially embodied in social institutions."[182] Metaphors are replete in social media discourse and are particularly important to this discussion. Some service members try explain social media as another tool—like their rifle. They explain the danger they perceive by likening it to being vulnerable to well-known enemies such as North Korea or Adolf Hitler. Service members also explain the technology by comparing it to everyday objects like a billboard or a newspaper. They often exaggerate the appearance and staying power of social media in society by calling it an overwhelming wave, tsunami, or a genie that is let out of the bottle. Collins notes that, "Our language and our social life are so intermingled that our habits of speech help determine the way we see the world and thus help form the basis for social interaction."[183] This is definitely the case with service members and their use of social media.

One approach I used in my analysis is based on the work of Sanna Talja, from University of Tampere in Finland, who wrote a comprehensive article on methods to analyze qualitative interview data. Talja's issue with discourse analysis is that because the author selects the text used for each topic, "consistency is an achievement of the researcher rather than a feature of the participants' discourse, and the context-dependent nature and cultural logic of the answers are missed."[184] She states that the interviewees all see the object in a different context and therefore present differing opinions and experiences when discussing it. The researcher cannot conclude there is only one accurate version of the truth. Instead, the researcher must look for "significant patterns and variations"[185] in the interview data he or she collects. Some ways to interpret this data includes analyzing inconsistencies and contradictions in one participant's answers; seeking

[182] Edwards, p. 34.
[183] Harry M. Collins. *Changing Order*, Chicago, IL: University of Chicago Press, 1992, p. 11.
[184] Talja, p. 4.
[185] Talja, p. 8.

repeated references to the same explanations or arguments; and identifying "basic assumptions and starting points, which underlie a particular way of talking about a phenomenon."[186]

Accordingly, for each of the four topics in the this chapter, I grouped my sources according to shared institutional standpoints in order to reveal the cultural logic that shapes the "truths" expressed by official DoD statements, individual decision-makers, and individual service members. Finding common concepts among interviews and statements helps the researcher understand the constructions people have generated about social media use in the military and understand how it shaped DoD policy. My discourse analysis will explore the discursive threads of risk (security and privacy), sociotechnological inevitability, responsible online behavior and youth. I will address each discourse separately and for each one, provide insights from STS and social science scholars and views from the different perspectives of the DoD institution and from individual policy makers and service members. I will look at how the metaphors are used to describe the technology have added to the confusion over the effects of social media. I will also explore how the various discourses emphasize selective aspects of social media in order to uphold or undermine established patterns of hierarchy and social control. I will explain how the discourses surrounding the use of social media by the DoD institution and service members, in the areas of security and privacy risk, sociotechnological inevitability, responsible online behavior and youth, shaped the outcome of the policy debate and brought it to closure.

3.2. RISK

How have both the initial policy debate and current discussions been shaped by competing discourses about risk: for example, those focused on security vs. those focused on privacy? The discussion of risk is replete with metaphors such as leaving fingerprints behind on the internet,

[186] Talja, P. 8.

storing information in the cloud, and data mining. Service members use these terms freely without fully understanding the technical details involved and the security or privacy implications associated with them. These metaphors shape the debate by associating particular images with social media, encouraging service members to make assumptions about the riskiness of online behavior in the absence of facts.

Risk seems to be the topic most often raised by service members and other relevant social groups. Nancy Baym suggests there exists an "uncertainty on the net…people are not sure they can trust other people to be who they claim they are…there is a central problem of anonymity."[187] I decided to separate risk into two separate categories, security and privacy, after analyzing the service members' interview data. There seemed to be a natural dividing line between a risk to a military unit and personal risk to the service member, based on service members' concerns.

3.2.1 STS Frameworks for Analyzing the Concept of Risk

I looked at two primary STS risk theorists, Ulrich Beck and Milton Mueller who discuss choices associated with taking and avoiding risk. The threat of risk can cause action or avoidance and be an excuse to exert control. In his work *Risk Society*, Beck--one of the most prominent risk scholars in the STS field, states risk is "a projected cause of present (personal and political) action."[188] He suggests we can look at "risk as a stimulus to action…risk has to do with anticipation…a time bomb is ticking."[189] The threat of risk forecasts a future that people need to take conscious action to avoid its consequences. It can become a powerful incentive for action. However, it can also be used as vindication to avoid doing something. "The center of risk

[187] Baym, Nancy p. 32.
[188] Beck, p. 34.
[189] Beck, p. 33.

consciousness lies not in the present but in the future…we become active today to prevent the problems and crises of tomorrow."[190] According to Beck, risk avoidance is an acceptable course of action. In the case of social media and he military, risk was quoted by senior leaders and network providers as the reason to block social media on all DoD networks prior to February 2010. In keeping with Beck's theory, DoD was avoiding the constructed consequences of the dangers of social media by blocking social media from the networks.

Some STS scholars believe powerful people use the threat of risk as an excuse to exert control. In *Networks and States*, Mueller said, "Security more often than not is associated with efforts to reassert hierarchy and control."[191] He cautions, "Risk positions have to be born scientifically--latent side effect: admits and legitimatizes the reality of the hazard."[192] Mueller believes risk will be used to limit the power of the internet because it is public and unrestricted. "Security is a generic watchword that signals the downside of the internet's openness and freedom."[193] People in authority can use fear to control an action or event and even to encroach on basic rights. "The drumbeat of fear provides a textbook example of 'securitization'…speech acts that characterize some problem as an existential threat in a calculated attempt to justify extraordinary measures such as the suspension of civil liberties."[194]

If we follow Mueller's logic, senior leaders used fear to strengthen their argument for blocking social media on DoD networks. The use of fear may be true. However, in the case of the use of social media, DoD senior leaders were not just trying to assert control and limit basic human rights. By their rhetoric, we can see the DoD senior leaders were truly concerned about

[190] Beck, p. 34.
[191] Mueller, p. 159.
[192] Beck, p. 34.
[193] Mueller, p. 159.
[194] Ibid, p 160.

service members' security, safety and privacy. Unlike Mueller's theory of those in control boosting their own authority, DoD senior leaders believed they were protecting the security and privacy of the troops by restricting their use of social media.

In the absence of policy, service members had to make their own choices on the use of social media. Some chose not to use it at all to avoid the risk. Beck would say they were "no longer concerned with attaining something 'good,' but rather with preventing the worst--self-limitation is the goal which emerges."[195] The service members who chose to use social media believed the reward was worth the risk and that the use of social media was beneficial to their lives. In their discourse I found service members self-limited their actions online in order to protect their security and privacy. They were aware of the risks social media posed and believe their responsible actions could mitigate the risk. Reaction to fear is still a choice. Beck believes anxiety and fear alone should not drive actions. "Solidarity from anxiety becomes a political force… it is still unclear how the binding force of anxiety operates, even whether it works…so far, anxiety has not been a foundation for rational action."[196] Unlike the theories of Mueller, Beck's theory supports the actions of the service members who chose to use social media despite the risk and the actions of the DoD leadership who overturned the ban on the use of social media.

3.2.2 Department of Defense View on Risk

The DoD's normal approach to risk is different from what Beck and Mueller describe, since a high level of social control is already built into the system and a certain level of risk is accepted and inevitable and manageable. But DoD's social media policy did not conform to their normal approach and was more similar to the dynamic described by Beck and Mueller where the threat of risk was used as an excuse to initially block the use of social media on DoD networks. DoD

[195] Beck, p. 49.
[196] Ibid.

issues guidance and doctrine in the form of Joint Publications. These Joint Publications are applicable to the entire Department of Defense including the military departments, combatant commands, and other authorized agencies. Joint Pub 1-02, *Dictionary of Military and Associated Terms*, contains common definitions across military doctrine, and defines risk as "the probability and severity of loss linked to hazards."[197] It furthermore defines a hazard as "a condition with the potential to cause injury, illness or death of personnel; damage to or loss of equipment or property; or mission degradation."[198] This kind of statement is not the drumbeat of fear Meuller wrote about, but very real outcomes normally associated with warfare. At the time of the initial policy decision to block social media on DoD networks, some DoD senior leaders believed the use of social media could be hazardous to personnel, equipment or accomplishing the mission. They were not just asserting their will as a quest for power.

The Department has a whole institutional process to diagnose, assess and mitigate risks into everything it does. Unlike Beck's theory of risk avoidance, DoD does not profess that one should avoid risk, it merely states that negative events are inevitable and a commander should do everything in his/her power to control the outcome in order to safeguard personnel, equipment, and the mission. This process is called risk management which is defined as "the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefit."[199] Military Commanders are taught in their basic level schools to assess risk from the early stages of planning, all the way to the completion of an operation. A commander continually revisits and reassesses risks and develops mitigation strategies to counter the apparent hazards.[200] In DoD publications, risk is not used to

[197] JP 1-02, p. 236.
[198] Ibid, p. 119.
[199] Ibid, p. 236.
[200] JP 5-0, p. I-6.

assert control as Mueller suggests; the military, by nature, already has control of its personnel and can exert consequences on those who perform outside of the standards of conduct.

In the social media case, DoD publications did not match DoD leader views, especially on the military side. With the decision to first restrict use of social media on DoD networks in 2007, the discourse was very much framed by fear of the unknown and speculation that the use of it put national security at risk. Mueller said, "In late 2008, U.S. effort to reframe internet security as a national security issue dominated by militaristic rhetoric and a state-centric view of society."[201] Mueller was absolutely right as you saw in the policy maker discourse in chapter two, but the truth remains that there are not very many examples of social media causing operational problems; it is mostly speculation about what "could" happen. In the end, the DoD doctrine and risk processes prevailed and the decision to block social media on DoD networks was overturned. DoD doctrine now states, it is up to commanders to assess and mitigate the risk involved with the use of social media.

3.2.3 Service Members' Views on Risk - Security

Risk (to security and privacy) dominated most of the conversations I had with service members and policy makers on social media use of military personnel. Because of the volume of material available on risk, I will discuss security first and then privacy. One of Talja's methods of discourse analysis is to identify repeatable arguments to discern common themes from peoples' statements on a topic.[202] Common themes in the security risk arguments are that military communications are being monitored and scrutinized by the enemy, even if it's a personal social media account; the enemy can aggregate bits of information found on social media sites; the military has not done enough research on the effects of using social media; there

[201] Mueller, p 179.
[202] Talja.

is a balance that service members struggle with between security and the openness that social media provides; and many service members are concerned about being located, above all other fears.

Many service members believe military networks are a target and different from civilian networks. President Obama, the Commander In Chief of the military, voiced concerns of information technology security his first year in office, "It's the great irony of the Information Age – the very technologies that empower us to create and build also empower those who would disrupt and destroy…one of your greatest strengths, in our case, our ability to communicate to a wide range of supporters through the internet--could also be one of our greatest vulnerabilities."[203] The President alludes to threats but does not point to a particular enemy. In their discourse, military members sometimes point to the current villain such as Al Qaida or North Korea.

The current DoD CIO, Ms. Teri Takai cautioned the House Armed Services Committee that, "DoD networks are "under constant attack from cyber security threats" coming from both the web and malicious software.[204] An Army colonel draws a distinction between military and civilian society security posture in that, "In the military, we have a slightly different challenge in that we have to understand operational security and that can be a challenge in a social media connected environment."[205] The DoD ASD for Public Affairs admits there is a conflict between security and use of social media. While he personally believes use of social media is a great idea, he also recognizes the tension service members have while trying to accept this new

[203] The White House. "Remarks By the President on Securing Our Nation's Cyber Infrastructure," *Office of the Press Security*, May 29, 2009.
[204] Theresa M. Takai, DoD CIO. "Improving Management and Acquisition of Information Technology Systems in the Department of Defense," *Statement for the Record, House Armed Services Committee on Emerging Threats and Capabilities*, Washington, DC, April 6, 2011.
[205] Interview with Army Colonel, Feb 6, 2012.

concept and places security first as a DoD priority. He stated, "But most great ideas are followed by internal struggle and roadblocks…Security is the defense industry's utmost priority."[206]

Training service members was identified as a method to mitigate some of the risk. A Marine Corps captain believes DoD should use social media, but also that the military should train service members in the use of social media like the weapons training they receive in basic training. "Hey this stuff is something you are going to be allowed to use, but it is also something that is very dangerous…just like your rifle. It can cause a lot of harm to people around you if you don't know how to use it correctly."[207] The metaphor about the rifle is used to suggest that training service members to use something responsibly that could be dangerous can mitigate some of the risk involved. The possibility of the responsible use of social media is a theme in the security risk argument. A female Army lieutenant colonel, who now leads the Army's social media office, said the Army's top leadership are telling Army commanders to ensure their soldiers understand the risks involved with using social media. "I know the leaders in my office, that's one of the things they recommend. When they speak to the pre-command course, that's one of the things they'll say, 'You should know what your soldiers are doing, to include on social media and train them to use it responsibly.' I mean our top Army leadership is actually telling leaders to do that."[208]

Service members have their own ideas on what they believe the problem is. Some have clear, definitive ideas on the subject that are largely unsupported by facts. An Army colonel stated simply, "Anything you put out there online is being collected."[209] After DoD decided to change the policy on opening the networks to social media, An Air Force network provider commented,

[206] Price Floyd. "In Defense of Social Media," *The Washington Times*, March 21, 2011.
[207] Interview with USMC Captain, Jan 3, 2013.
[208] Interview with Female Army Lieutenant Colonel, Oct 30, 2012.
[209] Interview with Army Colonel, Feb 6, 2012.

"We've clearly increased vulnerabilities just by opening them up."[210] A captain in Iraq, also a network provider stated, "My personal opinion is that Facebook for DoD units should be banned. Facebook is good, but it is extremely hard to control."[211] A first lieutenant in Afghanistan observed there is risk because service members are not responsible. "For the most part, people don't pay attention to what they post. You see cool stuff in the military and you want to take pictures and share it with your friends."[212] None of these service members provided a substantive argument or any facts to augment their opinion that risk exists.

Another stated concern for service members is operational security (OPSEC) and the ability for an adversary to collect bits of data from a group of related people, perhaps all in the same unit, and put together a larger picture of what that unit is doing. A Marine Corps gunnery sergeant said, "My biggest concern is OPSEC and that you can track people as a group. All members of this unit that are on the same deployment may each post a small bit of data, but an enemy could aggregate that data and get a more complete picture of what the unit is doing."[213] An Army colonel agrees with him and says service members must be careful of what they post. "There is a danger with social media of the ease of use causing people to be less aware of what they are sharing and what a potential adversary can do when they assemble all the individual pieces…it's the traditional OPSEC puzzle. You may only talk a little bit of a facet of a piece of information but when the bad guy has enough ears listening, enough sources of information, they can rapidly assemble the entire picture from several discrete point sources."[214] A public affairs major said soldiers were not careful enough during his recent Iraq experience, "We saw pictures

[210] Interview with Air Force Colonel, Jan 10, 2013.
[211] Interview with Captain in Iraq, Nov 3, 2011.
[212] Interview with First Lieutenant, Afghanistan, Mar 4, 2013.
[213] Interview with USMC GySgt, Apr 6, 2012.
[214] Interview with Army Colonel, Feb 6, 2012.

posted to people's individual accounts. Some pictures of people that shouldn't have been out on the internet--you never know who can get a hold of it and what they will do with it."[215] He said one of his major challenges was he "constantly had to remind conventional units working with Special Forces that there are some different rules here--there were definitely some OPSEC mistakes made over there."[216]

A National Guard Colonel offered a hypothetical example of an enemy piecing together information found on a service member's personal social media page. "I also kind of worry about identity theft, because there is so much other information that you can find on the internet that they can pick up random things from Facebook…and then you can google search somebody and find out a lot of information about her. I mean they could just start piecing together little bits and pieces about who you are and use that either in identify theft or to get access. They could just piece together so much information that they could mislead somebody based on your information."[217]

Another public affairs officer had a different, more positive experience concerning the use of social media. She was deployed to Iraq for fifteen months and now works in the Army social media office. "I've been working in this environment for a while and we've had relatively few incidents where there have been postings online and something has happened and then things were bad…and you are talking about one million people in the military and so many of them are young people…a lot of them are deployed and talking about all kinds of stuff online. But, we have relative few instances where we've had to go clean up a mess from a social media post."[218]

[215] Interview with Army Major, Feb 25, 2013.
[216] Interview with Army Major, Feb 25, 2013.
[217] Interview with ARNG Colonel, Nov 2, 2012.
[218] Interview with Army Lieutenant Colonel, Public Affairs Officer, Oct 26, 2012.

Some service members were concerned that social media was too new to use right away and recommended the military study the risks involved against the return on investment. A three star general stated, "We haven't measured the value of social media to the operational mission. What is the value of connecting people using social media? The risks are pervasive and it only benefits a few people."[219] An Air Force network operations director had the same concerns as the general, that the DoD had not studied it enough to make the decision to open the networks to social media. He asked me, "Has DoD done anything yet to track how it affects us?" And he cautioned, "We have opened ourselves to a huge, huge security risk."[220]

While some service members have clear, definitive opinions on the security risk of social media use on military networks, others believe there is a delicate balance involving social media use and security and they struggle with its implementation. The DoD leadership was aware of this struggle. A DoD civilian policy maker stated that while they were developing and staffing the policy, "There was a conflict of interest between openness and security."[221] The Acting DoD CIO at the time told me, "It is imperative to share—but we live in a world where you have to balance the need for information security with the need for information sharing."[222]

Talja says that in discourse analysis you must look for inconsistencies and internal contradictions in interviewee's statements to discover where the conflicts lie.[223] In exploring the struggle between the openness of social media and the military's need for security, I discovered many inconsistencies in service members' statements. These inconsistencies portray the frictions within service members' own personal views about the benefits versus the risk of social media

[219] Interview with three star general, Feb 13, 2013.
[220] Interview with Air Force Lieutenant Colonel, Jan 28, 2013.
[221] Interview with DoD Civilian, Dec 20, 2013.
[222] Interview with former Acting ASD NII/DoD CIO, Jan 20, 2011.
[223] Talja.

use. A retired Army colonel said about social media, "When appropriately and properly used, it's a powerful STRATCOM [strategic communications] tool." Later on in the interview, he was talking about opening networks to social media and used some metaphors to describe the situation. "It's like accepting nuclear rockets in North Korea-we keep ignoring and appeasing. One day we'll look back on this, like we did with Hitler, and wonder, 'How could we let this happen?'"[224] In one breath, the colonel touts the use of social media and in the next, he compares social media to accepting nuclear weapons in North Korea and Hitler. That is a significant inconsistency which illustrates the conflict service members have between openness and security.

An Army captain stationed in Hawaii also wrestled with this topic and went back and forth in his statement. "I think the military should use it to an extent. However, I can see how it can open up areas for OPSEC violations and a bunch of different ways you can do things it's not regulated for…But it is a good way to keep up the communications with families, about unit activities--but it can also be used against you on that side."[225] An Army colonel explains the situation this way, "You end up with kind of a dilemma because with social media, you are trying to make as flat a set of connections as possible and the purpose of OPSEC is to restrict the need to know something to those who don't need to know it."[226] Neither the captain, nor the colonel offered one position over the other as the solution, merely that they were considering the implications of both sides of the argument. They were both undecided as to their own position on the topic and this shone through in their discourse.

[224] Interview with Army Colonel retired, Apr 5, 2013.
[225] Interview with Army Captain, Dec 6, 2012.
[226] Interview with Army Colonel, Feb 6, 2012.

The public affairs major offered the following vignette which also portrays an undecided position. "A couple of weeks ago there was a video of a soldier who posted some helmet cam [camera] footage of getting shot at while he was on patrol in Afghanistan. At first I thought, 'Hey this is great, this is showing America what's going on out there. This could possibly be used to inspire people to join the military--to give our public a sense of what it's like to be in Afghanistan.' On the second hand, you are looking at a video that hasn't been screened by anybody--that has a soldier getting shot--that has some questionable tactics by a unit, some disregard for standard procedures that are part of military operations and some compromising video of positions of in this case an MRAP [Mine Resistant, Ambush Protected-vehicle] was in over watch of a building, and some of our TTPs [tactics, techniques and procedures] that could have been revealed. At this point it probably would be naïve to think that the Taliban did not watch this video. Whether or not anything was given away or detrimentally affects our mission, you never know."[227] This vignette illustrates the major's indecision and speculates that this piece of video was already being used by an enemy.

A support contractor, also retired Navy, had a similar observation, "A soldier took an ordinary camera and posted an hour of his patrol saying, 'This is what I did today.' When I first heard of it I was horrified, there were calls signs and TTP's [tactics, techniques, and procedures] recorded and posted. There was a lot of guys who agreed with me. But then, one of the generals said, 'I think this is really good--people can really see what's going on over there and what the soldiers are doing day to day.' We had a really good debate about it after that."[228] Examining these inconsistencies reveals that service members are considering the implications of the use of social

[227] Interview with Army Major, Public Affairs, Nov 14, 2012.
[228] Interview with government support contractor, Apr 15, 2013.

media and are conflicted over whether or not social media exposes them to risk and deciding if that risk is worth the benefit.

One of the other repeatable arguments I discovered was the service members' fear of being located as both a risk to security and privacy. An Air Force lieutenant colonel stated, "Risk and bandwidth are the two main reasons for not allowing social media. Just being able to surf, you could violate OPSEC--giving away your location quite easily."[229] The fear of location spans all ranks from the very senior to the very junior. An Army National Guard colonel explains, "It's like where two points collided where Facebook was getting big and we were in the war in Iraq and Afghanistan. You'd hear a lot about troop locations--especially from family members. 'Oh, they are flying back tonight, or they are flying back Thursday and we are all going to meet them at the airport at a certain time.' That to me is very dangerous."[230] An Air Force lieutenant colonel speaks of the past without social media as more secure than the present. "Back then we didn't have cameras with GPS's, so you didn't have to worry, but now it's a problem. A lot of people posting 'I've arrived' and give out their location."[231] Likewise, A male ROTC cadet stated, "I feel like it can lead to a really big problem if someone is possessive or stalkers or rapists--if they figure out how to locate you. You can easily locate people with Facebook if you have the training to do so or the capacity to learn."[232] A male Army colonel cautions, "I think the potential is there for a problem. People post locations and vacations. Now everyone knows you aren't home. If someone is trying to track you down and target you, they can find you."[233] A female National Guard colonel was more interested in personal safety, than unit safety. "There's

[229] Interview with Air Force Lieutenant Colonel, Jan 28, 2013.
[230] Interview with ARNG Colonel, Nov 2, 2013.
[231] Interview with Air Force Lieutenant Colonel, network engineer, Jan 28, 2013.
[232] Interview with ROTC Cadet #2, Oct 20, 2013.
[233] Interview with Army Colonel, Feb 17, 2012.

a creepy element where people can stalk you and find out information about you and then track you down. I mean it gives you information about where people are, like if you are in a restaurant, you use an app for that, it will tell the world on Facebook where you are. That to me is really creepy if someone is in the area, they could just go over there and meet her--or see her or whatever."[234] One of the younger interviewees, the first lieutenant in Afghanistan concluded, "People like to stalk people and Facebook makes it easy."[235]

Another related problem that surfaced was concern about family members giving away location information. An Army captain in Iraq offered an operational example from his own personal experience. "I actually found out more information about the unit replacing us at a previous location just by going to their Facebook site. They had a basic task organization, messages referencing when they were going, and to top it off, the FRG [family readiness group] leader posted the exact moment they landed at one of the intermediate stops and the name of the airfield."[236] The captain was horrified to see that conversation happen on the open internet. A Navy pilot, commander of a fighter squadron, told me, "I used to have conversations with my Navy wives before deployments. One of my huge things was the use of social media--the same thing as 'loose lips sink ships.' Don't talk about 'Bobby's leaving for six months' or 'I'm so excited, the ship comes in tomorrow.' You are giving away vital information. I was friends with a lot of the junior officers wives on Facebook and I would still see them do that stuff. I would have to say to them, 'Hey will you please take that off? If not just for their sake, for your own safety. You're letting everybody out there, whether they are a friend or not, know that your husband is gone for six months and you are alone. I mean some predator knows that you are

[234] Interview with ARNG Colonel, Nov 2, 2012.
[235] Interview with First Lieutenant, Afghanistan, Mar 4, 2013.
[236] Interview with Captain in Iraq, Nov 3, 2011.

living by yourself. I always try to express that to them. A lot of people don't realize that there are people out there who will look at that stuff and use it for evil."[237]

An Army Major provided me with an excellent example of using information provided by social media in an operational setting to collect intelligence. The military conducts force-on-force exercises at combat training centers where a unit will come in to train and face an opponent called OPFOR [opposing force]. The purpose is for units to plan for combat operations by rehearsing all the steps they need to in order to deploy and fight in a realistic training environment. The resulting force-on-force battle is unscripted and anything can happen to change the course of events. The major said, "In my previous job I was an OPFOR company commander. When units came in to train we would filter through their personal online content to find a way to gain access to their FOB [forward operating base] while training. The incoming company commander's wife tweeted about their anniversary on the unit's Facebook family support page. I was playing a role and pretended I knew him. I told him we were stationed together in Korea, knew his wife's name and that he had an anniversary coming up and I just wanted to say hi. The next time I saw him, he gave me access to places he shouldn't have. I was in their TOC [tactical operations center-central command center], I saw their plans up on the walls. I was able to gain a lot of intelligence with just this one visit. He approached me at the end of the exercise and said, he simply just didn't remember me and I wasn't in any of his Advanced Course pictures. I told him I was the OPFOR company commander and he was shocked. I told him I just googled him on Facebook and suggested he should probably be using the Army approved Family Readiness Group site [which is behind an Army firewall] to stay in contact with his family, plus he should probably lock down his Facebook profile so the world

[237] Interview with Navy Commander, Feb 13, 2012.

can't see it. He was absolutely shocked, but it was a good lesson for all involved and thankfully it took place at the training center."[238]

The same major shared with me another incident where one of the soldiers in that same training unit, during the same exercise, posted pictures on Facebook of the inside of his Stryker combat vehicle.[239] Again, the soldier had an open Facebook profile and the OPFOR was able to exploit it. "There was a video on his Facebook profile where he pointed to an object inside the vehicle and said 'this is what I'm not supposed to tell you about but isn't it cool?' At the end of the exercise we showed the company commander all the OPSEC information we were able to collect on all of his soldiers-there was just so much out there that wasn't protected. He took it all to heart and had some serious lessons learned...He told me, 'You didn't look familiar but you knew so much about me and the unit that I trusted you.' The moral of the story is that you can put together a few pieces and get a pretty complete picture about the unit."[240]

The concept of security risk was a concern to service members. Common themes arose of an enemy exploiting service members social media accounts and piecing together information that could cause harm to DoD personnel or units; the struggle service members face between openness and security; the need for DoD to really study the effects of social media on the military environment; and the fear of being located through careless use of social media. It is clear that service members struggle to define their position on the use of social media. They are aware of speculated threats associated with social media, yet lack any concrete evidence of an enemy actually using social media against the U.S. military. The discourse surrounding the

[238] Interview with Army Major, Feb 25, 2013.
[239] http://www.army-technology.com/projects/stryker/.
[240] Interview with Army Major, Feb 25, 2013.

struggle between security and openness shows the immaturity of the use of the technology of social media by the military thus far and the need to further explore this topic.

3.2.4 Service Members' Views on Risk - Privacy

Service members had various privacy concerns about the use of social media. Many service members were concerned about posting appropriate content because it would always be associated with them. They are also concerned with creating bad publicity for the military. I found that service members were very concerned about their own personal privacy on social media as was the DoD as an institution. In April 2010, journalist Theresa Cramer wrote about the issue of what she called, 'the social military.' She stated, "The Defense Department was interested in Web 2.0 tools but had to weigh its extraordinary privacy concerns against convenience."[241] Service members used many metaphors when discussing privacy and the conclusion that there is no privacy on the internet shone strongly in the service members' discourse. The privacy discourse intersected with the responsible online behavior discourse when service members discussed their public persona. They liken a personal social media profile to being put on a billboard or in a newspaper for the world to see. Service members were adamant that it is a personal responsibility to set security controls and there was a need to 'lock down' a social media profile so it is only available to people who are allowed to access it.

The expectation of privacy seems to have changed because of the use of social media. An Air Force lieutenant colonel stated bluntly, "The definition of privacy has changed in my lifetime. The expectation of privacy is not there."[242] An Army captain in Afghanistan stated, "Whatever you put on there [social media] is no longer your private property. It's now open to the public-

[241] Theresa Cramer. "A Case of the Social Military," *www.econtentmag.com* (Apr 2010).
[242] Interview with Air Force Lieutenant Colonel, Jan 28, 2013.

anyone can go on there and take it. None of your information is protected."[243] Even in Afghanistan, she wisely does not trust the military network to secure her information on commercial websites. An Army colonel who works in network security believes, "Anybody who uses the internet who has an expectation of privacy doesn't understand how TCP/IP works. If you are on the internet, you are leaving fingerprints everywhere you go. If you are participating in any kind of commercial activity on the internet, if you do internet banking, then your privacy is an illusion."[244] A Marine Corps pilot told me he avoids social media for the privacy aspect, yet he still believes his information is not protected. "Just because I don't get on Facebook doesn't give me the impression I have any greater privacy."[245] The Army colonel, brigade commander, once again gave social media the benefit of the doubt. "There's a lot of myths on there about privacy--it doesn't reach into your wallet and publicize your credit card numbers."[246]

The very public aspect of social media is not lost on service members. As you will see in the responsible online conduct section later, service members believe you should conduct yourself as if all of your actions are public. Service members are concerned about bad publicity for the military. Incidents such as the pictures of Army soldiers mistreating Iraqi prisoners at Abu Grahib and the pictures of the Marines urinating on dead Taliban in Afghanistan brought negative attention to the military worldwide. An Army major told me that in his unit, "We have a 'billboard policy'. Don't post it unless you are comfortable having whatever you post end up on a billboard."[247] An Army colonel likened it to being published in the newspaper. "Anything you put out there online is being collected. I try to remember that as I use it and I try not to post

[243] Interview with Captain in Afghanistan, Nov 20, 2012.
[244] Interview with Army Colonel, Feb 6, 2012.
[245] Interview with USMC Lieutenant Colonel, Harriet Pilot, Oct 27, 2011.
[246] Interview with Army Colonel, Brigade Commander, Nov 11, 2012.
[247] Interview with Army Major, Feb 25, 2013.

materials that I would not be comfortable seeing on the front page of the Washington Post."[248] A different Army colonel stated that training soldiers about the public nature of social media is necessary. "We've got to train all of our soldiers what is acceptable to be in the public domain, as opposed to what stays in the military domain because of operational security. Some may think they are making innocuous comments, but may not know the information is private."[249]

Some service members were just not that concerned, because they believe they are already acting responsibly and have nothing to hide. A Navy captain said, "So I'm not really all that concerned about privacy, but I don't really put anything out there that I'm really worried about. I haven't really done anything that I'm really worried about."[250] A female Marine lieutenant colonel stated her conduct is beyond reproach. "Being military is just public record basically. No, I don't worry about PII [personally identifiable information] stuff. If anyone wants to analyze my buying habits, have at it, because there is nothing kooky there."[251] However, an Army colonel says there is always room for improvement and service members need to look out for each other online. "There are absolutely people who have posted things, where you write them or call them and say, 'Do you understand what you just did?' and they are surprised."[252]

A ROTC cadet gives this example of his own personal responsibility on social media. "If you have nothing to hide, I don't think social media is bad. I don't have anything to hide, I don't care if people look at my stuff. If you google my name you'll see some stuff and that's it. There's probably one or two pictures of me in college that I might be a little bit red eyed with a bud light in my hand with my arm around some of my friends and stuff, but there's nothing crazy

[248] Interview with Army Colonel, Feb 6, 2012.
[249] Interview with Army Colonel, Feb 17, 2012.
[250] Interview with Navy Captain, Jan 3, 2013.
[251] Interview with USMC female LTC, Oct 30, 2012.
[252] Interview with Army Colonel, Feb 6, 2012.

in there. Nothing I'm ashamed of."[253] That was an interesting statement as he was not twenty one yet and should not have posted pictures of himself drinking alcohol online because it is illegal. The last two examples, the discourse implies that there is a boundary between normal behavior that is acceptable online and irresponsible behavior that should not be posted online. Many service members feel privacy is only a concern for those who have something shameful or illegal to hide. They believe social media is only a danger if one is irresponsible with it.

The metaphor of securing or locking down one's profile, in order to secure one's privacy, was a recurrent theme. The service members I interviewed, believed it was an individual's personal responsibility to set their security controls and restrict their personal profile so it was available to only those whom the owner chose to access his/her profile. An Army National Guard colonel stated, "Just in general, I have all of my stuff locked down. I just think there is way too much sharing."[254] An Army captain in Afghanistan said he is careful with his personal social media profile. "I am very concerned about privacy. I just make sure I don't post or put anything on there that I don't want anybody to see. At a minimum you can block certain people."[255] A ROTC cadet cautions about accepting relationships with strangers on social media. "I've gotten friend requests from people I've never met before and I don't know who they are. If I've never talked to you or seen you in my life, I'm not going to say you are my friend. I'm not going to let you know what's going on--I have no idea who they are."[256]

An Army National Guard major provides a hypothetical situation of what can happen if you mix work friends with your social media profile. "The negative is people who lack discretion. For example, my personal policy, I'm not Facebook friends with any of my downstream or

[253] Interview with USMC Captain, Jan 3, 2013.
[254] Interview with ARNG Colonel, Nov 2, 2012.
[255] Interview with Captain in Afghanistan, Nov 20, 2013.
[256] Interview with ROTC Cadet #1, Oct 20, 2012.

upstream coworkers and mine is locked down so they can't see it as friends of friends. The personal discretion negative part is let's say I work for you and I go home after a rough day and I say, my boss is such a pain in the butt. And I just broadcast that to the world. It's unprofessional, it's court martial-able [sic] in our particular arena because you just disparaged a higher ranking officer. Those are negatives that we haven't gotten around to yet."[257] The Army captain in Afghanistan agrees to separate family member information from work information. "For privacy, I try my best to block certain things and restrict certain people from seeing certain things I don't want them to see. There's some information like pictures that are just for family members only. I try my best to restrict as much information as I can or just not post it because I don't want it to be seen by the public."[258]

A female Marine told me she did not and would not ever have a Facebook page. When I asked her why she said, "My privacy issue is I'm a girl and I have a girlfriend. And I'm in the Marine Corps which is not so accepting of a girl with a girlfriend. Ergo, I have a privacy problem."[259] This Marine feels the loss of privacy due to social media would open her up to criticism and possible affect her performance ratings and perhaps limit her future opportunities in the Marine Corps. In an opposite example, a female Army officer told me she used social media to hide her homosexuality from the military. She would attend military events with a male friend and ensure many pictures were posted to Facebook so the military would not question her true sexuality.[260]

A Navy fighter pilot struggles with social media and privacy and had some pretty inconsistent thoughts. First he states, "I think you have to set up your privacy settings correctly. I had mine

[257] Interview with ARNG Major, Oct 31, 2012.
[258] Interview with Army Captain in Afghanistan, Nov 20, 2012.
[259] Interview with female Marine, October 30, 2012.
[260] Interview with female Army officer, Nov 8, 2011.

as public access, anyone could see it. I originally didn't see a problem with that. I had my work, my kids, where I lived, my family. My phone number was even on here. I was stupid enough to allow that to be public access--I've since changed it. I think you shouldn't list your occupation, particularly if it's military. You shouldn't divulge your navy.mil address, or your Joint Staff email address either."[261] Yet, I am Facebook friends with this officer and his Facebook profile right now contains a picture of him in his Navy uniform.

In another example of personal responsibility online, the Commandant of the Air Force Academy Preparatory School said, "We don't provide specific social media training as a formal class. In my first Commander's call to them, I talked about social media in a larger construct—there's good use of it and bad use of it. The cadets have to watch what they put on Facebook. An example is the Walter Canyon fire. Our basic training for the year started in the middle of the evacuation. The 10th Airbase Wing Commander was trying to get his arms around the fire response, as well as cope with the inaccurate dissemination of information and also inquiries as to its effect [on the base]. There were a lot of rumors that the cadets were spreading. There was a lot of exaggeration and what they didn't know, they filled in the missing information with what they thought should be the right information, but it wasn't accurate."[262] She also shared that young cadets do not really understand that whatever they post is not private. They also do not understand that the school leadership monitors Facebook. "We're working issues right now that surfaced on Facebook. One had an improper relationship--you could tell that from the Facebook posts. Also, two cadets had a physical confrontation and had a no contact order--they violated that—you could tell from their Facebook posts. It is maybe not an intended thing with the policy, but cadets are so free with using Facebook that it is helpful with the investigations we

[261] Interview with Navy Commander, Feb 13, 2012.
[262] Interview with Female Air Force Colonel, Jan 3, 2013.

need to do. It's not just us going out to find the information. The cadets will turn each other in and point the leadership to a Facebook page if somebody violates the honor code--that makes it easy."[263]

One of the stories that went viral in 2012 was about U.S. Marines urinating on Taliban corpses.[264] The incident was filmed in July 2011 and showed four Marines looking around before urinating on the corpses. The video did not surface on the internet until January 2012, but when it did, it went viral. This story was mentioned as an example of irresponsible and unacceptable behavior by several service members when discussing privacy on social media. An Army public affair major said, "But then at the other end of the spectrum we have service members doing things they are not supposed to be doing--conduct unbecoming, military members--whether its urinating on corpses, whether its cutting people's fingers off and posing with them, videos of things that should not be done, abuse of government funds, abuse of people, commission of crimes. Now that's the other end we have to deal with. We are pretty good at prosecuting those and doing something about it when they come to light. But the thing is, especially with the media it would be hard to control, we find out after the fact probably 99 times out of 100. So that's another way of prevention. It's one of those gaps, it's one of those risks that Commanders take."[265]

A Marine Corps infantry captain said, "I knew they were going to do it. Marines are going to take pictures of dead bodies. We don't need it [the behavior]. The Marines have undergone some pretty serious black eyes in the last couple of years, especially for the urination video. It's not worth it."[266] The Army captain stationed in Hawaii asked, "What about the Marines who

[263] Interview with Air Force Colonel, Jan 10, 2013.
[264] Lee Ferran. "Marine Who Urinated on Taliban Dead Says He'd Do It Again," *ABCNEWS*, July 17, 2013.
[265] Interview with Army Major, Public Affairs, Nov 14, 2012.
[266] Interview with USMC Captain, Jan 3, 2013.

urinated on the dead Afghanis? How was that appropriate to post? And who puts themselves out there like that?"[267] A female Army lieutenant colonel brought up the subject when discussing responsible conduct. "But I do think that some of the self-correction occurs because of the publicity around when someone makes a mistake. There have been times when that has been all over the news. Usually in a derogatory sense-like when the Marines were peeing on dead bodies. Obviously that's extreme but I think at large everyone sees when putting something like that out there is bad. And they see what happens to those people and then they think maybe I shouldn't do that."[268]

The discourse of security risk was different than the discourse of privacy risk. The security risk discussions were focused on a service member putting a unit or a large group of people at risk by his/her actions on social media. Senior leaders were concerned that service members would put themselves or the unit at risk through the careless use of social media, such as giving out unit location data. As a result the DoD networks were initially blocked from allowing access to social media sites, despite the lack of empirical evidence to back up the claims of security risk.

The privacy discourse was focused on a service member's personal conduct. The privacy discussion began with service members questioning the existence of privacy online and concluded with a service member's personal responsibility to exert self-control and the ability to control online content through his or her actions. There were many metaphors for conducting oneself as if in the public eye at all times, such as a newspaper or billboard. There was also a concerning conclusion that if one conducts oneself appropriately, he or she is safe online, no matter the content posted. This is not a logical conclusion, yet it is the one most often cited. What shines through in the privacy risk discourse is that service members clearly pride

[267] Interview with Army Captain in Hawaii, Dec 6, 2012.
[268] Interview with female Army Lieutenant Colonel, Oct 30, 2012.

themselves on being responsible and acting properly in public. Privacy risk is perceived as a personal responsibility, not one the organization is responsible for.

3.3 SOCIOTECHNOLOGICAL INEVITABILITY

How does the discourse of sociotechnological inevitability affect the policy debate? Does it conflict with the risk discourse? Technological inevitability is a deterministic theory about technological change. I use the term 'sociotechnological inevitability' in this dissertation to ensure the focus in on the 'social' element and how people react and adapt to the technology, not the technology itself. The argument for utilizing this theory to classify a technology is that when a technology is introduced, people will use it and over time, its use will cause the technology to evolve into something even more useful than intended at first. Technology is expected to be fully utilized by society and its social structures may change because of the technology. A criticism of sociotechnological inevitability theory is that it assumes the technology will succeed and become useful. There is no room for technological failure in the theory. Another criticism of this theory is that the technology itself is emphasized as the agent of change, rather than the social implications of it. The evidence of sociotechnological inevitability can be seen in the emerging vernacular of the public. The use of terms such as Twittered, Facebooked, Friended and Pinned as verbs show wide public acceptance of social media's continued presence in the world. Peoples' choices to share or not share the details of their private lives, online and publicly, are influenced by the fear that they will be "left behind" if they do not participate. This belief in the inevitable certainty of the future seems to actually foreclose debate over the use or non-use of social media by the military.

Social media use is part of a larger socio-technical system that extends beyond the military's control. Thomas P. Hughes, an American Historian of Technology and emeritus professor of

history at the University of Pennsylvania, believes it is possible for technological systems to acquire momentum and velocity from relevant social groups and actor networks.[269] When the technology is young, it is assumed to acquire momentum by social groups with vested interests, fixed assets, and sunk costs. In the military environment, social media seemingly acquired a technological momentum in DoD due to overwhelming support from users, the Congress, Public Affairs offices and even most of the Service Headquarters (except the Marine leadership). Because of the appearance of forward momentum of social media in society, the relevant social groups did consider partial solutions such as the hybrid solution of blocking only some social media sites or creating DoD only social media sites, in lieu of not being able to use social media at all. There was an assumption by DoD leadership and service members that the use of social media would somehow enhance the military's mission.

3.3.1 STS Frameworks for Analyzing the Concept of Sociotechnological Inevitability

In his paper on large technical systems, Hughes said, "Technological systems, even after prolonged growth and consolidation, do not become autonomous; they acquire momentum. They display a rate of growth suggesting velocity."[270] Baym stated in her study of digital communications that enablers such as "The internet and mobile phone came out of nowhere and took over our lives."[271] Many STS scholars believe the new technologies are changing the world and people's behaviors. Some service members said the same thing about social media. Shirky notes that, "We are living in the middle of a remarkable increase in our ability to share, to cooperate with each other and to take collective action, all outside the framework of traditional institutions."[272] Baym agrees with Shirky, but reserves judgment on whether that change is

[269] Hughes, 76-77.
[270] Hughes, p. 76.
[271] Baym, 150.
[272] Shirky, p. 20.

positive or negative. She believes, "Digital media aren't saving or ruining us or reinventing; they are changing the way we relate to others and ourselves in countless, pervasive ways."[273]

The change social media is causing in society is driven by peoples' desire to be connected to other people. Baym said humans drive to be social and connect is a guiding force in how society has transformed because of social media.[274] Shirky said the use of these technologies have spread beyond academic and corporate settings and are now fundamental in peoples' personal lives.[275] An associate professor at the Chinese University of Hong Kong, Jack Qiu, agrees there is transformation in society and attributes it to the widespread availability of mobile equipment.[276] Shirky agrees, but claims a technology has to have a sponsor who believes in it. "Historically, the success or failure of tactical architecture innovation has been dependent on the success of a product champion successfully positioning an innovation in a matter that enabled existing organizational leadership to support it."[277] In the case of social media, there was not much need for a champion to entice service members to use it, but there was a need for a champion in DoD to force the leadership to embrace it. The use of social media by service members on their private networks quickly became popular. It was a much harder feat to get the DoD leadership to embrace it.

STS scholars believe social media is indeed changing society and the way people connect and communicate with each other. According to these scholars, social media seems to have acquired momentum as evidenced by peoples' widespread use of the technology and possibly because of the easy availability of mobile handsets.

---

[273] Baym, 153.
[274] Baym, 151.
[275] Shirky, p. 21.
[276] Qiu, Jack. P. 127.
[277] Shirky, p. 51.

3.3.2 Department of Defense Views on Sociotechnological Inevitability

In order to get to what the DoD thinks about sociotechnological inevitability, we must explore the DoD's expectation for technological superiority, which is the belief that the U.S. armed forces must have the latest and greatest technology. Both sociotechnological inevitability and technological superiority assume success of the technology before implementation. The DoD leadership believes technological superiority over the enemies of the U.S. is imperative to accomplishment of its mission. The DoD releases the *Defense Strategic Guidance* approximately every four years to shape the direction and future of DoD's actions. In the most recent *Defense Strategic Guidance* released in 2012, President Obama, in his role as the Commander in Chief of the Armed Forces states, "As we end today's wars and reshape our Armed Forces, we will ensure that our military is agile, flexible, and ready for the full range of contingencies. In particular, we will continue to invest in the capabilities critical to future success, including intelligence, surveillance and reconnaissance; counterterrorism; countering weapons of mass destruction; operating in anti-access environments; and prevailing in all domains, including cyber."[278] In the same guidance, Secretary of Defense Panetta said, "The Joint Force for the future will be smaller and leaner, but will be agile, flexible, ready, and technologically advanced. It will have cutting edge capabilities, exploiting our technological, joint and networked advantage."[279] Both the President and the Secretary of Defense stressed DoD's need to strive for the technological advantage in the Department's highest level strategy document. Some DoD leaders confuse technological superiority with sociotechnological inevitability. The assume that just because a technology is new, it will be superior.

[278] Department of Defense. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Washington, DC: Office of the Secretary of Defense, Jan 2012.
[279] Ibid.

The Chief Technology Officer of the DoD, Mr. Al Shaffer, was recently asked what his priorities were for research and development. He replied, "We do research and engineering for three purposes. The first is to mitigate current or emerging threats from potential adversaries. The second reason is for affordability, to make current and future systems more affordable. The third reason that you do research and engineering is to create technology-based surprise for any potential adversary out there."[280] An example of 'technology-based surprise' is a new technology, such as development of an inertial measurement unit that provides troops their location without using the global positioning system (GPS). Then, if an adversary's only countermeasure is to jam U.S. GPS, it will not affect the service member's knowledge of his/her own location. This type of technological development assumes whatever product is developed will be able to "surprise" the enemy. It does not account for failure.

The leaders in DoD believe superior technological development is necessary for success. Secretary of Defense Gates previously assumed superior technology would help the U.S. to defeat Al Qaida. In a lecture in 2007 he stated, "It is just plain embarrassing that al-Qaida is better at communicating its message on the Internet than America."[281] Gates reiterated that point many more times since then. In 2008, he lamented, "Are we organized properly…when we're being out-communicated by a guy in a cave?"[282] In this case, Gates was disappointed the Taliban was subverting the U.S.'s superior communications technology. During the development of the latest communications equipment, the U.S. military leadership assumed the

[280] Defense News. "Interview with Al Shaffer; Acting U.S. Assistant Secretary of Defense for Research and Engineering," *Defense News Online*, Oct 23, 2013.
[281] Miles, Donna, "New Public Affairs Chief Sets Out to Transform Communications Processes," American Forces Press Service, Washington, DC, June 15, 2009.
[282] Ibid.

technology would give them the tactical advantage and in the Taliban's case, it did not. Therefore, sociotechnological inevitability is a flawed concept.

Ms. Teri Takai, the current DoD CIO, told lawmakers on Capitol Hill, "The increasing use of social media, smart phones, and tablet computers has made information sharing an expectation."[283] Other supporters such as Lieutenant Colonel (retired) John Nagl, claim that the more successful people are those who embrace social media. "Such discourse throws military conventions on their head and challenges the traditions of the chain of command that assure the smartest people able to make decisions are at the top…Innovative, forward-looking officers are clearly all over it."[284] A third view, held by Colonel Thomas D. Mayfield III, the Chief, Plans Division (G3), Headquarters U.S. Army Europe who cautions that not adopting social media can hurt the organization. "Failure to adopt these tools may reduce an organization's capabilities over time"[285] and "If military leaders do not fully understand these tools, they may miss their significant impact on the nature of future conflicts."[286] Another view that surfaced many times during my interviews with service members. "If you aren't there to communicate your message, someone else will do it for you."[287] Inevitability was a very powerful argument during the social media debate. Many service members and policy makers felt that social media use was unavoidable and would not be a choice. One Air Force Colonel told me, "Social media was a

[283] Takai, Teresa M. "Improving Management and Acquisition of Information Technology Systems in the Department of Defense," *Statement for the Record, House Armed Services Committee on Emerging Threats and Capabilities*, Washington, DC, April 6, 2011.
[284] Gordon Lubold. "Military Brass Joins Wired Troops." *Christian Science Monitor*, Boston, MA, January 21, 2009.
[285] Wells/Drapeau
[286] Thomas D.Mayfield III. "A Commander's Strategy for Social Media," *Joint Forces Quarterly*, Issue 60, 1st Quarter, 2011.
[287] Perry, Chondra. "Social Media and the Army," *Military Review* 90 (Mar-Apr 2010).

driving force; we've been overwhelmed."[288] These officers assumed the technology's use would be successful and that social media would somehow create a better way of doing business.

The Major General who previously worked at JTF-GNO said, "We saw a push to move towards these capabilities by the government…you hear about benefits for personal and operational use; keep the younger generation interested."[289] Another policy official, in the Marine Corps, involved at the time confided, "We were in the discussions, but we were being talked to, not being asked. The Vice Chairman of the Joint Chiefs of Staff was pushing hard. He wanted the public affairs guys using it."[290] A third policy official agreed that change started at the top level, "Internal cultural change about social media started with the Vice Chairman of the Joint Chiefs of Staff."[291] From the family side, there are many indicators of technological momentum. When asked about social media, Army wife, Mrs. Tara Crooks, stated "Use of these sites has boomed. I don't know a military family member who isn't on Facebook."[292] An Airman in the Delaware National Guard insinuates the change is evident and permanent, "I can't imagine deploying for long periods of time and relying on letters."[293] For others, the move to social media had great velocity. "It wasn't about one side or the other winning or losing, social media won…social media and the need to communicate was huge and tremendous-almost like a tsunami. It overwhelmed them."[294]

Mr. Price Floyd, the ASD for Public Affairs, believes the momentum had already caught the attention of the Secretary of Defense. "I wasn't trying to convince anyone because the decision had already been made by Secretary Gates. When I did my job interview with Secretary Gates,

[288] Interview with Colonel (retired), April 5, 2013.
[289] Interview with Major General, US Army, Apr 27, 2012
[290] Interview with policy civilian, March 20, 2013.
[291] Interview with policy action officer, April 15, 2013.
[292] Mike Chalmers. "Social Media Allow Military Families a Deeper Connection," USA Today, November 24, 2011.
[293] Ibid.
[294] Interview with Chief of Staff JTF-GNO, April 5, 2013.

he challenged me to bring social media to the men and women of the Armed Forces. We discussed the new social media tools that were now available and he said, 'Go make it happen.'"[295] Secretary Gates confirmed this in an interview with the *American Forces Press Service*. He said he "charged Floyd with enhancing the Department's outreach, particularly to 18-to-25 year olds in the military, in the United States, and around the world."[296] Like other senior DoD leaders, Secretary Gates assumed the use of social media would be a better way than the current method of recruiting and retaining younger service members. At the time, there was no evidence to suggest that this was the case. It is interesting to note that while Secretary Gates was charging Floyd with using social media, the generals in the Tank were simultaneously deciding to restrict the use of social media on DoD networks.

3.3.3 Service Members Views on Sociotechnological Inevitability

According to Talja, basic assumptions and starting points can be discerned from the discourse surrounding a subject.[297] In the subject of sociotechnological inevitability of social media, service members made three assumptions. First is that social media will be a successful technology that changes (or has already changed) society. Next is the DoD must keep up with the civilian world in social media; there is also a basic conjecture that the military is somehow falling behind the rest of society and needs to catch up. Lastly there is a morale dynamic. People connect or excuse their use of social media as a direct result of the social media use of family and friends.

General Martin E. Dempsey, the Chairman of the Joint Chiefs of Staff, believed in the inevitable success of the implementation of social media. The first time he ever saw a Facebook

[295] Interview with Mr. Price Floyd, May 29, 2013.
[296] Miles, Donna. "Gates, Mullen: Communications Technologies 'Strategic Asset' for United States," *American Forces Press Service*, Washington, DC, June 18, 2009.
[297] Talja.

page was on an iPad in between meetings in 2010. He said, "I don't really understand this, but I know it's big."[298] Dempsey was a quick learner and an early adopter of social media. He hired contractors to develop his official social media presence as he started his new job, first as the Chief of Staff of the Army and later as the Chairman of the Joint Chiefs of Staff. Dempsey is personally involved in the content displayed on his sites and does not want the content to sound like it was written by his Public Affairs Officer, instead of himself. He gained 5,000 followers in the first three months.[299] Today Dempsey has over 53,000 followers on his Facebook page and he continues to generate his own content.[300] In fact, General Dempsey hosted his first Facebook Town Hall on December 5, 2013 where he asked service members and families to post questions and he answered them in real time. It was a very successful event, in which the general took on a range of topics that were hot in the news at the time such as budget cuts, sexual assault and closing stateside commissaries.[301]

There is a discourse among service members on how social media changes society and how that change is inevitable. Shirky professes that social media is changing society and encourages collaboration. "Social tools don't create collective action—they merely remove the obstacles to it. These obstacles have been so significant and pervasive, however, that as they are being removed, the world is becoming a different place."[302] An Army Lieutenant Colonel believes, "Social networking is changing society only because it is a part of society. Where it wasn't before so society has changed because of it."[303] An Air Force Colonel was adamant that social media has changed society and can never be taken away. "Once you are granted a privilege, it

[298] Interview with Army Captain, Apr. 3, 2013.
[299] Ibid.
[300] https://www.facebook.com/GENDempsey.
[301] Jim Garamone. "Dempsey Addresses Issues During Facebook Town Hall," *American Forces Press Service*, Dec. 5, 2013.
[302] Shirky, 8.
[303] Interview with Male Lieutenant Colonel, Oct 20, 2013.

becomes a right…what are you guys Communists? You can't take it away now, we've become so dependent on it."[304]

Two main themes on how social media changes society is that it affects communications, especially face-to-face interaction and that everything happens faster when social media is used. Some service members were concerned that people are so dependent on electronic communication and social media that they will lose the ability to interact with other people face-to-face. A Marine Corps Colonel speculated, "I think it's going to hurt the next few generations--they will have a hard time communicating…interacting with people because it will all be social media."[305] An Army Lieutenant Colonel agrees with him, "People forget how to interact on a personal level, they forget how to communicate face to face."[306] A First Lieutenant deployed to Afghanistan believes that not only do people not rely on face-to-face communications any more, they jump to conclusions if the answer does not come back immediately. "Social media destroys conversation. We have become so disconnected. I mean you send an email and it takes people two days to answer back and that's unacceptable—people have already written you off."[307] A female Army Brigade Commander argues the opposite. In her current and previous jobs, she attempted to start a Facebook page for the organization and could not get her subordinates to buy into social media. One of the biggest complaints she heard back was that they believed it ruined human contact, which is important to soldiers. She disagreed wholeheartedly. "I talk to people about Facebook because I want them to use it and Army officers tell me, 'I won't use Facebook because it will replace face to face interaction.' Can you believe that?"[308]

[304] Interview with Air Force Colonel, Jan 10, 2013.
[305] Interview with USMC Colonel, Nov 1, 2012.
[306] Interview with Army Lieutenant Colonel, Jan 17, 2013.
[307] Interview with First Lieutenant, Afghanistan, Mar 4, 2013.
[308] Interview with Army Colonel, Brigade Commander, Nov 11, 2012.

Fort Huachuca has a human intelligence school where soldiers learn how to build rapport with the local populace of other countries where the United States may be involved in operations. "They learn basic questioning, screening and interrogation techniques" and pass the intelligence they collect to their headquarters.[309] I have an Army friend who teaches at that school and he told me, "The soldiers today…we are experiencing a 20-24% attrition rate. People cannot pass the courses we are teaching them because of their inability to engage one on one in a conversation, because they grow up with the social media and texting where it's so impersonal. They can't carry on a conversation and they can't even write a paragraph on what they just talked to the person about--and it's because of social media and the technology today."[310] I asked him to elaborate on that and he continued, "First they can't carry on a conversation, I don't know if it's a matter of memory. They don't have to write the way we had to write. Everything is condensed, like LOL--the way they write is abbreviated. What is really hard for them to do is show empathy or identify with what the other person is talking about, because it's been so impersonal via social media, because you don't see the emotion of that person. When you see them in person you can see their facial expressions and can understand what they are conveying to you. But when it's done over the internet or text, it's not emotional.[311] This colonel truly believes social media is contributing to the downfall of the profession in human intelligence. In this case, he did not assume success, he assumed failure. He was no open to the possibility that his students, who spend a lot of time online, could possibly develop new techniques for gathering human intelligence online.

[309] Cory Marshall. "Intel Training: 90YS Goes Inside Ft. Huachuca's Military Intelligence Training, *KGUN9 News*, Ft. Huachuca, AZ, Nov. 8, 2013.
[310] Interview with Army Colonel, Jan 19, 2013.
[311] Interview with Army Colonel, Jan 19, 2013.

My other friend who was a former West Point professor backs up the Colonel's statement about younger officers not knowing how to write. She said of her students, "Their lab reports were terrible. I remember thinking where did they learn how to write?"[312] A Marine Colonel agrees with her. "That's what I meant by the next generation. They're going to have trouble standing in front of people, they're going to have trouble articulating, they're going to have trouble writing because most of the writing for social media isn't academic writing."[313] Another friend, a Marine Corps lieutenant colonel spoke with the commanding officer (CO) at officer candidate school (OCS) about the ability of the candidates to communicate. "The CO at OCS talked about college graduates coming to OCS. The lack of ability to communicate is shocking. You put them in a room and give them a few pieces of paper--and they are supposed to write an essay. I kid you not, one guy misspelled his name three times. They are challenged just to write a full sentence."[314]

When discussing how the use of social media could change military society, service members made assumptions about the success or failure of the technology. They were speculative about people losing the ability to communicate face-to-face and even to write academically. Within this theme, there was a lack of facts or research to back up any of these claims.

Another discourse thread on how social media changes social action in society is that everything is faster. The two public affairs officers I interviewed had some very strong opinions and examples of how the use of social media has positively influenced their ability to do their jobs. I conducted these interviews several years after the social media policy was implemented, so their statements are not assumptions, they are based on their personal experiences in their

[312] Interview with female Army Lieutenant Colonel, Oct 30, 2012.
[313] Interview with USMC Colonel, Nov 1, 2012.
[314] Interview with female Marine Corps lieutenant colonel, Oct 30, 2012.

jobs. One public affairs officer stated, "One of the things it gives us is immediacy. And that is huge in the media world. Not only for dealing with your internal audiences but also with your external media and those people that we need to inform back in America. When we used to communicate primarily, we used to communicate in written products, in email, you either do a voice conversation, some sort of voice teleconference on some type of VTC system or you would use straight old email. When those restrictions had been lifted and the Army, in a sense, encouraged us to use social media more--you still do the same amount of staff work, but the responses seem to be a lot less encumbered and a lot more immediate. You can interact to influence a story in ways we never had before. We routinely answer questions now via Twitter and a lot of it in different military organizations."[315]

I asked the public affairs major to try to quantify how he thought social media affected his job and he replied, "I could not say it's a hundred percent increase or a 5000 percent increase but just in the last three years I have probably used social media in my normal army public affairs job, daily. Sometimes depending what the event is, hourly, several times during the day-that's something I did not do in 2008 or 2009."[316] When asked similar questions, the public affairs lieutenant colonel commented, "It gives us another dimension to reach people instantly. People don't have time to read email, but they do have time to scan a quick tweet that comes up on their computer and if they have a link, they can follow it easily, rather than opening up emails--it's like instant information straight to your brain."[317] My friend at the human intelligence school at Fort Huachuca (who actually is an advocate despite his previous comments about the students) added, "There are great things that it can do. It's a great way to spread the word. For so many

[315] Interview with Army Major, Public Affairs, Nov 14, 2012.
[316] Interview with Army Major, Public Affairs, Nov 14, 2012.
[317] Interview with Army Lieutenant Colonel, Public Affairs Officer, Oct 26, 2012.

people it's a part of their life now. It's a daily habit. For example, we now do Facebook presentations. The CG [Commanding General] will use it to do a question and answer session--to do sensing sessions. It's faster than the post newspaper which is only printed once a week. It's used as a way to spread the information faster."[318] As my interviews progressed over three years, service members because accustomed to the social media policy and were more in support of it than in the earlier interviews.

I searched for some real world examples of how social media has changed the military society or the way service members do their jobs. The public affairs lieutenant colonel told me, "I'd say that having Facebook on my smart phone makes a huge difference in whether I even use it, because I get updates on it and I'm always holding it. I'm always on it."[319] I found articles on using social media in a crisis situation, a technique that is becoming more popular. Edward Lundquist, a Navy contractor, wrote an article about supporting operations in Haiti. "The military can leverage social media to provide real-time situational awareness of conditions on the ground, based on information being shared by victims or first responders in an affected area. The January 2010 earthquake in Haiti demonstrated the power of the global crisis community to visualize information as it was flowing in real time via Twitter, SMS [standard message service], text messaging and imagery."[320]

In an operational example, An Army Lieutenant Colonel said that in Afghanistan, every attack on a coalition member is investigated and there have been some new additions to the forms they have to fill out due to social media. "So anytime there was an IED [improvised explosive device] or an ambush on a patrol you had to fill out a report and a portion of that report

[318] Interview with Army Lieutenant Colonel, Jan 19, 2013.
[319] Interview with Army Lieutenant Colonel, Public Affairs Officer, Oct 26, 2012.
[320] Edward Lundquist. "Crisis Tool: Social Media Can Provide Situational Awareness During Disasters…In 140 Characters or Less," *Sea Power*, February 2011, pp. 10-14.

was asking every member of that patrol, 'when was the cell phone call you made?'; 'what was the last thing you posted to Facebook?'; and 'when did you post it?' There has to be some genesis for that to be on the report--some intel [intelligence] at some level."[321] This form did not exist on an earlier deployment; its creation was entirely influenced by social media.

Another example was given to me by an Army major who recently returned from Afghanistan and said he saw social media gain more and more relevance every day. "One incident that happened was President Obama arrived in Kabul [May 2012] unannounced. We had media analysts who searched social media. One of the local Afghans saw the President moving from one site to another and tweeted it. Our media analyst picked it up. At first there were 3-4 Twitter feeds reporting it. Within 30-40 minutes it grew to a couple of hundred. That's how our chain of command was notified President Obama was in Kabul. This was the first instance where our commander saw the value in it. After that he wanted a weekly social media roll up. We saw a huge change of methodology and mentality after that."[322] This example is important because when the President travels to a military area of responsibility, the threat level goes up. While the major understood the President's travel plans should be kept as private as possible for security reasons, he believed if the local populace knew the President was there and the commanders on the ground did not, service members' lives could be in danger if they were not aware of the heightened threat level. The use of social media is still maturing within the DoD. Public Affairs officers, commanders, and others continue to explore innovative ways to capitalize on this new technology.

Sociotechnological inevitability can be characterized by comments that the use of social media has somehow overwhelmed military society. The whole premise of sociotechnological

[321] Interview with Lieutenant Colonel, US Army October 30, 2012.
[322] Interview with Army Major, Feb 25, 2013.

inevitability that there is no use avoiding social media. Social media is here to stay and the DoD needs to adopt social media to keep up with the civilian world. An author in the *Military Review* states, "But you should ask, 'Can I afford not to become involved in this mainstream method of sharing my message?'"[323] A corollary to that is that the military is already behind in use of social media and has to struggle to keep up. In regard to how the interest in social media started in DoD, a major general told me, "We saw a push to move towards these capabilities by the government."[324] He was of the opinion that DoD had to keep up with the civilian world and that they were way ahead of the military.

Many service members use metaphors to describe the arrival of social media. One Army colonel had a lot to say about how inundated our military society is now with social media. "Social media was a driving force, we've been overwhelmed. It wasn't about one side or the other of the military winning, social media won. Social media and the need to collaborate was huge and tremendous-almost like a tsunami. It overwhelmed them."[325] I asked him what the military's reaction should be to this situation and he said, "It was always a balancing act. I felt like a wave was coming that we couldn't overcome. The genie is out of the bottle. We'll never put it back in--we should exploit it for what it's worth."[326] The metaphor of the tsunami and the genie out of the bottle portray a force so strong, it cannot be stopped. A Marine Corps colonel also believes there is no way to stop the advance of social media so the military accepted it. "I think they realized they couldn't stop it. As long as you are professing your personal opinion in a public manner still and it's not put out as the Marine Corps position, you are OK. It's difficult because people have so many different devices and they are all over the battlefield. There's no

[323] Chondra Perry. "Social Media and the Army," *Military Review* 90 (Mar-Apr 2010).
[324] Interview with Major General, Apr 27, 2012.
[325] Interview with Army Colonel retired, Apr 5, 2013.
[326] Interview with Army Colonel retired, Apr 5, 2013.

way to stop it."[327] Neither of these colonels professed a desire to stop the advance of social media. They merely opined that the use of social media could not be stopped; its use is inevitable. Which technically is untrue, the DoD could and did ban social media from its networks at one time and has the ability to do so again. Some intelligence units ban the use of social media now and service members comply.[328] However, the DoD could not restrict personal use of social media.

The discussion of sociotechnological inevitability and the need to keep up with technology often involves sweeping generalizations about who is using it. A DoD civilian policy maker told me, "Today everybody has a smart phone."[329] And a Marine captain said, "Everyone I know, with the exception of my parents, is on Facebook."[330] An Army colonel concluded that all people are on social media and the DoD has to change in order to keep up. "I think there is a place for it in the military. We've got to learn to communicate within the existing way people interact--it serves some purpose along that line."[331] The Army major public affairs officer, speculates that all public affairs officers and all Army leaders support the use of social media. "Those people that are still holding onto the idea that we have to engage only in standard press conferences are few and far between. They have their time and place, but I have not run into a senior Army Public Affairs person and so far, I haven't found a general officer or an SES [Senior Executive Service], who totally discounts it. They want to engage in these areas. And I think the message we are getting across is this is important, this is the way communications is going. Twenty years from now we may be onto something else but right now social media is what we

[327] Interview with Marine Corps Colonel, Nov 1, 2012.
[328] Interview with Army Colonel, Jan 19, 2013.
[329] Interview with DoD Civilian, Dec 20, 2011.
[330] Interview with USMC Captain, Jan 3, 2013.
[331] Interview with Army Colonel, Feb 17, 2012.

are working with."[332] An Air Force Colonel I interviewed said he believes it is his duty to keep up with the young people who he says are *all* on social media. "If the younger generation is going to use it, I at least wanted to set it up and learn about it; then at least I have an educated opinion, because at least I tried it. Me, as an Air Force leader, need to be able to communicate with my Airmen, Lieutenants and Captains. I need to be able to communicate with them on their level."[333]

An additional thread within this discourse of keeping up, is the fear of being left behind. The ASD for Public Affairs at the Secretary of Defense level states that DoD, as an organization, is very behind our civilian counterparts and even its own workforce. "Social media, after all, is a tool for communication, development, collaboration and transparency. The best part of social media platforms is that the American workforce is already taking part in these new ways of communicating. We in the defense industry are catching up with our own workforce."[334] An Army brigade commander, stationed in Kuwait, had a different twist. "I tell people that if you aren't on it, you don't know what people are saying about you. So you can ignore it if you want to, but it's not going to keep you off the net. And besides that, it's how people communicate, so if you aren't doing it, you don't understand. I didn't understand it until I got on it."[335] An Air Force Colonel agreed with her point that those who are not on social media do not understand its potential. "Usually people who don't like it, haven't used it. I don't know how people can hate something they don't understand."[336]

[332] Interview with Army Major, Public Affairs, Nov 14, 2012. An SES is a government civilian at the highest rank.
[333] Interview with Air Force Colonel, Jan 10, 2013.
[334] Price Floyd. "In Defense of Social Media," *The Washington Times*, March 21, 2011.
[335] Interview with Army Colonel, Brigade Commander, Nov 11, 2012.
[336] Interview with Air Force Colonel, Jan 10, 2013.

I had interesting discussions with service members who were about to retire and retired about the utility of Linked In in their job searches. I asked a Navy Captain if he was going to use it in his transition to civilian life. He thought he was behind because he was not using it to broadcast his connections. He said, "Because of my pending retirement, yesterday I was on my work computer trying to get a linked in account set up. All these guys say you have to get Linked In. They're saying a lot of employers, especially if it's one of these defense contractors. They go to your Linked In profile to see who you are friends with, buddies with. I don't think I'm going to get a job as a business development guy because I don't know fifty admirals and fifty generals. I just don't have those contacts--but they say you have to list these guys, they have to be on your page so your potential employers know you know them."[337]

Not everybody believes the use of social media is inevitable. An Army colonel, also about to retire, did not see the utility of Linked In. She preferred the more traditional route of face-to-face networking. She commented, "It's not like I am going to use Linked In to get a job. If I were in the market for a job, I wouldn't be doing it through Linked In. I would be connecting to people in a networked way--but I would be calling them up in their offices and say, 'Hey, let's get together for coffee sometime. Let's get together for lunch' and networking that way. I feel very confident that when the time comes I will have a job--but it won't be because of Facebook or Linked In."[338]

Whether it is the desire to keep up or the desire to not be left behind, most of the service members I interviewed believed in the inevitability of the advance of social media. DoD as a whole is pursuing innovating solutions involving social media and has found positive results, especially in the public affairs arena.

[337] Interview with Navy Captain, Jan 3, 2013.
[338] Interview with ARNG Colonel, Nov 2, 2012.

The last topic in the sociotechnological inevitability discourse is the idea that service members participate in social networking for morale purposes. There were negative and positive responses to family and friends dynamic, but overall, it was accepted as the way people are communicating today by the people I interviewed. An Army lieutenant colonel in Hawaii explained, "People are getting their needs met with online friendships."[339] An Army lieutenant colonel and former professor at West Point said, "When we were teaching, we saw it kept cadets more connected with friends and family from home. It think it's the same thing with deployments or if you are assigned overseas and not in the same time zone as your family and friends. In the past, you might talk to them once a month, and now it's a daily conversation that you could be having not only with your friends and family, but those who are part of your past years ago."[340]

The Army public affairs major accepts the change that social media introduces. "I understand that a way to communicate with someone now is to have a relationship with somebody on Facebook and say 'Hey guess what I did today, I did x, y and z.' And that's great, we encourage sharing. It's the 21st century example of letter writing."[341] The Air Force lieutenant colonel that ran the Air Force network in Southwest Asia from 2007-2009, told me, "One general officer had a daughter in college and wanted to open the networks because 'it's the only way she communicates with me.'"[342] The lieutenant colonel was not a supporter of social media on the military networks at the time and commented to me about the general, "Oh so your poor parenting practices are a risk to the Air Force."[343]

[339] Interview with Army Lieutenant Colonel, Jan 17, 2013.
[340] Interview with Female Lieutenant Colonel, Oct 20, 2013.
[341] Interview with Army Major, Public Affairs, Nov 14, 2012.
[342] Interview with Air Force Lieutenant Colonel, Jan 28, 2013.
[343] Interview with Air Force Lieutenant Colonel, Jan 28, 2013.

I had two service members tell me they considered deleting their Facebook accounts, but did not because of their own morale. The first lieutenant deployed to Afghanistan said, "I contemplated deleting my Facebook account, but I didn't because I am in Afghanistan and it is my lifeline."[344] An Army major who works in the network security field also deliberated deleting his account. "I'm personally not a big user for a couple of different reasons, I contemplate deleting my account almost every day because of certain requirements of my job. But my family uses it and Twitter so I continue to monitor it."[345] These two officers had a conflict between their concept of security risk and their desire to use social media to connect with their family. Both chose their families and social media over their perceived security risk.

I also had three people say family and friends are not an excuse to be on social media. The DoD civilian policy maker was commenting on the dispute about social media and said, "They made it sound like putting it on the DoD networks was the only way for Service members to stay in contact with their families."[346] He went on to say that it's an easy way, but not the only way. He was a former Navy Lieutenant Commander and reminisced, "I was in the Navy in the '80's and '90's…we didn't need that much contact with our families."[347] The Marine Harrier pilot was completely against the whole idea of social media. "I don't want 100 friends, I don't need 100 friends, what I want is five or six true, deep trusted individuals and that's what I'm looking for. When you only have five or six friends, I can keep up with them on the phone. I can keep up with them over coffee."[348] He is not alone; an Army colonel had pretty much the same view. "I'm not against social media, it just something I don't have a strong desire to use it. The way I

[344] Interview with First Lieutenant, Afghanistan, Mar 4, 2013.
[345] Interview with Army Major, Feb 25, 2013.
[346] Interview with DoD Civilian, Dec 20, 2013
[347] Interview with DoD Civilian, Dec 20, 2013.
[348] Interview with USMC Lieutenant Colonel Harrier Pilot, Oct 27, 2011.

stay in contact with friends is phone calls or I see them. It's just not a tool that I feel compelled to use."[349] A Marine Corps lieutenant colonel agrees, "I can't even keep up with email. People I care about I talk to or I see and if I don't, so be it. I don't want to be that interconnected."[350] These three officers stated their family and friends were still important to them, but they chose alternate methods of communication other than social media to stay in contact.

The discourse on the sociotechnological inevitability of social media seems one-sided. The definition of sociotechnological inevitability assumes the success and future refinement of the technology. STS and social science scholars, DoD publications and service members all believe social media changed society and the way people communicate. The DoD leadership are proponents of technological superiority as evidenced by the fiscal year 2013 budget where the DoD received roughly half of the federal budget for research and development.[351] The DoD leadership clearly desires technological superiority to achieve the technological advantage over an enemy. The fear of not keeping up technologically with an adversary drives the DoD to experiment with and adopt new innovations. However, this view presupposes superior technology will lead to U.S. victory. This was not the case with the Taliban whom Secretary Gates said out-communicated the U.S. military from a cave.[352]

There have been some successes for social media within the DoD. Senior leaders such as General Dempsey and ASD for Public Affairs Floyd utilized social media effectively as a tool for public outreach. However, some senior leaders are concerned social media interferes with

[349] Interview with Army Colonel, Feb 17, 2012.
[350] Interview with female Marine Corps lieutenant colonel, Oct 30, 2012.
[351] John F. Sargent, Jr. "Federal Research and Development Funding," *Congressional Research Service*, Washington, DC, Dec. 5, 2013.
[352] Miles, Donna, "New Public Affairs Chief Sets Out to Transform Communications Processes," American Forces Press Service, Washington, DC, June 15, 2009.

face-to-face and written communications without considering that social media introduces a new way of conducting business.

The metaphors such as a tsunami or a genie that has escaped from a bottle pre-suppose that social media is a force that cannot be stopped and are very one-sided. Such is also the case with the fear of not keeping up or being left behind. Service members also expressed a conflict between security risk and keeping in touch with their loved ones, which is not a rational argument; it is not a choice between family and the use of social media. Others argue that while their family is important, using social media is not. The one sided-ness of the arguments of sociotechnological inevitability are telling. Sociotechnological inevitability is a flawed concept from the start because of the presupposition of success and because the term implies the driver is technology and not "the social" element. The belief in the inevitability of social media ends the debate before it starts, because service members have already reached a conclusion.

3.4 RESPONSIBLE ONLINE BEHAVOIR

What is the discourse around responsible online behavior? There is evident tension between the stated norms and actual behavior: how is this rationalized and what are the possible implications for policy? Responsible online behavior is often hotly debated in the discussion of social media and the military. The inability to control the use of social media by service members, families and DoD civilians is frustrating to military leaders. The shift from being able to reasonably control the DoD's external information to finding out something is already published without being vetted challenges the risk-averse culture of DoD. The concept that the institution of the DoD must technically control service members' actions contrasts with the trust leaders put in service members' actions every day when they arm with them weapons and send them into battle. Military leaders debate whether service members are "responsible" enough

with the limited guidance already published, and question if the policy should be rewritten to be more specific. For instance, the social media policy first published in February 2010 did not address a service member's personal responsibility while using social media. Is it necessary to specifically state that service members will be punished if they violate operational security or is that adequately covered by referencing the Joint Ethics Regulation, which has no specific mention of social media?

The military has the technical ability to control its members' actions on the networks by controlling access, and there is a precedent for reversing a policy of open access. In 2009, a DoD network in Afghanistan was penetrated by a foreign intelligence agency and the infection was spread through the use of flash drives. The DoD's response was to immediately ban the use of flash drives on all DoD networks.[353] This ban is still in effect today and the military continues to physically enforce that policy at the network enterprise level. The same is true of access to social media. The DoD could easily restrict access to any social media sites on government networks, but that action would still not solve the issue of service members' use of social media on their home or commercial networks. The DoD could publish a policy banning service members from creating and using social media accounts and service members would have to comply or face punishment. There are examples that show precedent within DoD to control service members' personal actions such as banning service members' public criticism of the President, their ability to join a gang, get a tattoo on their neck, or even to grow a beard. It is therefore possible for DoD to enforce a ban on social networking, but is it necessary? Can DoD trust its service members to be responsible?

[353] William J. Lynn. "Defending a New Domain," *Foreign Affairs*, Council on Foreign Relations, September/October 2010.

3.4.1 Social Science Frameworks for Analyzing the Concept of Responsible Behavior

In exploring motivations for responsible behavior, I found some social science works that tried to address what inspires people to behave responsibly. Dr. Stephen Kaplan, a psychology professor at the University of Michigan, offers us the "Responsible Person Model,"[354] which looks at alternative ways to motivate people to be responsible other than altruism and force. He speculates that if people are made to feel informed, competent, and able to learn they are more likely to be responsible. In the case of social media and the military, the current open policy on using social media seems to be an example of this. In a paper on human behavior, Hungerford, Volk and Ramsey dispute Kaplan's theory by stating that simply teaching people about something does not influence behavior, citing unwanted teen pregnancy and venereal disease as examples. They believe the individual must own the issues and be empowered to do something about them.[355] Hungerford, Volk and Ramsey would say that the fear of punishment under the Uniform Code of Military Justice (UCMJ), (aka military law) motivates service members to act responsibly online. They quote Kelly and Thibaut's theory on social influence and interpersonal communication which provides motivators for compliance with policy. Hungerford, et. al. believe people will comply because of perceived authority, reciprocity and mutuality.[356] First, people will comply with authority they deem to be legitimate. In the military, an order, whether it be verbal or written policy, is seen by service members as legitimate. With reciprocity, people will comply if they are placed in some sort of debt. In DoD, service members comply with policy because they swore an oath when they joined, that they will follow orders. Lastly, people

[354] Stephen Kaplan. "Human Nature and Environmentally Responsible Behavior," *Journal of Social Issues*, Vol 56, No. 3, 2000, pp. 497-8.
[355] Harold Hungerford, Trudi L. Volk, and John Ramsey. "Instructional Impact of Environmental Education on Citizenship Behavior and Academic Achievement," Paper presented at the *North American Association for Environmental Education Conference*, South Padre Island, TX, Oct. 21, 2000.
[356] Ibid.

will comply if there is a mutuality, where they is an equal relationship between the influencer and the influenced. Jointing military service requires a contract. The military agrees to provide training and a job and the service member pledges to obey orders. It is a mutual relationship where both parties benefit.

Hungerford, et. al. also quote Fishbein and Ajzen's theory of planned behavior which states 'behavioral intention' is the key determinant of behavior.[357] This is influenced by three elements: a person's attitude toward performing the behavior; the perceived social pressure to adopt the behavior; and perceived behavioral control, which consists of control of beliefs and perceived power. This theory fit in with my study of social media and the military because service members accept conforming to military policy. Those who choose not to accept it, are eliminated from the Service. There is definitely peer pressure in the military to follow the rules. There is also perceived behavioral control in the military. Service members respond to control by regulations and policies because there is the potential consequence under UCMJ if one of these is not followed. While there is not an equal relationship among service members of different ranks, all service members regardless of rank pledge to follow the same orders, regulations and policies. The orders, regulations and policies prescribe acceptable behavior and all service members follow it or face the consequences of not following it.

From a social media perspective, social science scholars recognize a change from controlled ability to publish information to a completely unrestricted environment based on the technology. Shirky notes a new paradigm, "Filter-then-publish, whatever its advantages, rested on a scarcity of media that is a thing of the past. The expansion of social media means that the only working system is publish-then-filter,"[358] which is a significant changed based on a characteristic of the

[357] Harold Hungerford, Trudi L. Volk, and John Ramsey.
[358] Shirky, p. 98.

technology--the sudden available publication platform of social media. Shirky concludes, "Mass amateurization has created a filtering problem vastly larger than we had with traditional media, so much larger in fact that many of the old solutions are simply broken. The brute economic logic of allowing anyone to create anything and make it available to anyone creates such a staggering volume of new material that no group of professionals will be adequate to filter the material."[359] There is much speculation from social science scholars on what makes a person decide to act responsibly. Whether it's the need for self-esteem, the need to feel respected, or the fear of consequences, the opinions on why people behave responsibly are diverse. The change in the availability of publishing platforms means, people have to react to this sudden freedom. Because of the volume of available platforms for social media, there is no way to administer control or filter content. Similar to the privacy risk discourse, people have to decide on their own to act responsibly and accept any consequences that may result from their behavior.

3.4.2 Department of Defense Views on Responsible Behavior

The DoD has its own discourse on responsible behavior, ethics and accountability for one's actions whether it is online or not. This discourse starts with the Code of Conduct. The Code of Conduct was developed during the Korean War as a directive from President Eisenhower to guide the behavior of all military members during combat or captivity because in World War II, service members were confused about appropriate actions. It was last modified by President Ronald Reagan in 1988. Article six of the code states, "I will never forget that I am an American, fighting for freedom, *responsible for my actions*, and dedicated to the principles

[359] Shirky, p. 98.

which made my country free." [360] The DoD makes it quite clear in the Code of Conduct that all service members are expected to be responsible for their own actions.

Ethics are taught at every level military school from basic level training on up to general officer training. The DoD has its own Standards of Conduct office run by the General Counsel (lawyers) which publishes ethical guidance, training packages, and encourages employees to seek counsel before proceeding in a manner they deem to be questionable. This office published a DoD Directive on Standards of Conduct which states, "DoD personnel shall perform their official duties lawfully and comply with the highest ethical standards."[361]

To supplement this Directive, the OSD General Counsel produced the *Joint Ethics Regulation* which is the single source of standard ethical guidance for DoD employees. The regulation clarifies that DoD employees include all members of the armed services (to include the Reserves and National Guard) and DoD civilians. The *Joint Ethics Regulation* covers everything an employee needs to know about financial and employment disclosure, post-employment rules, enforcement and training. It states that "DoD employees shall become familiar with the scope of and authority for the official activities for which they are responsible…Sound judgment must be exercised. All DoD employees must be prepared to account fully for the manner in which that judgment has been exercised."[362] It further states that, "Each DoD employee will set a personnel example for fellow DoD employees in performing official duties within the highest ethical standards."[363]

---

[360] Deland, Troy. "The Military Code of Conduct: A Brief History," *Pacific Air Forces*, Kunsan Air Base, Republic of Korea, Feb 9, 2011. Accessed Nov 11, 2013 at http://www.pacaf.af.mil/news/story.asp?id=123241828.
[361] Department of Defense. *Standards of Conduct*, DoD Directive 5500.07, Washington, DC: Office of the Secretary of Defense General Counsel, Nov 29, 2007.
[362] Department of Defense. *Joint Ethics Regulation*, Washington, DC: Office of the Secretary of Defense General Counsel, Aug, 1993, p. 7.
[363] Ibid, p. 14.

The expectation of the Department of Defense as directed by the President, as Commander in Chief (via Presidential Executive Orders) and the Secretary of Defense (via DoD Directives) is that service member are responsible for their own personal actions, display ethical behavior at all times, and understand that they will be held accountable for the actions they take. The code of conduct, service members' ethics training, and the *Joint Ethics Regulation* are constantly referenced in the discourse of service members' use of social media. The *Joint Ethics Regulation* is referenced in both the initial and final social media policies in the section containing the expectation of service member behavior.

3.4.3 Service Member Views on Responsible Online Behavior

There are many interpretations of what constitutes responsible online behavior and who should enforce it. There is an individual's own personal responsibility and self-regulation for acceptable conduct but there is also an expectation of the institution that it will require and/or train service members to act responsibly and bestow consequences on those who do not. Service members view responsible behavior as a duty of their profession. Staff Sergeant Dale Sweetnam from the Army social media office, believes the guidance is simple, "It is important that all soldiers know that once they log on to a social media platform, they still represent the military. The best way to think about it is, if you wouldn't say it in formation or to your leader's face, don't say it online."[364] This intersects with the privacy risk discourse where service members can violate their own privacy by not realizing how public social media can be. However, social media is an option that service members have a choice of using or not using. According to my interviewees, it is becoming more common for the military to provide training and guidance on responsible social media use before deployments.

[364] Cheryl Rodewig. "Social Media Misuse Punishable Under UCMJ," *U.S. Army*, Ft Benning, GA, Feb 9, 2012.

Service members understand their duty to be responsible online as members of the military. Captain Steve Symanski, a military lawyer at Fort Benning, GA, said in a media interview, "Just because you delete it, doesn't mean that 1000 people haven't seen it. We are expected to be soldiers 24x7, whether it is in formation, in the bars and restaurants off post or on Facebook and Twitter."[365] His coworker, Private Alejandro Francis, echoes that sentiment with his own example, "I mean, I put up pictures that are appropriate. And I know if I have to think about it twice to put it up, then I won't put it up."[366] While self-regulation is common, there are still incidents as mentioned above with the Marines where service members act irresponsibly. A young Marine Corps Captain who deployed to Afghanistan twice likened it to his weapon and stated people choose how to act. "I think it's just another tool to be responsible or irresponsible with, the same way someone is responsible or irresponsible with a weapon. It doesn't matter what rank you are, if you are in a combat zone, you have a loaded weapon. You're taught how to use it. There's irresponsible people with dangerous things like that. Facebook is just another thing."[367] The captain's use of the tool metaphor for social media is his way of articulating the need to train people to act properly.

One recurring issue has been particularly troubling and that is service members in theater posting thoughts on Facebook about combat deaths before the next of kin has been properly notified by the military. Colonel Deborah Skillman, chief of the Casualty Mortuary Affairs Branch at Army Human Resources Command, said in an *Army Times* interview, "There have been a few occasions where close friends of the soldier have not abided by the restrictions and have contacted family members of casualties either telephonically or through social media…All

[365] Rodewig. "Social Media Misuse."
[366] Audie Cornish (Host). "All Things Considered," *National Public Radio* Interview, May 21, 2012.
[367] Interview with USMC Captain, January 3, 2013.

of these soldiers believe in their hearts that they are doing the right thing. Unfortunately, they are not."[368] This kind of incident is of concern for DoD leadership. The DoD Instruction on *Personnel Casualty Matters Policies and Procedures* requires the next of kin of a fallen service member be notified in person by a two-person uniformed detail. The casualty may not be reported to the media until twenty-four hours after the next of kin is notified.[369] There have been several incidents in Iraq and Afghanistan where a family found out via social media that a service member was killed.

An Army captain, stationed in Afghanistan in 2012, told me, "No matter what you tell the soldier, you can't control what they put online. You know, you inform them [soldiers] and hope they make the right decision to post things online such as if there is a KIA [killed in action] or something--where the spouse or the family member hears about it prior to the military actually making contact with that family member to let them know their family member or significant other passed away. You know…that type of thing. It affects that process the Army has in place to inform next of kin and family members. That's the most impact that I've seen so far with the social media."[370] An Army first lieutenant in Afghanistan also experienced this. "A soldier from another based died and his friend put on Facebook, 'My best friend died.' That's how his Mom found out--can you imagine that? His poor family. The blackout didn't really do anything--the military didn't have control over the commercial network and couldn't block it."[371] Even though the service member did not release the name of the deceased, the family knew who their son's best friend was and extrapolated that it was their son that was killed.

---

[368] Gould, Joe. "Social Media Complicate Army's Death Notifications," *Army Times*, May 6, 2012.
[369] Department of Defense Instruction. *DoD Personnel Casualty Matters, Policies, and Procedures*, Number 1300.18, Undersecretary of Defense (Personnel and Readiness), August 14, 2009.
[370] Interview with deployed Army Captain, Nov 20, 2012.
[371] Interview with Army First Lieutenant in Afghanistan, Mar 4, 2013.

The Marine Corps is also concerned about social media interfering with proper death notification. A Marine Corps colonel told me, "It [social media] was banned for a while and then they allowed people to do it. The fear is its external communication, if somebody dies or is a casualty. The Marine Corps is very specific that the notification is done face to face. That is one of our biggest concerns."[372] When I was a network director in Southwest Asia in 2008-2009, my operations center used to 'black out a base' when a service member was killed so that no internet traffic from that base could go back to the United States until the next of kin were notified of the death. It was a technical solution to a very serious problem. The Army captain in Afghanistan in 2012 told me that policy has changed, "No we can't shut down the base. We can't do that anymore. It's just a verbal order."[373] At the time, the captain could not tell me why the policy changed from when I was there to four years later when she was there. I found out in later interviews, the policy change was due to the proliferation of affordable, commercial cellular service in Afghanistan. The DoD could not block commercial networks and instead addressed it with an order.

The examples I used above were incidents where a participant in a questionable act posted irresponsible content on social media on the internet and had to face the consequences. In a Navy example, a mere observer of the act can be irresponsible and post content that was never intended for the internet. Captain Owen Honors was the Executive Officer on the aircraft carrier Enterprise. He made some videos with inappropriate content concerning subordinate female officers in compromising positions and homosexual jokes intended for viewing on the ship's internal network as a morale booster on a deployment. A shipmate shared the content with someone outside the deployments, and it eventually ended up on social media. Due to the

[372] Interview with Marine Corps Colonel, Nov 1, 2012.
[373] Interview with Army Captain in Afghanistan, Nov 20, 2012.

content of the material that was posted, the Navy relieved Captain Honors of his duties and ended his career. Even though he did not post the content, Captain Honors was responsible for generating it, did not control the source or audience of it, and he was fired for it.[374] Clearly, the DoD is serious about service members being responsible for their own actions.

From Talja, we learn that broad conclusions can be drawn from interview data to show how people construct certain situations. Four of these broad constructions emerged strongly in the discourse from my interviewees surrounding responsible online behavior. The first is that social media is a waste of time and anyone using it in the workplace is not doing their job. Second, military members are somehow expected to behave more responsibly than their civilian counterparts. Third, in the absence of policy, people will make up their own rules. And lastly, if the use of social media is denied, service members will bypass network security in order to use it. The following examples illustrate these points.

In finding common themes, Talja suggests looking for specific events or points in time that multiple people refer to. Three different policy makers all referred to March Madness, a Division I college basketball tournament, as the point in time when DoD starting considering blocking content in order to conserve bandwidth. Apparently, people were watching streaming video during the workday and the extra traffic on the network during this event caused the internet to run slower for everyone else. A DoD civilian stated, "It all started with U-Tube and March Madness--it was a bandwidth issue."[375] The three star general in charge of operating and securing the networks mentioned it as well, "We could monitor network statistics and we found that 75% of the NIPR [unclassified network] bandwidth was going to things like March Madness, financial sites and dating services. It was costing the government a lot of money for a

[374] Corinne Reilly. "Captain Who Made Racy Videos to Retire From the Navy," *Virginia Pilot*, January 28, 2012.
[375] Interview with DoD Civilian, Dec 20, 2013.

lot of non-government work."[376] A retired colonel widened the aperture to include more than just basketball. "The IAP's [internet access points] were saturated because of it--March Madness, any kind of sports playoff."[377]

In keeping with the three star general's comments, another theme is that employees who are performing unofficial business are wasting the government's time and money and there is empirical evidence to support this. The same general claims, "There are studies out there-you should google them-that show that six hours a day are wasted by the average employee."[378] An Army Lieutenant Colonel agrees, "90% of the usage had nothing to do with the intent of the memo. Most of that 90% of use were people wasting time at work. There are studies to back that up. The majority of the statistics show that a very small percentage of people are using it for legitimate work purposes."[379] He also said it was personally troublesome to him that people are wasting time and work and the government is paying for the bandwidth. "DoD continues to have an increase in pipes and most of it is for non-official use. That aspect bothered me."[380] A Navy pilot said his conscience prevented him from using his computer for non-official business. "I still have that residual guilt from way back like, 'don't use your work computer for personal stuff.'"[381] A retired colonel gave me a vignette from his active duty days. "I was at a media event with the Deputy Commander of DISA. A young reporter asked her, 'Don't you think soldiers have the right to surf the internet?' It's funny they look at it like that. It's grounds for dismissal in the civilian world for fooling around at work on the internet all day."[382]

[376] Interview with three star general, Feb 13, 2013.
[377] Interview with Army Colonel retired, Apr 5, 2013.
[378] Interview with three star general, Feb 13, 2013.
[379] Interview with Army Lieutenant Colonel, Jan 17, 2013.
[380] Interview with Army Lieutenant Colonel, Jan 17, 2013.
[381] Interview with Navy Captain, Jan 3, 2013.
[382] Interview with Army Colonel retired, Apr 5, 2013.

A female Army colonel points out that there is no cogent evidence supporting the argument that people are just wasting time at work using social media. She offers that it can be useful to have access to so much information. "There are lots of complaints about people wasting time using social media at work, but there does not seem to any measurement of how much quicker assignments can be completed, how much better the quality research and analysis is, how much more creative and adaptive workers can be because of access to so much information, how much better leaders are able to help care for soldiers and family members because there is so much access to interact with them, share information, etc."[383] Despite the lack of empirical evidence, the feeling that social media at work equated to people wasting time and money was dominant in the interviews I conducted. While not everyone felt that way, it was a common construction of more senior leaders.

One noticeable construction of responsible online behavior is that members of the military are somehow more responsible than their civilian counterparts. There is also no empirical evidence to back up that claim, however it is often cited within this discourse by service members. There are two angles to that construction, one is that a sense of responsibility is innate to service members and the other is that there is a personal responsibility expected of military members by their peers.

A Marine captain assured me, "There is some ember in every one of them that wanted responsibility--that they wanted to do something for their country."[384] A Marine colonel believes this expectation is good to a fault, "I think that's one of the problems with the military. When you are a civilian, you don't get judged nearly as closely as any military."[385] A retired soldier,

[383] Interview with Female Army Colonel, May 15, 2013.
[384] Interview with USMC Captain, Jan 3, 2013.
[385] Interview with USMC Colonel, Nov 1, 2012.

now working as a DoD support contractor said, "There are fundamental good things about a soldier that should never change."[386]

Some attribute the goodness to the training service members go through, though they believe a certain type of person joins the military--one seeking responsibility. "I think they [military people] are more responsible in general because of their training. It's also an all-volunteer force and most people who join the military are looking for some sense of responsibility and training in their lives--they want to be something."[387] The Marine captain gives young Marines the benefit of the doubt. "I think often times we sell our Marines short. I think they are responsible individuals for the most part. They listen to instructions, they follow directions. They want to be good service members. I think that what happens is sometimes there might be a misunderstanding or lack of command emphasis on what is appropriate and what is not appropriate."[388]

An Army captain also believes soldiers are responsible, and gives examples of how soldiers follow the rules by not posting careless content. "It's all about military bearing, they know what they are supposed to and not supposed to post and they just obey the rules. There are rules of Army OPSEC. If you go downrange, you don't post pictures and say, 'I'm here, we only have one gate open, this is our only entry and exit point, we'll take this route' or 'oh I got another convoy at five o'clock like we do every day.' You don't post stuff like that that could give away your TTP's [tactics, techniques and procedures]."[389] Clearly, service members are also serious about being responsible for their own actions.

[386] Interview with DoD Support Contractor, Apr 15, 2013.
[387] Interview with USMC Captain, Jan 3, 2011.
[388] Interview with Army Major, Public Affairs, Nov 14, 2012.
[389] Interview with Army Captain, Dec 6, 2012.

The Army has seven core values: loyalty, duty, responsibility, respect, selfless service, honor, integrity, and personal courage. An Army lieutenant colonel refers to these ideals as a reason soldiers behave responsibly. "I think they behave because they care about each other. I think also they want to represent the Army values."[390] Service members expect other service members to adhere to the code of conduct and the values of their respective organizations. This expectation is instilled at a young age. I talked to two Reserve Officer Training Corps (ROTC) cadets who were very aware of the military's expectation of their conduct. One said, "They are representing who we are in their off time. So whatever we do, even if we aren't in uniform, people still know we are in the military. We still represent the military everywhere we go."[391] The other ROTC cadet drew a distinguishing line between his military friends and his civilian friends for social media use. "My military friends are not as active on Facebook. They don't put a lot of personal stuff on there."[392] The first ROTC cadet said much the same thing, "I don't see as many of my military friends posting things like they tell everyone about what's going on."[393] An Army lieutenant colonel brought the conversation around to her own personal responsibility as a military member. "I see myself as a public picture. If I wouldn't do it in public in my uniform, I wouldn't have it on Facebook. We need to act like the soldiers we are."[394] This discourse shows service members believe that because they are in government service, they should act appropriately and responsibly—even while off duty.

Another minor theme that arose in responsible online behavior is that in the absence of policy, people make their own rules. Most of the service members I interviewed took responsibility for

[390] Interview with Army Lieutenant Colonel, Public Affairs Officer, Oct 26, 2012.
[391] Interview with ROTC Cadet #2, Oct 20, 2012.
[392] Interview with ROTC Cadet #2, Oct 20, 2012.
[393] Interview with ROTC Cadet#1, Oct 20, 2012.
[394] Interview with Army Lieutenant Colonel, Public Affairs Officer, Oct 26, 2012.

their actions on the internet and believe it is their duty to behave responsibly. A University of Dayton study on Generation Y and the use of social media found that, "Most people don't exaggerate deviant behavior, most behave…However, the most significant form of regulation is the self-policing of the users themselves."[395] A first lieutenant in Afghanistan confirmed her unit made up their own rules when they discovered people exhibiting risky behavior online. "People were taking inappropriate pictures and posting them on Facebook--like of the flight line. We had to make up our own rules. We made signs and posted them saying not to take pictures."[396] This self-regulation ties back to the section of the code of conduct and the expectations the DoD has for service members' responsible behavior. The institution instills a sense of duty and responsibility into its recruits.

Some of the young people were adamant about their own personal good behavior. A ROTC cadet offered, "If you want to know what I'm doing, I'll tell you straight up. I feel like I monitor myself. I just want to be a better person--to be the best that I can be. I ask myself, 'Is that reaction appropriate?', 'Can I answer that way?', and 'Is that the right thing to do?' I monitor myself to do the right thing."[397] The other ROTC cadet mused, "I just don't get why people put pictures of themselves doing illegal things on Facebook."[398] The first lieutenant in Afghanistan said, "You have to question yourself before you hit send."[399] And an Army captain topped it off with, "I'm kind of a rule follower."[400] An Army colonel trusts young service members to be responsible. "My approach on it was to let them know there are things that are clear violations,

[395] E.J. Westlake. "Friend Me If You Facebook; Generation Y and Performative Surveillance," *The Drama Review*, Volume 52, No. 4(T 200) Winter 2008, pp 21-40.
[396] Interview with First Lieutenant, Afghanistan, Mar 4, 2013.
[397] Interview with ROTC Cadet #1, Oct 20, 2013.
[398] Interview with ROTC Cadet #2, Oct 20, 2012.
[399] Interview with Army First Lieutenant in Afghanistan, Mar 4, 2013.
[400] Interview with Army Captain, Dec 6, 2012.

they should use their own good judgment to not put information on these sites. You are all grown men and women--use your judgment on these sites."[401]

Service members also spoke of this responsibility from the perspective of other peoples' actions. One of the ROTC cadets said, "It's making good decisions in whatever ways you are doing that, like throughout any aspect of life. I would say with Facebook, it's the same thing. Don't put stupid things on there or disrespectful things toward other people. You should show respect for whoever can view your profile."[402] The first lieutenant in Afghanistan offered this example, "I mean, have some professionalism--we need to be professional. I've seen a West Pointer post, 'I can't wait to get out of the military' and list all the military's flaws."[403] An Army colonel declared, "It has caused people who otherwise would not have considered sharing something to when they are using Facebook or similar social media sites to learn to put a filter in place. Would I want to share this? Should I share this? Is this something appropriate to share?"[404] The Army captain believes soldiers simply need to regulate themselves, "That's a heck of a load on a supervisor who doesn't need to be worried about that. Mainly it needs to be self-restricted. Soldiers need not post what they shouldn't post."[405] A female lieutenant offered a different twist on self-regulation--the fear of consequences. "I do think that some of the self-correction occurs because of the publicity around when someone makes a mistake. There have been times when that has been all over the news-like when the Marines were peeing on dead bodies. Obviously that's extreme, but I think at large everyone sees when putting something like that out there is bad, and they see what happens and then they think, 'Maybe I shouldn't do

[401] Interview with Army Colonel, Feb 17, 2012.
[402] Interview with ROTC Cadet #1, Oct 20, 2012.
[403] Interview with Army First Lieutenant in Afghanistan, Mar 4, 2013.
[404] Interview with Army Colonel, Feb 6, 2012.
[405] Interview with Army Captain, Dec 6, 2012.

that.'"[406] An Army major involved in public affairs was very positive about soldiers self-regulating themselves during his deployment. He traveled extensively around Afghanistan and monitored the press and social media very closely as part of his job. He said, "I was in Afghanistan for a year with soldiers doing this and I can come up with maybe three or four things that probably shouldn't have been out there in an entire year."[407]

These personal examples show the DoD expects its service members to act responsibly and service members, in turn, believe it is part of their duty to act responsibly. However, the stated norms do not always match up with the actual behavior. Prior to February 2010 when the networks were blocked, service members would knowingly bypass network security protocols in order to access social media. Bypassing the network controls crosses over into the security risk discourse. It is not responsible behavior to bypass security to access blocked content. There were two ways identified to get around network security. The first is to find some loophole in the network security system that allows you to access social media. The second is to use a private network to post content. While this method doesn't affect military network security, it affects operational security which was of major concern to service members.

A common approach in Afghanistan (in 2008-2009) to get around the network content filter was to use https:// instead of http://. The content filter the Army was using in Afghanistan at the time, could not interpret content under secure connections, so secure socket layer (SSL) transactions could not be blocked. There are also more technical ways to avoid the content filter, such as using a proxy server or a virtual private network. Technically savvy soldiers could do a quick internet search to find many methods to bypass network security.

[406] Interview with Female Lieutenant Colonel, Oct 30, 2012.
[407] Interview with Army Major, Public Affairs, Nov 14, 2012.

An Army captain I interviewed by telephone in Afghanistan confirmed the earlier workaround, and she was able to compare pre-policy to post-policy. "The first deployment we found a way around it because it was not authorized--now they openly allow it."[408] Another Army captain, located in Hawaii, told me that in his experience, "Even if you regulate it, there's always going to be a way to bypass it--and soldiers will find that way so they aren't restricted."[409] A Marine gunnery sergeant offered a different method to bypass the restriction. "When I was on a ship, the Marines were not allowed to use social media and the Navy was. People will find a way around the rules. I just jumped on a Navy guy's computer and logged into my account."[410] An Army lieutenant colonel, also stationed in Hawaii spoke of an incident where soldiers had to bypass a content restriction to do their jobs. "After the tsunami, we had bandwidth issues in the Pacific. We blocked everything but the .gov and .mil sites. At the lower level where they are executing, they need access to more than just .gov and .mil sites. We had to tell the J3 [operations officer], "Hey you are hurting yourself. The J4 [logistics office] legitimately shops on Amazon or other shopping places. In that case, soldiers took their laptops to Starbucks where Starbucks became their place of duty. Joe finds a way to get it done."[411]

This leads to the other thread in the bypassing security discussion, using an alternate network to post content. There was much discussion on how if social media is blocked on the .mil network, service members will still use social media on their home networks. This links to the sociotechnological inevitability discourse. Most talked of the futility of blocking on the military networks because it would not solve the operational security problem as shown in the death notification vignettes. One of the policy makers told me, "It all has to do with people's personal

[408] Interview with Captain in Afghanistan, Nov 20, 2012.
[409] Interview with Army Captain, Dec 6, 2012.
[410] Interview with USMC GySgt, Apr 6, 2012.
[411] Interview with Army Lieutenant Colonel, Jan 17, 2013.

behavior. It's an ethics issue. They would do it anyway when they got home to their personal networks."[412] There are also those who believe the transition to mobile solutions is a factor. "People are going around it—they don't need their work email to do it. As long as they have a cell phone and a 3G connection, they can post. Not allowing it on the military networks isn't solving it. They are all doing it anyway. They all have I-phones."[413]

In another example, a Marine captain was out on a remote outpost in Afghanistan where he was the senior officer. As such, he had control of the network content and what to block. He believes that in all deployments, information will make it back to the home front regardless of the method. He said he discussed the subject with his platoon sergeant and decided to allow social media. "We thought about it [unplugging social media], I talked about it with my platoon sergeant, we definitely talked about the pros and cons of doing it. The pros were they could stay connected with home, the families could continually know they are OK. The downside is I knew that information was passing over the internet that shouldn't be passing over the internet. However we were also allowed to use phones, you can't take phones away so if the information is going to make it back, it's going to make its way back somehow some way. If they wanted to convey information, taking Facebook away doesn't necessarily stop that."[414] This discourse accepts social media's role in society as a communication method and stops any real debate on the topic. It is a foregone conclusion that social media use will prevail.

The discourse around responsible online behavior shows that social science scholars speculate on why humans act responsibly with multiple possibilities. DoD tries to instill a sense of responsibility in its service members with regulations and training. The Code of Conduct

[412] Interview with DoD Civilian, Dec 20, 2011. He was referring to any soldier in slang, as in 'GI Joe.'
[413] Interview with Mr. Price Floyd, May 29, 2013.
[414] Interview with USMC Captain, Jan 3, 2013.

directly states that service members are responsible for their own actions. There are still examples of irresponsibility, such as posting a death on social media before the next of kin is notified or the Captain Honors incident, which portray that people make choices with their actions. There is also concern that people are wasting time at work using social media or bypassing network security in order to use it. That contrasts with a belief that service members are more responsible than civilians on social media and in the absence of policy, service members decide to act responsibly for the most part and self-restrict their content. One could conclude that the sense of trust and personal responsibility the DoD leadership sees in service members led to the decision to open the networks to social media. A good example of that is changing the policy in Afghanistan from blacking out a base if someone is killed, to giving an order that nobody will post anything about the incident until the next of kin is notified. However, there are plenty of other incidents to break that trust and it could be argued that the sociotechnological inevitability argument is the reason the networks were opened. I believe both were factors in the decision, but not the only two factors. Youth and their technophilia are often construed as the sole reason for opening the networks to social media.

3.5 YOUTH

What is the discourse around youth (and their supposed technophilia? How is that affecting views of policy? For this paper, I consider any person under thirty as youth. According to the annual DoD demographic profile, sixty six percent of the active duty military force is under thirty years old.[415] With such a large portion of the force being so young, there is a discourse surrounding the youth and their love of technology that weaves through the three previous discourses. Comments on youth most often credit young service members with making

[415] Defense Manpower Data Center. *2011 Demographic Profile of the Military Community*, Washington, DC: Department of Defense, September 2012.

inevitable the change to adopt social media in the DoD. Many sources are cited saying younger workers will be more productive if given access to web 2.0 tools at work.[416] Another justification often heard is that young people will not choose to work for the government if those tools are not available to them."[417] Opponents to the use of social media say young people are careless and irresponsible when using social media.[418] Leaders have expressed opinions in the media and in response to my interview questions that they are afraid that young soldiers or family members may post information that risks the security of the military organization.[419] But plenty of other leaders say they trust young service members to act responsibly.

The assumptions that frame this discourse—in particular, the assumption that young soldiers have radically different values and behaviors from their elders—are often unsubstantiated and in some cases have been shown to be inaccurate. This is similar to a recent DoD debate on allowing homosexuals to serve in the military openly. There was much discourse on how young people were the ones who positively affected the policy change. But when questioned about the 2010 study on the repeal of the 'Don't Ask, Don't Tell' policy, the report author, Army General Carter Ham stated, "I really expected to see a very stark, generational difference. There's some of that, but it's not black and white like I thought. My sense is, all the old farts like me are going to be very much opposed to change and the youngsters would say, 'Get over it,' and 'it's not a big deal.' It's not so much a generational issue."[420] I suspect it is the same with the decision to allow social media on the DoD networks. The youth discourse could have resulted in a policy change that unfairly targets the young as irresponsible. It has been suggested that more senior

[416] Bonvanie, Rene. "Social Media In the Office: Two Truths and a Lie," *Forbes*, June 10, 2010.
[417] Interview with Brigadier General, U.S. Army, April 12, 2012.
[418] Interview with Lieutenant Colonel, US Marine Corps, October 27, 2011.
[419] Interview with Colonel, U.S. Army, November 8, 2011.
[420] Ed O'Keefe. "Transcript: Interview with 'Don't Ask, Don't Tell' Report Co-authors." *Washington Post*, Washington, DC: December 20, 2011.

level service members should be tasked to monitor younger members' social media interactions. The military already monitors "official" social media and military websites for "responsible" content, but has not mandated supervision of service members' personal sites.

3.5.1 Social Science Framework for Analyzing the Concept of Youth

Four Harvard scholars recently compiled a comprehensive report from empirical data on youth and digital media. They discovered that elders were concerned with possible risky behaviors on line by youth in the areas of contact risks, cyberbullying and privacy problems. The adults in the study were concerned about how youths make decisions online, especially that "they do not evaluate quality according to the adult-normative criteria emphasizing credibility, accuracy and authority."[421] The scholars advocate a mandate for a public policy discussion, based on empirical research, concerning youth, digital media and information quality. The study found the most cited reasons for adult concern were (1) youth do not evaluate credibility, accuracy and authority; (2) youth too easily disassociate the message and the source; and (3) youth do not distinguish commercial context.[422] Adults had fears that compounding vulnerabilities from a combination of the above factors would happen and youth would put themselves at personal risk because they would not be responsible online.[423]

In the end, the Harvard scholars concluded "The fears about possible harms are just fears. There is little evidence of any discrete and distinctly identifiable cases of harms resulting from bad information online or from incorrect application or interpretation of information online."[424] There is not a large difference in how adults and youth evaluate information. Youth are not any

[421] Urs Gasser; Sandra Cortesi; Momin Malik; and Ashley Lee. "Youth and Digital Media: From Credibility to Information Quality," *Harvard University*, Berkman Center for Internet and Society, Pub No. 2012-1, Cambridge, MA: Feb 16, 2012, p10.
[422] Ibid, 71.
[423] Ibid, 75.
[424] Ibid, 119.

more vulnerable online and can be just as responsible, and in some cases more responsible, than adults.[425] The "immersion of youth in digital media may lead to youth adapting and being more, not less, able than adults to make effective evaluations in the web context."[426]

The concept of adults needing to supervise youth who can possibly behave irresponsibly is a common theme in social science scholarship concerning digital media. Jack Qiu, a professor of Communications at the Chinese University of Hong Kong, believes, "Advertising and marketing are major factors behind contemporary youth culture online. Youth form information networks of information and technical support that are supplementary to the key institutions of education and family."[427] In *Personal Communications in the Digital Age*, Baym likened it to the development of the automobile which led to fears that teenagers would isolate themselves from society and their families.[428] Qiu also discusses an inequality in the family structure and stressed the helplessness of youth. He states, that previously youth were at a disadvantage. They had no control and could not leave the family. In the past, elders had control over youth's actions.[429] The ability to be online changes all of that. The internet opened a brand new world for youth as they could "go" places they did not have access to before. But Qiu also reminds us, that youth are more likely to lose control of their spending on information technology products or simply just lose their handset.[430] Hughes, indirectly compliments youth when he says, "Old systems like old people tend to become less adaptable."[431] I found a whole other discourse on youth in my interviews that agree with Hughes and say youth are flexible, grow up with the technology of social media, and that is an advantage. The social science scholars identified distinct adult fears

[425] Urs Gasser; Sandra Cortesi; Momin Malik; and Ashley Lee, 77.
[426] Ibid.
[427] Qiu, p. 153
[428] Baym, p. 41,43.
[429] Qiu, p. 125-132.
[430] Qiu, p. 133-134.
[431] Hughes, p. 51.

of youth not being responsible online. As the Harvard study shows, there is not much empirical evidence to support that fear.

3.5.2 Department of Defense Views on Youth

The military does not formally address youth as a relevant social group in any of its publications. However, the federal government published a report entitled *Net Generation: Preparing for Change in the Federal Information Technology Workforce* in 2010. The Deputy DoD CIO at that time, Mr. Dave Wennergren, co-chaired the study and the report is posted on the DoD CIO website as an authoritative source. While the report addresses more than just the DoD, the Department represents 41% of the federal workforce,[432] so I consider it relevant. I also interviewed Mr. Wennergren and he intimated that what was in the book was absolutely relevant to DoD. In fact, he gave me a copy of the book and encouraged me to use it as a source in my dissertation.

The report's central idea is that youth behave differently because they grew up in a digital world. It makes statements such as, "The net generation understands intuitively the power of Web 2.0. They are the first cohort of young people to have been immersed in an interactive, hyper-stimulating, digital environment since birth, having 'grown up digitally'"[433] and "Members of the net generation are 'digital natives.' Having grown up with technology in every aspect of their lives, IT capabilities are second nature to them."[434]

The report claims that federal recruiters will actively search for job candidates that possess the latest Web 2.0 knowledge and schooling. The report also makes sweeping statements about

[432] United States Office of Personnel Management. *Sizing Up the Executive Branch of the Federal Government: Fiscal Year 2012*, Washington, DC: Jan 2013, p. 7.
[433] Federal Chief Information Officer Council. *Net Generation: Preparing for Change in the Federal Information Technology Workforce.* Washington, DC: Apr 2010, p. 63.
[434] Lisa Chen, Mike Dover, and John Geraci. *The Generation Gap: Youth as Recognized Authorities*, New Paradigm Learning Corporation, 2006, 1, quoted in Federal CIO Council. *Net Generation: Preparing for Change*, p. 63.

youth and their work habits based on recent research papers on youth in the workplace. One of the generally stated norms about the net generation is their use of and reliance on social media. In their study on the generation gap, Chen, Dover and Geraci state "The net generation has grown up in an interactive world. They are used to pulsing their social networks for information and feedback and working collaboratively on tasks."[435] Other scholars, like Tapscott and Gilles, claim the next generation is adapting the workplace to themselves instead of them adapting to it. Basically, "Blocking social networks and discouraging any non-work internet usage basically prevents them from taking a break on their own terms, whether it be for gaming, blogging, surfing or chatting,"[436] and this is unacceptable to the youth of today. Another claim from the *Federal IT Workforce Study*, is that the youth 'need' social media and are anxious without it. "The deprivation of connectivity to the internet has a visceral impact on the net generation."[437] The *Federal IT Workforce Study* and the research that it supports claim that youths' experiences are different from adults' experiences and that social media affects youth more so than adults.

General Martin E. Dempsey, United States Army, the Chairman of the Joint Chiefs of Staff and the nation's highest ranking military officer, understands the impact social media has had on society and worries about young people disqualifying themselves from military service by posting pictures of themselves on social media doing something wrong or worse, illegal. In a December 2013 speech, Dempsey said, "I worry a bit about the young men and women who are now in their teens, early teens, and who probably underestimate the impact of their persona in social media and what impact that could have later in life on things like security clearances and

[435] Lisa Chen and Ian DaSilva. *Architecting the Future: Net Gen Career and Talent Management Processes*, Ngera Corp: 2008, p. 11-12, quoted in Federal CIO Council. *Net Generation: Preparing for Change*, p. 63.
[436] Don Tapscott and Bill Gilles. The 8 N-Gen Norms: Characteristics of a Generation, p. 13, quoted in Federal CIO Council. *Net Generation: Preparing for Change*, p. 63.
[437] Federal Chief Information Officer Council. *Net Generation: Preparing for Change in the Federal Information Technology Workforce*. Washington, DC: Apr 2010, p. 63.

promotions."[438] In one sentence, Dempsey's concern transcends the youth discourse and crosses into security and privacy risk, sociotechnological inevitability and responsible online behavior. His basic assumption is that it's inevitable that potential recruits are on social media, that young people have the potential to act irresponsibly online, and their behavior online has inherent security and privacy risks. While DoD does not formally address youth as a separate social group, very senior leaders such as Wennergren and Dempsey have made public statements on youth adding to this discourse.

3.5.3 Service Members' Views on Youth

Youth enters the discourse as a subset of the privacy and security risk, sociotechnological inevitability and responsible online behavior discourses. Some leaders, like a female Colonel in the Army, believe that youth put others at risk because of their irresponsible behavior. "I think it [age] absolutely makes a difference. Because I don't think young people think before they write. They write something and post it out there, if they post a photo, or they post what they consider to be funny. They don't get it because they are young. I think that is all part of youth and inexperience."[439] Social media could also be used as a lesson for youth on acting responsibly. One Captain told me, "Our battalion commander used to get the S6 [signal officer on the battalion staff] to put up all the pictures of the lieutenants from weekend at the Monday staff meeting. It was a teaching point--it's such an integral part of younger soldiers' lives."[440]

A young Marine who was a platoon commander in Afghanistan on a remote outpost said after the urination incident, he would not let his Marines take personal cameras off the forward operating base (FOB) because he did not trust them not to post the pictures. "You couldn't take

[438] Associated Press. "Gen. Dempsey Worries Teens' Social Media Use Could Disqualify Them From Military Service," *CBS News*, Washington, DC, Dec. 4, 2013.
[439] Interview with female Army Colonel, November 2, 2012.
[440] Interview with Army Major, Feb 23, 2013.

cameras out of the patrol base with the exception of squad cameras. The little chip would go directly into our COC [command operations center]. It was controlled. It was signed in and out. So any photographs from that would never make it to the internet. I never let them take helmet cam's [cameras] out. I wouldn't let them take personal cameras out. We never took anything like that outside the wire. That was our platoon policy because honestly I didn't trust the younger ones."[441]

An officer in Command of the Air Force Academy Prepatory School in Colorado Springs said it is so important for young people to be connected that depriving them of that is an excellent method of punishment. "When a cadet is in trouble, the cell phone is the first thing taken away--it's an umbilical cord."[442] She said she addressed the use of social media in her first Commander's call with the cadets just to make them aware that there are standards in the military regarding conduct. "Younger people grew up posting and with email, there's just no filter. It's definitely something we have to talk to them about. They are used to ongoing electronic conversations that the world can see."[443]

Not everybody believes only youth are irresponsible with social media. When I asked a National Guard Major his opinion, he replied, "I don't think there's any evidence that says that. I see a lot of Colonel's posting dumb stuff on there too. I think the mistakes that are made are soldiers of all ranks who don't understand the risks."[444] Likewise, a female brigade commander told me a fellow commander confided his fears to her about social media and she thought they were overblown. "I was horrified that a brigade commander told me he was actually afraid social media would replace the face to face interaction of leadership. That younger people would use it

[441] Interview with young Marine Captain, Jan 3, 2013.
[442] Interview with Commander, US Air Force Academy Prep School, Jan 3, 2013.
[443] Interview with Commander, US Air Force Academy Prep School, Jan 3, 2013.
[444] Interview with National Guard Major, October 31, 2012.

to avoid direct contact. I think that's ridiculous. We have so many terrific young leaders in the military who would never do that."[445]

In keeping with the sociotechnological inevitability discourse, youth are also touted as the future of the DoD and it is often stated that the DoD needs to evolve to use the tools the youth are using. Secretary of Defense Gates looked to American youth as the United States' representatives to foreign countries who require modern skills that enable them to identify with indigenous youth. In a press interview, Secretary Gates spoke of hiring Mr. Price Floyd as the ASD for Public Affairs, "I want somebody who can tell us how the Department of Defense communicates with our own people, most of whom are 18 to 25 years old…And somebody who can communicate with people that same age around the world, where we've got operations going on.[446] Deputy Secretary of Defense Lynn stated social media was used to reach the young as a recruiting tool "The defense department depends on social media for recruiting so the Services can reach young people--that's the demographic we are trying to reach." Colonel Mayfield from European Command said, "Senior leaders must be trained to have an understanding of what the soldiers and junior officers already know--the 'digital natives' will be critical to success in the social media environment as well."[447]

In the next section, I separated the comments from older service members from the comments of younger service members to see if there was a distinction in the common themes of each social group. Many interviewees made sweeping statements about older people or younger people without many facts or real life vignettes to back up their statements, which was not the

[445] Interview with female brigade commander, November 8, 2011.
[446] Donna Miles. "New Public Affairs Chief Sets Out to Transform Communications Processes," *American Forces Press Service*, Washington, DC, June 15, 2009.
[447] Thomas D. Mayfield III. "A Commander's Strategy for Social Media," *Joint Forces Quarterly*, Issue 60, 1st Quarter, 2011.

case in the other three discourses I studied. The senior officers I interviewed, had an overwhelming opinion that youth were irresponsible with social media. They also commented on a constructed view of youth's expectations that social media would be ubiquitous in society. The younger service members were a little defensive about personal responsibility and thought there were responsibility and security violations at all ranks, not just the young. The younger service members did also agree there was an expectation of youth to use social media.

In the interviews with the more senior service members, there was much comparison of youth and more senior service members' actions. A Marine colonel said, "Older people see it as a more public environment whereas younger people are just throwing crap out there. Anybody can say whatever they want. That's what it goes back to. I don't feel like they have as much responsibility with what they are saying. Because they are a lot more comfortable with it, everybody does it. It's a lot easier, whereas old people shy away. One, they're not as familiar with it and the other is that they more understand the impacts."[448] A female Air Force colonel agrees, "It all has to do with maturity level and age. An occasional reminder is more than sufficient for Majors and above. Younger folks up to Captain need a little more direct attention."[449] She then makes a statement that implies that younger soldiers are not trained on operational security like the training she went through when she was young. "Those older like us, learned about OPSEC [operational security] when we were young. Controlling [the content on] Facebook is just another application of that."[450] An Air Force lieutenant colonel states that the military was somehow different when she was younger, and has no respect for the

[448] Interview with USMC Colonel, Nov 1, 2012.
[449] Interview with Female Air Force Colonel, Jan 3, 2013.
[450] Interview with Female Air Force Colonel, Jan 3, 2013.

responsibility of today's youth. "There were those before the digital world who care about laws. The youth don't care, they consider social media a right."[451]

The theme of comparison continues with a male Army lieutenant colonel's comments on security, "It's a little bit generational in my opinion. I don't think the current generation has as much of an appreciation for the security risk."[452] The same officer then accuses the younger generation with not caring. "The older people may not understand the technology and the younger people don't care."[453] An Air Force colonel believes it is not a conscious decision to care or not to care. "They don't think about it be being sexual, political, or profane—the younger generation just doesn't think about it."[454] A female Air Force colonel agrees, "Younger folks grew up with posting and email-there's just no filter. There's definitely a disconnect we need to talk to them about. The youth are used to ongoing electronic conversations that the world can see."[455] The Air Force lieutenant colonel believes youth do not really understand the consequences of using social media. "Younger people do not have the maturity to understand that online presence is forever--even if you hit delete."[456] A Marine Corps colonel agrees, "I think people that are older generally are a little more thoughtful about what they put out. I think the younger people don't realize the impact of what people are actually reading about what you are saying. I think younger people tend to think whatever you say is OK. Far greater than an older person that would be concerned about 'what is the impact of what I just said?' in a public environment."[457]

[451] Interview with Air Force Lieutenant Colonel, Jan 28, 2013.
[452] Interview with Male Army Lieutenant Colonel, Oct 30, 2012.
[453] Interview with Male Army Lieutenant Colonel, Oct 30, 2012.
[454] Interview with Air Force Colonel, Jan 10, 2013.
[455] Interview with Female Air Force Colonel, Jan 3, 2013.
[456] Interview with Air Force Lieutenant Colonel, Jan 28, 2013.
[457] Interview with USMC Colonel, Nov 1, 2012.

A female colonel accuses younger service members of hiding behind digital media instead of confronting an obstacle (or a person) face-to-face. "They don't get it because they are young. I think that is all part of youth and inexperience. I mean I think today's culture--today's young people are so much more sarcastic and so much more 'in your face' than we were. I mean when we were lieutenants, you still had all the drama, but you would generally face it head on, face to face, you would man up and tell somebody off. You didn't hide behind your computer screen and do it from miles and miles away. And you didn't do it in such a way that it affected other people."[458]

Not everyone thinks youth are irresponsible with social media. An Army brigade commander tried to get one of the junior officers in her command to start a unit Facebook page and found little interest. She said, "I'm astonished as how many people, people younger than me, like my Majors aren't interested and don't communicate that way. I thought everybody did. I'm having to drag people to get on."[459] A Navy Captain, a helicopter pilot, trusts his sailors' use of social media, "I think young sailors are responsible. Maybe I am just naïve. Those dudes trust me to drive the bus and I trust them in the back. I trust them. I know them well."[460] When I prodded him on the subject as to why he trusts them so much, he said, "I never gave my guys guidance on social media. I just let them go, I didn't mess with them. Part of it is a trust thing, but part of it for me was a bandwidth thing--I had a lot of stuff to worry about; like we never got shot at we never shot anybody. Nobody got killed, we never had any crashes while I was in command--but I was always worried about that crap. You know we're trying to launch helicopters in the Persian Gulf, day, night, shitty weather, mountains, desert--that's the crap I was worried about

[458] Interview with ARNG Colonel, Nov 2, 2013.
[459] Interview with Army Colonel, Brigade Commander, Nov 11, 2012.
[460] Interview with Navy Captain, Jan 20, 2013.

and whether some guys were sending--or what they were doing on their email accounts. I just didn't really care. I just really didn't have the bandwidth to really think about that or worry about it. And what's the worst that could happen, you make a fool of yourself?"[461]

A Marine Corps helicopter pilot had a different view. She believes people are a product of their environment and draws a distinction between students who attend military versus civilian colleges. "For Marines or DoD personnel, they are generally responsible with a few outliers. The public at large…For college kids what is responsible or not? I think it gets skewed based on education level or what kind of environment they are in as far as what's considered responsible or not. I think people have enough common sense not to put illegal things on there. This is all assumptions based on the fact that it didn't exist when I was in college and I wasn't in a normal college environment [she attended the U.S. Naval Academy]. I think maturity comes with age and maturity comes with environment, i.e. if you are in a frat house or a huge party school, then what may seem mature…the aggregate level of maturity is much lower."[462]

Another theme within the youth discourse, by older service members is speculating on how young people use social media and their expectation the technology would be there for them to use. A three star general involved in the social media decision told me, "The Services were split on their positions on social media. One of the reasons given was young people expected to use the military networks like they use their home networks."[463] Another senior official, the Acting DoD CIO, stated two themes publically many times, "We want the Department of Defense to be the employer of choice for the 'net generation,'" and "The millennial workforce expects to use social media."[464] There were many positive comments in this thread and rumination that it might

[461] Interview with Navy Captain, Jan 20, 2013.
[462] Interview with USMC Lieutenant Colonel, helicopter pilot, Oct 30, 2012.
[463] Interview with three star general, Feb 13, 2013.
[464] Interview with former Acting ASD NII/DoD CIO, Jan 20, 2011.

be a good thing that younger service members are poised to take advantage of social media. An Air Force colonel mulled, "I think the younger generation understands how to access information quick too as far as agile decision making. I think they understand how to leverage technology so well that there are all kinds of positives in that vein that we're probably just realizing."[465] A different Air Force colonel divulged the difference between his use and younger service members' use of social media. "I consider Facebook something I do on my computer or laptop. They [youth] have a much more mobile attitude about it."[466]

An Army lieutenant colonel also believes there is a difference between older and younger service member's attitudes toward social media, "I think it may be more generational. I think the new generation just coming in the Army now are more apt to share everything. They assume that it's OK and that's just the way the world works."[467] A retired Navy officer, now DoD support contractor declared, "For youth, it's a culture change. They expect instant results."[468] An Army major says the younger generation cannot live without it, "It's such an integral part of young soldiers' lives."[469] The retired Navy support contractor, assumes older people struggle with the technology and offer, "If you don't understand it [social media], ask your kids. Ask your young soldiers. It's implicit with kids, they'll show you how to use it."[470] As for how younger service members use the technology, an Air Force colonel says, "The younger generation use it like an old school chat room. The young use it as an immediate planning tool. They use it to contact friends to make dinner or event plans."[471]

[465] Interview with Male Army Lieutenant Colonel, Oct 20, 2012.
[466] Interview with Air Force Colonel, Jan 10, 2013.
[467] Interview with Male Army Lieutenant Colonel, Oct 30, 2012.
[468] Interview with DoD Support Contractor, Apr 15, 2013.
[469] Interview with Army Major, Feb 25, 2013.
[470] Interview with DoD Support Contractor, Apr 15, 2013.
[471] Interview with Air Force Colonel, Jan 10, 2013.

The Marine Corps Harrier pilot believes social media is a move toward the positive, "I think it depends on your generation. People who have grown up with this stuff. It seems to be less of an issue with them because they are used to it. This is just a matter of course with them, nothing out of the ordinary."[472] He said on his deployments to Iraq and Afghanistan, "Facebook was absolutely a must. That's the way the younger generation communicates and that's also the way my younger Marines communicate with their parents--and that's the way their parents communicate with us."[473]

The younger service members had very strong opinions that there is no difference between younger or older service members' actions on social media. An Army National Guard major said, "I think the mistakes that are made are soldiers of all ranks who don't understand the risks."[474] The first lieutenant in Afghanistan agreed, "Responsibility is not about being young or old, it's just something people do—either they are or they aren't."[475] The Army captain in Hawaii was indignant, "I don't think young people are any more irresponsible than older people. I've seen some majors and lieutenant colonels post some pretty dumb stuff."[476] He also said responsible conduct is about personal responsibility, whether you are young or older. "It's all about military bearing, they know what they are supposed to and not supposed to post and they just obey the rules."[477]

A Marine Corps captain was very vocal on the subject of youth and responsibility. He pointed out there are plenty of young service members entrusted with high security clearances. "Military personnel are privy to a lot more sensitive information in general than civilians. In the

[472] Interview with Army Colonel, Feb 17, 2012.
[473] Interview with USMC Lieutenant Colonel, Harrier Pilot, Nov 27, 2011.
[474] Interview with ARNG Major, Oct 31, 2012.
[475] Interview with First Lieutenant in Afghanistan, Mar 4, 2013.
[476] Interview with Army Captain in Hawaii, Dec 6, 2012.
[477] Interview with Army Captain in Hawaii, Dec 6, 2012.

Pentagon, it's probably about the same but throughout the country, the 1% of the population that is the military is privy to some very serious national security information. And sometimes at the higher levels, like at the Top Secret level, there are these intelligence analysts that are Privates with a Top Secret clearance. You know usually they are selected for their responsibility level. They're a little bit more mature, but still they have access to insane amounts of very sensitive information and then they are on Facebook."[478] His point is that senior leaders in the DoD trust them to be responsible or they would not have that access.

Young people also commented on how ubiquitous social media is with the younger generation. A Marine gunnery sergeant speculated, "I'd say about 99% of the people under 30 are on Facebook. Probably about 60% or over 30 are on Facebook, I mean it's just used more I think by younger people. It's a fairly recent thing. I mean when did Facebook come about 2002 maybe? It's only about ten years old. I just think the younger generation kind of took off with it."[479] The first lieutenant if Afghanistan, the same officer who called her Facebook page, her *lifeline* during her deployment said, "Young people got so comfortable growing up with Facebook. People get so obsessed with it, it becomes such a part of their lives."[480] The gunnery sergeant offered this example from his deployment. "Young people need to be connected and it's gotten worse. In 2002, I was on a ship and there was no expectation of contact with loved ones except by letter, and those were few and far between. In 2008, everyone was on social media and expected to talk to their family every day. The library onboard ship has a few machines that anyone can use and the line is sometimes fifty people deep waiting for ten minutes on the computer."[481]

[478] Interview with Marine Corps Captain, Jan 3, 2013.
[479] Interview with USMC Captain, Jan 3, 2013.
[480] Interview with First Lieutenant in Afghanistan, Mar 4, 2013.
[481] Interview with USMC GySgt, Apr 6, 2012.

The discourse on youth was completely inconsistent. Both young and older service members made sweeping generalizations about each generation as did social science scholars and DoD leadership. A unique quality of the youth discourse is that it underpins all of the other discourses I looked at. Many of the older service members I interviewed thought youth in general were irresponsible online, a possible security or privacy risk, and there was no way to stop youth from using social media—it is inevitable and DoD should embrace it. The younger service members I interviewed said they are indeed responsible online, service members of any rank can be a security risk, and they agreed social media technology use is inevitable. There were dissidents in each social group who took the opposite position, making any analysis inconsistent. If you recall in chapter two though, the DoD senior civilians eventually overturned the ban on social media. Clearly from the comments captured in this section, Secretary of Defense Gates, Deputy Secretary of Defense Lynn, Assistant Secretary of Defense of Public Affairs Price and Acting DoD Chief Information Officer Wennergren were all very much influenced by the youth discourse and it had a direct effect on overturning the policy.

3.6 Chapter Conclusion

The discourses surrounding risk (security and privacy), sociotechnological inevitability, responsible online behavior and youth directly affected the decision to open the DoD networks to social media. I explored these discourses from the view of social science scholars, DoD as an institution, and from individual service member interviews to discover how these discourses shaped the policy shift from blocking social media on DoD official networks, to openly allowing it and encouraging its use. Through discourse analysis, I found that the concept of security and privacy risk were of much concern to all, yet this discourse diminished over time as this work progressed. Yet, service members struggle with the balance of cost versus benefit of using social

media. They like the ability to contact their friends and family often during deployments, but are sensitive perceived risks associated with social media. The success of social media in society directly affected DoD's views on the subject. Whether it is the desire to keep up or the desire to not be left behind, the members of DoD accepted the use of social media by DoD as inevitable, resulting in a permissive social media policy. This widespread acceptance eclipsed the security and privacy debates, rendering those concerns as less important than the need to contact family and friends through social media while deployed.

The discourse surrounding responsible online behavior shows that DoD expects its service members to accept responsibility for their actions online and in return, service members believe it is their duty to act responsibly online. However, the stated norms do not always match up with service members' actual behavior. There are several recent examples of poor behavior on social media in the news which causes senior leaders to question the responsibility of those under their command, especially youth. Youth, as employees of DoD, are often credited solely as the reason DoD opened its networks to social media. However, the youth discourse is inconsistent, containing many sweeping generalizations. It was a combination of the discourses of security and privacy risk, sociotechnological inevitability, responsible online behavior and youth that influenced the senior leaders in DoD to reverse the social media policy and mandate the open use of social media on all DoD networks. In the next chapter, I will explore the post policy environment.

CHAPTER 4
A POST POLICY ANALYSIS OF THE EFFECTS OF THE SOCIAL MEDIA POLICY ON THE DEPARTMENT OF DEFENSE

In this chapter, I will analyze the new post-policy effects on the Military Services associated with allowing social media on the DoD networks. I will compare the original February 2010 policy with the amended September 2012 policy and discuss the results of my interviews in 2014 with network providers from the Air Force, Army, Marine Corps and Navy in order to discern how the new policy affects their Service networks and network operations procedures. I will also present a proposal to amend an existing conceptual framework for innovation in capability development to include policy, or in the case of social media on DoD networks, the lack of policy, as a factor in delivering and sustaining operational capabilities.

4.1 Changes to the Social Media Policy from February 2010 to September 2012

The table below contains the significant changes from the initial policy to the final policy concerning use of social media on DoD networks. The Directive Type Memorandum (DTM) is a temporary policy issued when DoD leaders want to publish a policy quickly. It requires a signature from the Secretary of Defense or Deputy Secretary of Defense.[482] The DTM 09-026 was signed by Mr. William Lynn, the Deputy Secretary of Defense. The intent was to fill a policy gap quickly until a formal policy could be written and staffed Department-wide. The DoD staffed and signed DTM 09-026 in nine months in order to provide formal guidance to DoD Components and service members, specifically for the use of social media, which was a contentious topic at the time. The original title was, *Responsible and Effective Use of Internet-based Capabilities*. The purpose stated, "This memorandum establishes DoD policy and assigns

[482] http://www.dtic.mil/whs/directives/corres/writing/DoD_Issuances.ppt.

responsibilities for the responsible and effective use of Internet-based Capabilities, *including social networking services (SNS)*."[483]

The final Department of Defense Instruction (DoDI) establishes policy and assigns responsibilities within a functional area assigned in a DoD Component Head's charter. DoDI 8550-01 falls within the DoD Chief Information Officer's charter and is signed by Ms. Teri Takai. The title and scope of the policy changed during the deliberate process and thirty two months it took to arrive at policy closure. The final title of the new social media policy is *DoD Internet Services and Internet-based Capabilities*. The purpose of the policy expanded from establishing policy for "responsible use" of Internet-based Capabilities to "Establishing, operating and maintaining DoD Internet services on unclassified networks to collect, disseminate, store and otherwise process unclassified DoD information."[484] The final policy still covers the use of social media, but it does not specifically focus on the social networking aspects of Internet-based capabilities like the previous policy in the DTM. The definition of Internet-based capabilities remains consistent between the initial and final policies.

	DTM 09-26, Feb 25, 2010	DoDI 8550.01, Sept 11, 2012
Title	Responsible and Effective Use of Internet-based Capabilities	DoD Internet Services and Internet-based Capabilities
Purpose	To establish policy for responsible and effective use of Internet-based capabilities, including social networking services	To establish policy regarding establishing, operating, and maintaining DoD Internet Services on unclassified networks to collect, disseminate, store and otherwise process unclassified DoD information
Signature	Deputy Secretary of Defense	DoD Chief Information Officer
Applies To	All authorized users of the NIPRNET	Specifies DoD components such as OSD, Joint Staff, Defense Agencies,

[483] Deputy Secretary of Defense. *Directive Type Memorandum 09-026 – Responsible and Effective Use of Internet-based Capabilities*, Department of Defense, Washington, DC: Office of the Deputy Secretary of Defense, February 25, 2010, p. 1.
[484] Department of Defense Instruction. *DoD Internet Services and Internet-Based Capabilities*, Number 8550.01, DoD Chief Information Officer, September 11, 2012.

	DTM 09-26, Feb 25, 2010	DoDI 8550.01, Sept 11, 2012
		etc. Specifically states it applies to contractors and non-DoD entities supporting DoD
Networks	NIPRNET	Includes NIPRNET, but extends responsibilities to apply to MWR, military exchange, and lodging program networks
Policy (a)	DoD networks open to Internet-based Capabilities	DoD networks open to Internet-based Capabilities
Policy (b)	Commanders can temporarily limit access for OPSEC or bandwidth concerns	No mention of this
Policy (c)	Can continue to block prohibited sites such as pornography or gambling	States decisions to operate networks shall balance benefits and vulnerabilities
Policy (d)	Users must conduct themselves within the standards of the Joint Ethics Regulation	Users must conduct themselves within the standards of the Joint Ethics Regulation
Policy (e)	No mention of this	Commanders can provide alternate, stand-alone capability to access Internet-based Capabilities for mission or morale purposes
Definition of Internet-based capabilities	Consistent between the two documents	Consistent between the two documents
Personal Devices	No mention of this	Policy specifically states it does not prohibit employees from using Internet-based capabilities for personal purposes on personal devices
Privacy	No mention of this	Shall not be used to collect, disseminate, store or process non-public DoD information
Public Websites	No mention of this	Guides operation of DoD public websites
Education/ Training	No mention of this	Requires education and training of users for clearance and release authorization of DoD information
References	12 references	69 references
Definitions	3 definitions	31 definitions
Pages	9 pages	49 pages

Table 4.1 Changes in DoD Social Media Policy from Feb 2010 to Sept 2012

The purpose and scope of the policy changed significantly during the thirty two months between the release of the initial and final policies. Because the DTM was a hastily developed policy, it did not specifically state the specific DoD components it applied to. The initial policy merely stated it applied to all authorized users of the NIPRNET. The final policy was more deliberate and specifies some of the DoD Components it applies to, such as the Joint Staff, OSD and Defense Agencies. The DoDI also states it applies to DoD contractors and non-DoD entities supporting DoD that use the NIPRNET. Additionally, the final policy extends its scope beyond the NIPRNET to Morale, Welfare, and Recreation (MWR), military exchange and military lodging networks.

The policy language matured in the final version, but became less specifically focused on the use of social media. Both policies state the DoD networks will be open to Internet-based capabilities and that users should conduct themselves within the guidelines of the Joint Ethics Regulation, which guides the ethical conduct of service members and DoD civilian employees. The statement that was so important when publishing the DTM, that military commanders could temporarily limit access for OPSEC or limited bandwidth concerns, surprisingly does not appear in the final DoDI. The initial DTM also states that network operators can continue to block prohibited sites, such as pornography and gambling websites and this also does not appear in the final DoDI. Instead, the DoDI states that "decisions to collaborate, participate, or to disseminate or gather information via DoD Internet services or Internet-based Capabilities shall balance benefits and vulnerabilities. Internet infrastructure services, and technologies provide versatile communication assets that must be managed to mitigate risks to national security; to the safety, security, and privacy of personnel; and to Federal agencies."[485] This nebulous statement infers

[485] Department of Defense Instruction. *DoD Internet Services and Internet-Based Capabilities*, Number 8550.01, DoD Chief Information Officer, September 11, 2012, p. 2.

that commanders have decision authority in certain instances, however it was more clearly stated in the initial DTM.

The final DoDI had several statements that did not appear in the initial policy document. The first is that commanders may provide an alternate, stand-alone network capability to access Internet-based Capabilities, so that they do not have to be allowed on the DoD networks. The DoDI also specifically states that DoD policy does not prohibit DoD employees from using personal devices to access Internet-based Capabilities for personal use. The final policy addresses privacy in that DoD capabilities shall not be used to collect, disseminate, store or process non-public DoD information. There is a large section in the final DoDI, which does not appear in the initial DTM, concerning the governance and use of public websites and education and training of DoD personnel for clearance and release authorization of DoD information. Finally, because it took thirty-two months to finalize the policy in a deliberate process, the page count increased from nine to forty-nine, the references increased from twelve to sixty-nine, and the definitions increased from three to thirty-one.

Over the course of thirty-two months, the DoD attitude towards the use of social media changed drastically. The initial policy was focused on preventing the military services and network providers from restricting access to social media. The final policy seems to accept the use of social media by DoD and is instead focused on the responsible use of internet services by service members. This shift is evidenced by the service network providers' statements in the next section. Almost all of the network providers I interviewed three years after the social media policy took effect, believe the social media policy is here to stay and the responsible use of social media is a leadership issue. Controlling access to social media by technical means is not

necessary if leaders can control content by leadership of people via direct orders and written policy.

Most of these network providers have been in the DoD for over twenty years. In their experience, restricting access to social media is not an effective technique to achieve the 2010 policy goal of the responsible use of social media. Smart phones now provide an alternate means of access to social media, even in austere environments such as Afghanistan. Service providers believe educating users and promoting the responsible use of social media will allow DoD to keep up with the advances in society and use social media to its advantage.

4.2 Service Post Policy Actions

From January to February of 2014, I interviewed officer and civilian network providers in the Air Force, Army, Marine Corps and Navy to discover how the current social media policy affected their respective networks. The basic questions I asked were (1) Are you following the current DoD social media policy and guidance? (2) Did you see a difference pre- and post-policy? (3) Have you experienced any recent issues with service members posting notifications about the death of a colleague on social media before the next-of-kin is notified properly by the DoD leadership? I separated these sections by Service to see if there were any trends particular to any Service that stood out as unique.

4.2.1 Air Force

I spoke with an Air Force Lieutenant Colonel about the current status of the Air Force networks. He was in command at Malmstrom Air Force Base, Montana at the time of the policy shift to open the networks to social media in February, 2010. He shared, "At Malmstrom, we had a unique problem in that we only had a ten megabit pipe coming into the base. After the policy came out, we delayed implementation until we got more bandwidth coming in. When

they finally upgraded the bandwidth, Malmstrom fully allowed social media on the networks."[486] He also said the base leadership informed service members on the base that the command had submitted a work order for a network upgrade for more bandwidth and as soon as it was installed, network operations would open the Malmstrom networks to social media in accordance with the initial policy guidance. At that time, the Air Force leadership, at Malmstrom Air Force Base, took advantage of the provision in the initial DTM for commanders to block Internet-based Capabilities for bandwidth concerns.

The same lieutenant colonel was the base communications officer in Kandahar, Afghanistan from the summer of 2012 to the summer of 2013. He said in Kandahar, "The Air Force paid $100,000 per month for an alternate network; we called it Morale Net. So there was no need to open the military networks to social media. We operated and controlled the Morale Net as a stand-alone network--it worked better than the Air Force network."[487] The September 11, 2012 social media policy DoDI specifically states the current policy "Does NOT [sic] prevent unit commanders or Heads of the DoD Components from providing alternate, stand-alone capabilities to allow access to Internet-based Capabilities for mission or morale purposes."[488]

When asked about service members posting about deaths on social media before the next-of-kin is notified, the lieutenant colonel said, "Getting people to behave responsibly is a leadership issue…The year I was in Afghanistan, there were four aircraft crashes where people were killed. We did shut down the Morale Net and went to 'Comm Minimize'[489] on the military networks

[486] Interview with Air Force network director, Jan 27, 2014.
[487] Interview with Air Force network director, Jan 27, 2014.
[488] Department of Defense Instruction. *DoD Internet Services and Internet-Based Capabilities*, Number 8550.01, DoD Chief Information Officer, September 11, 2012.
[489] Comm Minimize is a military term for blocking non-mission essential traffic on the networks. Basically the network provider only allows access to .gov and .mil websites for a limited period of time. I have seen it used during deaths and fiber cuts where you have to minimize the civilian traffic going across the networks to preserve bandwidth.

until the families were notified…but that only affected Kandahar. We also gave orders not to mention it to people back home until the families were properly notified."[490]

4.2.2 Army

The Army and Air Force operate completely separate networks in Afghanistan. I spoke with the Director of the Joint Network Control Center-Afghanistan (JNCC-A), who operates and manages the Army base level networks in Afghanistan in 2014. He said, "The networks are open to social media in Afghanistan now and we have not had significant issues as a result of social media use. Each Regional Command (RC)[491] has its own policy….basically, it all comes down to the personality of the leadership. There is a standard and it's the leadership's job to enforce it. In RC East where I am, we do block streaming media social sites, like YouTube during the day to conserve bandwidth, but sometimes for a big sporting event, we'll ease up on it--and at non-peak duty hours, we allow it."[492] The JNCC-A Director believes that since the February 2010 decision to allow social media on the networks, DoD has raised the awareness of its service members and adequately trained them to be responsible online. "Of course we've incorporated a lot of training since the early days and people are more aware of the risks…some of it is just awareness. We've turned our screen savers into cybersecurity propaganda screens for education…they list all the do's and don'ts now."[493]

I questioned him about the KIA issue and he mentioned there was shift in network operations in Afghanistan from just four years ago when he was last there. In the early years of the war, there were no alternate means of communications available to service members besides the

[490] Interview with Air Force network director, Jan 27, 2014.
[491] The NATO International Security Assistance Force partitioned Afghanistan into six sectors called regional commands. Each command is led by a different partner nation. RC-East includes the provinces of Bamyan, Ghazni, Kapisa, Khost, Kunar, Laghman, Logar, Nangarhar, Nuristan, Paktika, Paktiya, Panjshayr, Parwan and Wardak. It covers 46,000 square miles, approximately the size of Virginia, and shares a portion of the border with Pakistan.
[492] Interview with JNCC-A Director, Jan 24, 2014.
[493] Interview with JNCC-A Director, Jan 24, 2014.

military networks. Now that there are civilian providers, it changes the control the military had on communications entering and leaving the country. He said, "When I was there before, if there was a soldier killed, we would use the blue coat proxy at the FOB [Forward Operating Base] level to block transmissions back to the states. It is grossly ineffective because there are now other methods of communicating with home. It became pointless. There is now a 3G network and 32 cellular providers in Afghanistan…everyone has a smartphone. Since at least May 2013, it is treated it as a leadership issue and an order is issued instead of blacking out the base. We haven't had one incident since I've been here of anyone in the Army revealing a KIA before the family finds out."[494]

I also talked to the Army Lieutenant Colonel whose most recent assignment from 2012-2013 was my old job in Kuwait at the TNOSC running the wide area network to Kuwait, Afghanistan, Qatar and Bahrain. Presently he is stationed in the operations center at United States Cyber Command (USCYBERCOM) observing the DoD networks in real time. He believes the issue of social media has moved to the background based on other more important priorities to DoD at the moment. "I don't think we train to social media awareness very well--but I think that's because social media does not appear to be a significant problem relative to the other big rocks we've had to move recently that require additional Soldier training. From suicide awareness/interdiction to sexual assault prevention, same sex marriage, force reductions and new evaluation schemes/forms, social media is just not a hot topic in terms of training…I've seen social media integrated into OPSEC training and encountered some good social media awareness training aids…but the evolving nature of the social media platforms, what type of information that they make available/public, the various privacy settings and schemes of the social media

[494] Interview with JNCC-A Director, Jan 24, 2014.

providers make this a challenging landscape to capture in training time and materials…If significant loss of life, limb, eyesight or information could be directly attributed to social media, it might be more of concern for leaders right now. In terms of networks and information, I think 'insider threat' is a much greater concern at the moment, yet there is little training related to 'insider threat' detection and even fewer tools and instrumentation designed to defeat it."[495]

The lieutenant colonel told me his commanding general, was pressuring him to come up with metrics on social media use on the Army networks to build a case to block it again. He said he tried to capture good metrics but the Army really did not have to proper tools for capturing them. He told me the following story. "The commanding general's position was 'Am I running an operational network or am I running a commercial ISP?' For the better part of the forty-odd weeks that I worked for him, I routinely briefed Facebook 'usage' on the network each week at our update to the Army Central Command Commanding General. Again, our quantification and measurement metrics sucked. We just didn't have to tools to measure bandwidth 'consumed' by Facebook or other social media. At best, we could count Facebook 'hits,' which was basically a measurement of how many HTTP get requests we saw go out to an address in the facebook.com top-level domain. This metric did not measure actual bandwidth consumed, nor did it account for content embedded in Facebook that came from other domains…But we could count, measure and compare 'hits,' and that's what we briefed, with Facebook being the overwhelming champion each and every week by an order of magnitude of five to ten over the number two capability on the list. But the idea to block Facebook never gained any traction because the NIPR user experience was pretty decent and consistent, and the SIPR troubles that did occur

[495] Interview with USCYBERCOM Operations Officer, January 9, 2014.

could never be attributed to insufficient bandwidth resulting from everyone surfing Facebook."[496]

This lieutenant colonel did not think it was possible to reverse the current DoD policy allowing social media on the DoD networks. "Unless users are in a bandwidth-constrained environment, with early entry or austere conditions, I think social media usage is here to stay…at least where it is permitted. Right now on NSA's [National Security Agency] networks, Facebook and LinkedIn are blocked 24/7. NSA is both DoD and IC [Intelligence Community] so they can get away with it. But I think resistance to social media is OBE [overcome by events] at this point in DoD."[497] By using the term OBE, this officer allows for coping with events beyond his control. He gives us a sense of inevitability, not surrender or failure. He acknowledges that the world of military operations is incredibly busy and that over time, even a contentious topic, such as social media, can become accepted as routine because there is no time to explore further options and it is not a priority anymore. His last anecdote was about the Air Force taking advantage of the new policy provision to supply an alternate 'Morale Net' in Kandahar. "Air Force Central Command (AFCENT) purchased 'Morale Net' for airmen in the barracks…Basically, it was free but crappy wifi. As a result, social media was blocked on their work networks since the command was paying for personal wifi for off-duty use. Now, the price tag was expensive…tens of millions of dollars for Morale Net--and the free wifi bandwidth sucked. It's not a practical solution and does not scale to CONUS or outside of the AOR [area of responsibility]. But it was a unique idea…I have no idea how much money AFCENT 'saved' by doing this, but I thought the approach was interesting."[498]

[496] Interview with USCYBERCOM Operations Officer, January 9, 2014.
[497] Ibid.
[498] Ibid.

4.2.3 Marine Corps

The post-policy interviews I conducted for the Marine Corps showed an increasingly more positive attitude toward social media. I followed up a year later with the Marine Corps civilian I interviewed previously, who is responsible for information assurance and protection on the networks. He said the challenges of social media have changed over the past year. Instead of focusing on how Marines could possibly either infect the network or post inappropriate content, the focus today is protecting Marines from foreign intelligence or criminals. "The social media concern shifted from concerns about OPSEC, to concerns about facing an intelligence act or criminal activity."[499] He says a new tactic they are seeing more and more on the Marine Corps network are people impersonating general officers on social media in order to defraud other people. The Marine Corps calls this kind of attack an 'evil twin' and has developed a policy and set procedures to counter this different kind of attack. "A new tactic we have is we do an 'evil twin' search to see if people are impersonating a general officer on social media. We collect the URL's for all the general officer official social media sites so that if there is an impersonator, we can get it shut down right away."[500]

When asked if the Marine Corps networks were open to social media, the civilian IA manager said they were following the current policy requiring open access. "We still do blocking based on mission need. It's still a bandwidth issue--do you want your organizational email to work or do you want people to use social media? We can restrict bandwidth and functionality so they don't want to use it. It's not shut off but we've not made it efficient to use because of other mission needs."[501] He did say there was some selective blocking of types of social media based

[499] Interview with Marine Corps civilian IA manager, Feb 7, 2014.
[500] Ibid.
[501] Ibid.

on that site's philosophy on appropriate content. "Somebody turned Tumblr on for recruiting and it's X rated. Facebook has decency rules that don't exist in Tumblr. We figured, they don't need Tumbler--so we turned it back off."[502] The Marine Corps network operators believe that even though the new social media policy does not specifically say the network providers must continue to block pornography and gambling sites, they are covered under a different network operations regulation to not allow prohibited sites on their networks.[503]

Another change noted by the Marine Corps civilian was that more people have smart phones now so they do not need to access social media on their work computer. He believes the use of it on official government networks has gone down significantly. "Social media on mobile platforms will be interesting. The young people are using their smart phones instead of their desktops to do social media. It's no longer a bandwidth issue that I have to deal with. It's not the big issue that it was—the use of social media has gone back into the homes and on their personal devices. It's not so much an issue on the networks right now."[504] A year previously, this government civilian predicted the policy would allow the Services to selectively restrict content if they had a good reason. He called the focus on restricting access, 'Shiny object syndrome.' Since social media was a new capability and it was unknown if the threat really

[502] Ibid.

[503] I had not heard of this issue previously and it had been three years since I looked at Facebook's privacy policy so I looked again. Facebook has something they call community standards where they will report and remove content based on violence, threats, self-harm, bullying, harassment, hate speech, graphic content, nudity and pornography. Tumblr also has community standards but they appear to be looser than Facebook's and do not have direct consequences. As a comparison, I looked at each community's stance on bullying and harassment. Facebook's policy is very direct. "Facebook does not tolerate bullying or harassment. We allow users to speak freely on matters and people of public interest, but take action on all reports of abusive behavior directed at private individuals. Repeatedly targeting other users with unwanted friend requests or messages is a form of harassment."[503] Tumblr's policy is more of a guideline for use, not an actual policy with consequences. "Be thoughtful when posting anything involving a minor. Don't post or solicit anything relating to minors that is sexually suggestive or violent. Don't bully minors, even if you are one. Being a teenager is complicated enough without the anxiety, sadness, and isolation caused by bullying."[503] Facebook has consequences if you violate their decency code, in that if you violate their code, they will inactivate your account. Tumblr has no such provision.

[504] Interview with Marine Corps civilian IA manager, Feb 7, 2014.

existed, he stated, "I predict the policy will shift. We won't completely restrict access. We may restrict access from certain platforms. We already restrict it a little. We don't allow photo updates, instant messaging, or Farmville on our networks."[505] Today he still calls the attention on securing Marines from the dangers of social media 'shiny object syndrome,' but believes a social media brand presence is now necessary. "I think the social media policy was passed because they were reacting to shiny object syndrome. It was the cause du jour--people wanted to be seen working in it and using it. People wanted to look cool to young people. However, now I truly believe you need a social media brand presence. If I don't have one, anyone who claims to be me is me."[506] This is similar to what I have heard in previous interviews speculating that if a person is not on social media, someone else is making reference to them thereby giving them a social media persona they are not aware of. Representing yourself as a unique individual is now known as branding. In just a year, this civilian shifted his position from wanting to block social media to believing it necessary for the Marine Corps to be properly represented with a brand presence.

I also spoke to a Marine Corps colonel who had several different experiences using social media for official work tasks. He said social media use and the acceptance by the Marine Corps has "gotten better--the Marine Corps has always been ultra-paranoid about security the way we have been with general information. People think, 'If I post this, am I going to get in trouble?'"[507] This colonel believes the culture in the Marine Corps is currently changing to support the use of social media and young people are a great influence. "The young are all about it, they are leading the way. They have the ability now to stand up and speak for the

[505] Interview with Marine Corps civilian IA manager, Mar 20, 2013.
[506] Interview with Marine Corps civilian IA manager, Feb 7, 2014.
[507] Interview with Marine Corps Colonel, Feb 7, 2014.

command."[508] He shared an example that inspired him to encourage the use of social media in his own command. "My niece went to Navy boot camp recruit training. Her family was able to track her progress in the class through social media, just by liking the command's page. Once the school posted a picture of her in action--that picture was shared by every member of her family and all of her friends. Look how much publicity the Navy got just for that one shot."[509] He had a different experience when he tried to implement the use of social media in a Marine Corps school. "I tried to do the same thing as the Commander of the Marine Corps Communications and Electronics School in Twenty Nine Palms. I found to get people to post things is tough. I had to give a special order to have my people post stuff every week. The families want to know what is going on and I feel we owe it to them to give them feedback on how their child is doing."[510]

In 2009-2010, the same Marine Corps colonel worked for the Combined Security Transition Command – Afghanistan (CSTC-A), who were responsible for training the national police forces of Afghanistan. He said, "Over there, we didn't block anything. In fact, we started Facebook and YouTube pages for the command. The public affairs office worked for me. My guidance was they had to write a story and post it every single day. We had our interpreters put the stories in Dari and Pashtu and post them on Afghan social media sites." I asked him if the Afghan people were on social media as well and could he tell if they were reading the stories? He said, "We had a young Navy kid in Combat Camera who knew all about Google News. If we posted stories on Google News, we got hits from all over the world. You can run Google's analytics to see where the hits come from. It was kind of cool to see that your stories were being shared

[508] Ibid.
[509] Interview with Marine Corps Colonel, Feb 7, 2014.
[510] Ibid.

globally."[511] The colonel said the use of social media was accepted because his commanding general was a supporter of social media and encouraged people to share what they were doing on it. "I worked for Major General Caldwell in Afghanistan. His philosophy was, 'We have a good news story to tell. I don't care if its good news or bad news, as long as it's accurate news.'"[512]

The colonel shared one more story with me of a different type of use of social media. "When General McChrystal was the Director of the Joint Staff, he understood the need for putting the news out there. He told his Directors, 'I'm going to be in this chat room during the day and I'm going to task you in there.' It was a new process that they didn't pay attention to in the beginning, but once the general started using it, everyone jumped on board."[513] The acceptance of the use of social media has always been more successful if there is a general officer sponsor or supporter. "My boss at the time was General Basla. He went to the National Security Agency (NSA) for the day where as you know, you can't have your cell phone or blackberry in the building. He got a short notice tasker in that chat room from McChrystal to work on policy language for the coffins coming back to Dover Air Force Base. There was a time crunch because there was something in the news about it that day. His staff saw the task, we got it in real time in the chat room. He didn't even know he had been tasked until he got back and we had a whole binder of stuff ready for him with the draft policy language all done. If General McChrystal had sent an email to General Basla point-to-point, Basla would've been the only one who had seen it and that would have significantly affected our response. Putting information out there in the domain where people can see it is a good thing."[514]

[511] Ibid.
[512] Ibid.
[513] Interview with Marine Corps Colonel, Feb 7, 2014.
[514] Ibid.

4.2.4 Navy

I spoke to a Navy Captain who was the Communications Officer for Strike Group Eisenhower based out of Norfolk, Virginia. She said she was against the use of social media at first but a member of her crew convinced her there was value in it. "I was Strike Group Eisenhower N6 [communications officer] out of Norfolk, Virginia in 2009. We had to decide if we were going to allow Facebook on our ship. We found we could analyze the bandwidth flow to see what people were doing…and then there's always the question of if these people are doing official business--can the bandwidth handle it? At first I was like, there is not a snowball's chance in hell that we should allow this. My master chief had to convince me that it was a good thing. We need the ability to conduct official business at all times. Of course we have what we call 'River City Comms' where we cut off all the pipes if we need to. We have the processes in place to handle it if something were to happen. It's OK as long as we can control who has access when we need it."[515] River City is a slang reference to the song in the play *the Music Man*, 'Ya Got Trouble.' If a Navy ship encounters trouble on board such as a death of one of the crew or an attack on the ship, the Captain will declare River City which means the network access off the ship is turned off until the problem is resolved.[516] It is similar to the Army, Air Force and Marines blacking out a base in Afghanistan when a service member is killed.

Since this reference was in 2009, before the official policy came out, I questioned her on why the Strike Group decided to allow it. She told me, "At the time we didn't have a good reason not to adopt social media. There was an article in the ship's newspaper when we rolled it out. It was a big deal--we were reaching out to the younger generation and their families. At the time the CNO [Chief of Naval Operations] had a blog, the Navy had an official Facebook page and so did

[515] Interview with Navy Captain Comms Officer, Feb 19, 2014.
[516] Stewart, Joshua. "Limited Online Access Stresses Sailors at Sea," *Navy Times*, April 15, 2012.

Recruiting Command--the CNO was a big proponent of social media. The Navy was trying to appeal to the younger generation. The youth are not going to look at a navy.mil site to get their information, but they will friend the Navy on Facebook and get information that way."[517] This Navy captain had much to say about the younger generation--which she also defined as thirty years old and less. Her comments were much like those of the more senior officers in the previous chapter. "This younger generation grew up with social media usage. That's how they communicate--if you take it away, you may as well cut off their right arm."[518] She also expressed the previously voiced concern of responsible online behavior and the risk of privacy violation. "The younger generation's idea of privacy is very different than ours--the stuff they put out there on the net is not the stuff I would put out there."[519]

When I asked her about what was different in the Navy post-policy, she said that in the absence of policy, her command made up its own to compensate. "The only thing we did differently after February of 2010 was we created a Strike Group Instruction containing guidance on use of different communications platforms. It was more than just social media. It included not plugging in your IPOD on the SIPRNET, not plugging in USB devices, basically the 'Do's and Don'ts' of using the official networks. We needed a way to hold people accountable. There's always a consequence for violating the rules as long as the rules are clear."[520] This Navy captain's views were very much in line with many senior officers I interviewed as much as three years earlier. The Navy's decision to expand their social media policy to include more than just social media was the same resolution DoD came to two years later.

[517] Interview with Navy Captain Comms Officer, Feb 19, 2014.
[518] Interview with Navy Captain Comms Officer, Feb 19, 2014.
[519] Ibid.
[520] Ibid.

I also talked to a Navy captain who was the commander of the Network Node at the Hopper Information Services Center in Suitland, MD. He told me, "At the time [pre-2010 policy], social media was a complete unknown. Competing expectations playing out were not a good thing--there was no universally held position in the Navy. Some rue the day we allowed social media on the networks. Some are concerned about wasting time at work or OPSEC violations. Some are firmly committed to the other side and embrace it fully. All sides have a point."[521] The captain was a supporter of social media and said he was an early adopter. He believed social media is good for morale while out on the ship, especially his own morale. "It was a big deal for our Navy people. We gained the ability to stay in communications with our family. You know you have those guys who say, 'Back in the good old days, you got on a ship for six months and nobody needed to call home.' Well I don't remember those as the good old days. It is so much better having instant communications than waiting days on end for the mail to show up on the helicopter every three weeks."[522]

As an intelligence officer, the Captain believes it has changed the nature of his job somewhat. "There are so many good things we are doing with it now. I'm in the intelligence community, we are using social media for crowdsourcing to find out all kinds of things. The challenge is putting in the right rewards mechanisms to influence behavior. The old bureaucratic way of doing things isn't enough to get people to work together anymore. You know the old strategic estimate where you study an enemy like the Soviet Union for a long period of time for future events that may or may not come? That is not the dynamic in intelligence right now--it's a need for immediate information. We feel like we missed it with the Arab Spring and have to catch up

[521] Interview with Navy Captain Intelligence Officer, Feb 28, 2014.
[522] Interview with Navy Captain Intelligence Officer, Feb 28, 2014.

with the rest of the world."[523] He also believes youth are more innovative with social media and have taught more senior people a different business process with respect to control. "With social media, groups form. I'm excited by it. Us older people had to learn how to cede control. The young people--the way they do it now is to talk amongst themselves and make decisions. They're not waiting for us to do it for them."[524] The potential loss of control was an important consideration to the captain. He brought up the 2013 Kenyan election crisis and said "Governments can't hid from public knowledge anymore by controlling the media."[525] He did say the Navy could still retain control while at sea by regularly practicing and employing River City operations to minimize use of the unclassified networks during a crisis.

4.2.5 Service Comparison

The Air Force stayed consistent with its reaction to the social media policy in chapter two. As seen at Malmstrom Air Base, it did not rush to comply. Instead, the Air Force calculated the effect on current operations and delayed opening the networks at some bases until the bandwidth was upgraded to support social media. The Air Force also took a unique approach in Afghanistan at Kandahar Air Base by providing an alternate, free morale network base-wide for recreational internet use, so they could block the access to social media on the military network. This was such a success, the Air Force asked DoD to include it in the new social media policy—and OSD complied.

The Army has accepted access to social media as inevitable. While some senior leaders still resist, overall the Army accepts the current policy and has moved on to solving bigger problems

[523] Ibid.
[524] Ibid.
[525] Interview with Navy Captain Intelligence Officer, Feb 28, 2014.

such as suicide and sexual harassment. The Army believes responsible online behavior is a leadership issue that can be supported by training and awareness.

The Marines have completely shifted their position on social media from one of banning social media from the networks, to embracing it fully and exploring how to brand the Marine Corps on social media. The Marines also accept the use of social media as inevitable and like the Army, believe leadership is key to responsible online behavior. The Marines have shifted their concerns from the fear of individual Marines compromising themselves and their units on the networks to protecting individual Marines from outside threats such as fake profiles and financial attacks.

The Navy was a supporter of social media from the beginning, largely due to the isolation at sea. Social media provided sailors with a more immediate means of communicating with family and friends, than the previous method of random mail helicopters a few times a month. The Navy officers seemed confident that if necessary, the Navy can always go back to blocking social media since there is no other way to communicate off a Navy ship than the ship's communications system. This is not the case for the other Services, with ground-based missions as we have seen with the proliferation of cellular networks in Afghanistan. The issue of service members posting information about a KIA before the next-of-kin is properly notified did not appear to concern any of the current network providers from any Service.

All the network providers assured me their Services are following the current social media guidance. However, the Army lieutenant colonel that now works at U.S. Cyber Command stated the networks at NSA and U.S. Cyber Command are not open to the use of social media and there is no morale network provided. In the last chapter, a different Army lieutenant colonel said the Army networks in Korea and U.S. Strategic Command are not open to social media as well. It

appears that most DoD networks are open to social media, but there are still some pockets of resistance who do not allow open access to social media. In the next section, I will propose an amended construct for a colleague's theory on a framework for innovative capabilities.

4.3 A Conceptual Framework for Innovative Technology

In his 2009 article, "A Conceptual Framework for Innovation in Capability Development," John Garstka, a Department of Defense acquisition professional and noted author, proposes a four element model to understand the role of different types of innovation in capability development. Military capability development involved creating a material solution to satisfy an operational need.[526] Garstka believes, "Military organizations need to be able to innovate successfully to develop and sustain competitive advantage. Militaries that have failed to innovate have often suffered at the hands of competitors who have more effectively developed and employed new warfighting abilities."[527] He introduces the possibility of disruptive innovations that challenge the existing organizational values or business processes. Garstka professes that when an innovative technology is introduced, the organization, processes and people all require adjustments to accommodate it.

An example of a disruptive innovation used in Garstka's paper was the radical invention of the steamship in 1819. At first, steamships could not compete with sailing ships for transoceanic missions and found their niche in rivers and lakes where they could steam ahead without relying on wind. As steamship technology improved, they finally outperformed sailing ships when crossing oceans. Once the steamship became the default method of transoceanic passage, the

[526] Chairman of the Joint Chiefs of Staff Instruction, "Joint Capabilities Integration and Development System," CJCSI 3170.01H, Washington, DC, 10 Jan 2012.
[527] John Garstka. "A Conceptual Framework for Innovation in Capability Development." In Crosscutting Issues in International Transformation, Interactions and Innovations Among People, Organizations, Processes, and Technology, edited by Derrick Neal, Henrik Friman, Ralph Doughty, and Linton Wells II, Washington, DC: National Defense University, Dec 2009, p 22.

companies that made sailing ships in the commercial shipping markets failed and eventually went out of business. Not one sailing ship builder converted to making steam ships.[528]

In his paper, Garstka studied several innovation frameworks including the H.J. Leavitt and Massachusetts Institute of Technology (MIT) models that attempted to capture reasons for organizational change. Using those models as a starting point, he developed his own theory in his Revised Four Element Model as shown in Figure 4.1.[529]

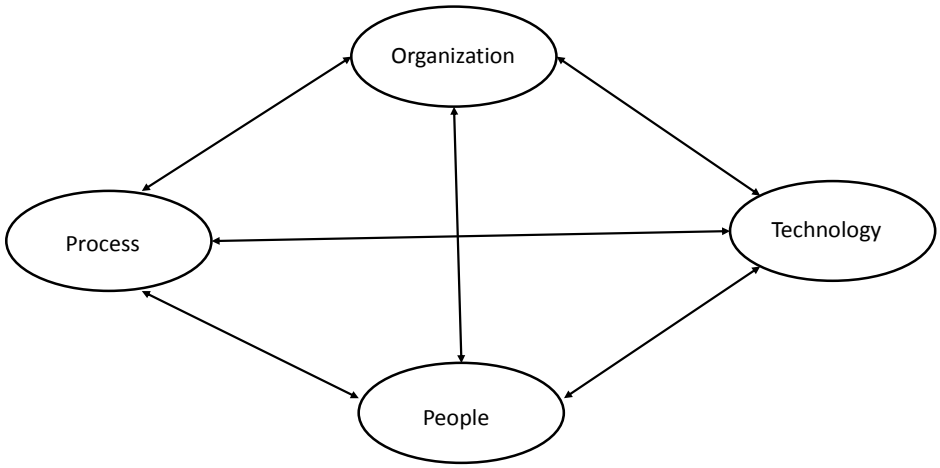

Figure 4.1: Garstka's Revised Four Element Model

According to Garstka, the four elements in the model, organization, people, process and technology are necessary to deliver and sustain operational capabilities. 'Organization' refers to the structure of DoD. 'People' represents the roles and the skills of the users of the technology, who are the service members and government civilians employed by DoD. 'Process' denotes a set of activities taken to achieve a goal of the DoD. It is focused on the business practices of the

[528] Ibid, p. 30.
[529] Ibid, p. 39.

organization. The 'Technology' is the disruptive technology. The model itself illustrates the interconnections among the four elements and suggests that a change in any one element affects the other three.

Using Garstka's example of the steam ship in his revised four element model, the innovative technology is the steamship. The people (or customers) at first resisted the use of steamships for transoceanic missions because they were not economically advantageous. As the steamship technology improved and became more economically feasible, the customers became open to change. In the process element, the lake and river shippers quickly switched to using steamships instead of sailing ships because of the steamship's innovative ability to move without wind. Eventually, as transit by steamship became economically affordable, the transoceanic shippers changed their processes and converted from sailing ship transport to steamship transport. The organizations also changed as the desire for steamships increased. New organizations formed in order to build steamships to meet the demand. As the steamship technology improved and the desire for sailing ships decreased, the sailing ship organizations failed and went out of business. Garstka argued that over time, the processes, organization and people catch up with the innovative technology and come to a state of closure or normalization. In a DoD acquisition and in Garstka's paper, this state is called "initial operational capability."[530] Garstka states the technology often initially outpaces the processes, people and organization. He then asserts, in the use cases that he studied, the processes have to catch up with technology before the organization and people change.

[530] Department of Defense. *Dictionary of Military and Associated Terms*, Washington, DC: Chairman of the Joint Chiefs of Staff, Nov 8, 2010 (as amended Feb 14, 2014), p. 128. In DoD, there is a future state called "full operational capability" that is more mature which signifies that every until that is supposed to have that capability has it and is capable of maintaining it. The distinction in DoD Acquisition is that during Initial Operational Capability, the capability development is over, yet units are still procuring and employing it. At Final Operational Capability, every unit has it fully deployed.

Below is Garstka's visual implementation of his model where in Figure 4.2, technology leads organization, people and processes. In Figure 4.3, the processes catch up with the technology before the people and organizations advance.

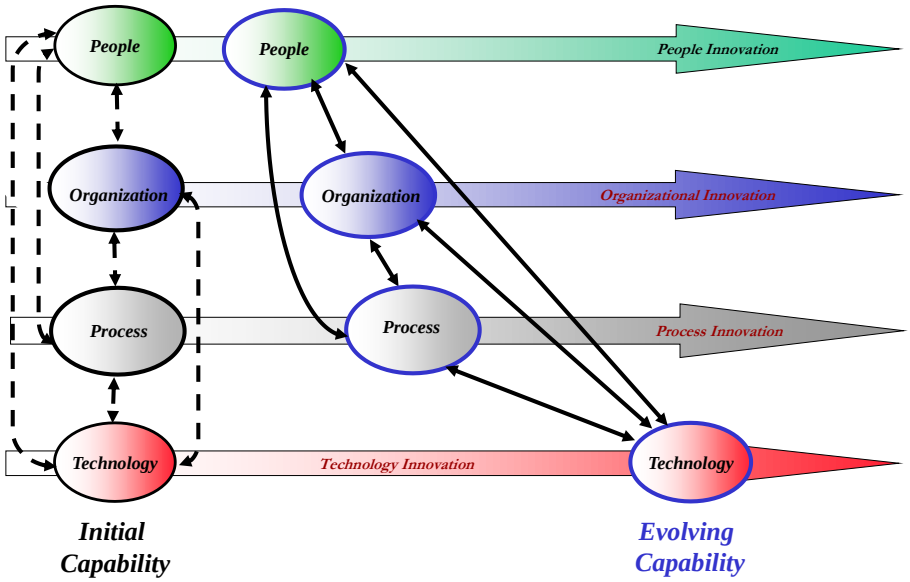

Figure 4.2: Technology Innovation Leading[531]

[531] Garstka, p 46.

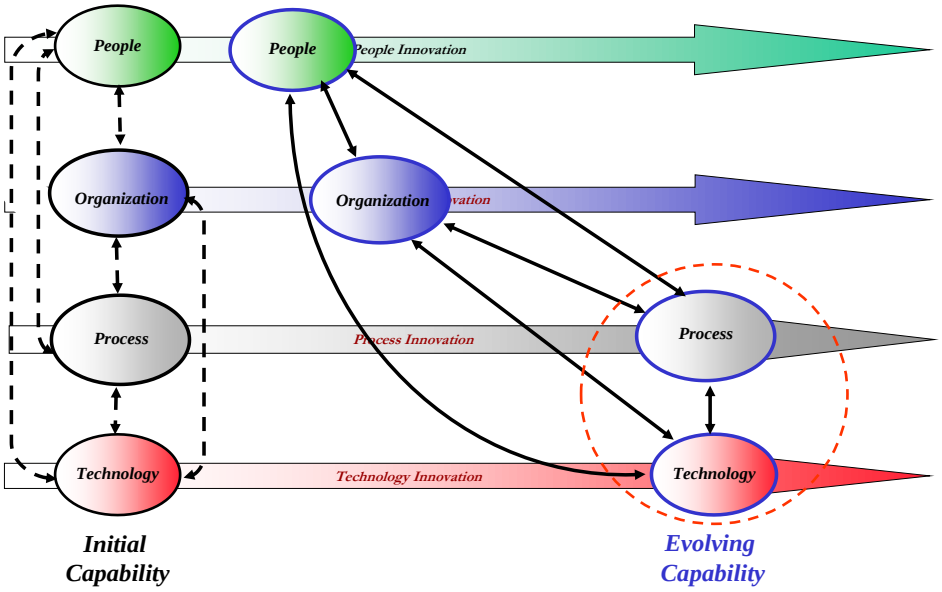

Figure 4.3: Process Links Up With Technology[532]

In the final stage shown in Figure 4.4, the people and organizations catch up to the processes and technology and the entire system reaches initial operating capability.

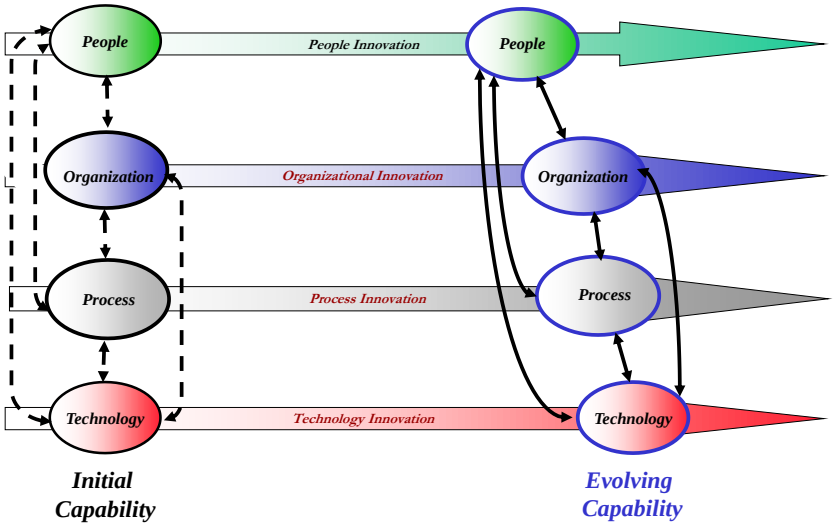

Figure 4.4: Initial Operating Capability[533]

[532] Ibid, p. 47.
[533] Garstka, p. 47.

4.4 A Proposal to Expand Garstka's Model to Include Policy as an Element

I believe social media is an innovative technology with the possibility to have a profound effect on the people, organizations, and processes of DoD. However, if we put the adoption of social media by the U.S. military into Garstka's model, it does not follow the exact same pattern as his other case studies. At the beginning, when social media is introduced, the technology outpaces the people, organization and processes of DoD as portrayed in Figure 4.2. The social media case study deviates from Garstka's model shown in Figure 4.3, where the process is supposed to catch up to the technology before the people and organization. In the case of the introduction of social media to DoD, the absence of policy while the topic was debated prevented the organization and processes from evolving. Conversely, the people progressed because they developed social media skills on their personal home networks as shown in Figure 4.5.

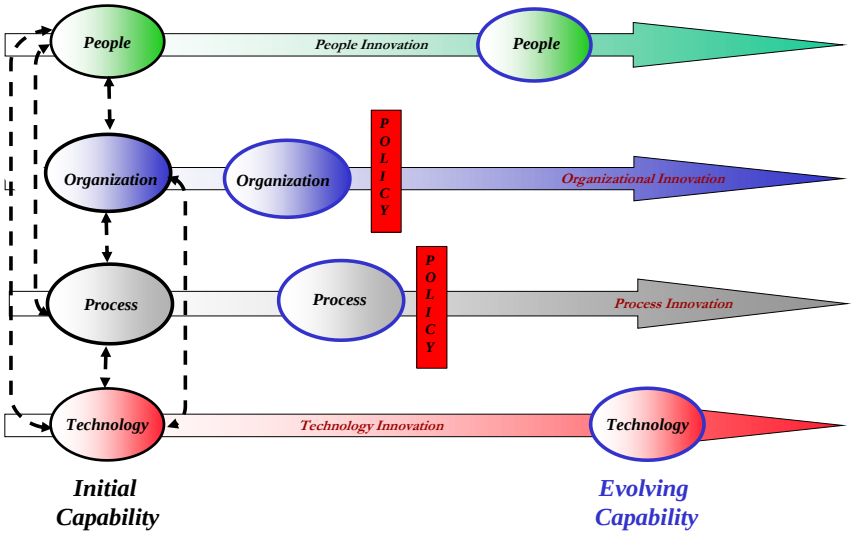

Figure 4.5: Absence of Policy Blocks Progress of Organization and Process

I believe Garstka's Four-Element Model should be expanded to a Five-Element Model to include policy, since the absence of policy was able to halt the progress of the organization and

processes. Doctrine is loosely included in Garstka's definition of process but doctrine and policy are not equivalent entities. According to the DoD *Dictionary of Military and Associated Terms*, doctrine is "Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative, but requires judgment in application."[534] The DoD Instruction outlining the DoD Directives Program defines DoD Policy as, "A set of principles and associated guidelines to direct and limit DoD actions in pursuit of objectives, operations and plans."[535] Doctrine is a recommendation that requires judgment of military personnel in a process, whereas policy is directive in nature. Below, in Figure 4.6, is my modification of Garstka's model to include policy as an element.

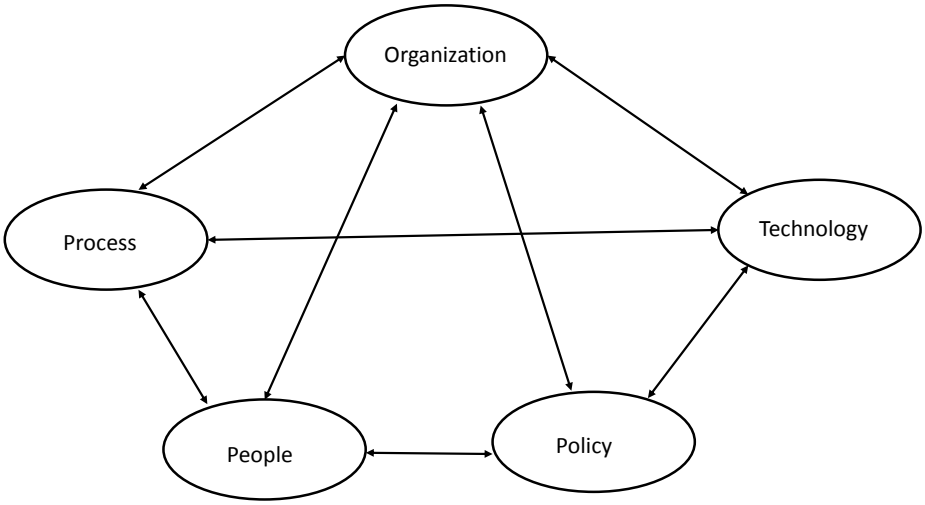

Figure 4.6: Expanded Five-Element Model

[534] Department of Defense. *Dictionary of Military and Associated Terms*, Washington, DC: Chairman of the Joint Chiefs of Staff, Nov 8, 2010 (as amended Feb 14, 2014).
[535] Department of Defense Instruction. *DoD Directives Program*, Number 5025.01, Director of Administration and Management, August 30, 2013, p 35.

The existence of policy or the lack thereof also affected technology, organization, people, and processes. The lack of a DoD social media policy, in some cases such as the Marines, who banned it entirely, held back the exploration of the utility of the technology. The organization of DoD did not change in the absence of policy. The processes to use social media were also lagging since JTF-GNO banned most social media from DoD networks. However, people developed social media skill sets from using social media on commercial networks in their personal lives. Figure 4.7 is a depiction of policy holding back organization and processes, while people evolve.

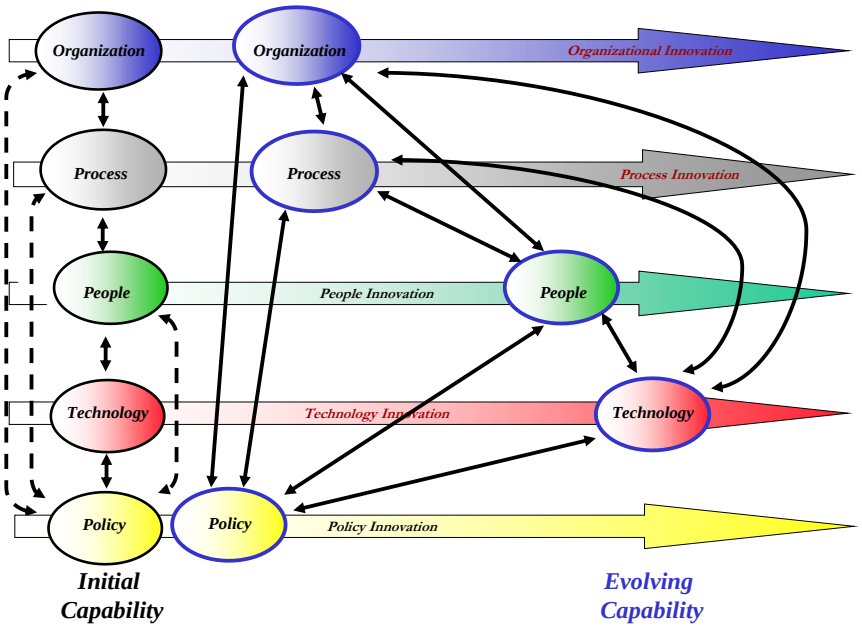

Figure 4.7: Policy Holds Back Processes and Organization

When the DoD social media policy was first signed in February 2010, it absolutely affected organization, people, technology and the processes. New offices were created to handle social media for DoD. People were now provided official training and guidance to run social media sites and to use social media responsibly. Processes sprung up and were documented throughout the DoD on how best to use social media to accomplish DoD's goals and missions. The next

several paragraphs detail some specific changes to organization, people and processes after the DoD official released the social media policy.

Organization changes include the Office of the Secretary of Defense, Joint Staff and each Service creating their own Social Media Offices within their Office of Public Affairs. General Dempsey, the former Chief of Staff of the Army, hired contractors to manage his social media roll out when he assumed the position of the Chief of Staff of the Army.[536] Other senior leaders assigned people within their staffs to organize and monitor the unit's official and family member support groups social media presences as a part of their jobs.[537] Another change to DoD organization was the Defense Advanced Research Projects Agency (DARPA), a DoD organization created to discover or develop innovate technology solutions in support of national defense, created an entire program office to research Social Media in Strategic Communications. The general goal of this new office is to develop a new science of social networks built on an emerging technology base of capabilities.

People's skill sets have changed by the introduction of social media. As stated above, some service members are assigned as managers of their unit's social media presence as a result of a process change. This requires some self-study and some DoD provided training materials on how to create and maintain a social media site as well as familiarity with the official rules of DoD about social media. People also have to decide how they want to use social media and if they want to participate in the official DoD social media presence or restrict their social media use to their personal lives, or a combination of the two.

There are many examples of how the DoD processes changed to adjust to the technology of social media. General Dempsey, now the Chairman of the Joint Chiefs of Staff, and other senior

[536] Interview with Army Captain, April 3, 2013.
[537] Interview with Marine Colonel, Feb 7, 2014.

leaders have started having Facebook Town Halls, where they inform people they will be on Facebook for a block of time and answer questions live online.[538] A traditional Town Hall usually takes place in an auditorium where people gather and ask questions of the senior leader face-to-face. Service member or family members sometimes did not have the opportunity to participate because they were working or at a family event. A Facebook Town Hall allows participation from just about anywhere with a smart phone. Another change has been the frequency with which a service member can contact home while on deployment. Service members now can have daily contact with their families and even help a child with homework regularly. The old model was infrequent contact whenever a service member could get to phone or get on a computer to send an email, as opposed to the daily, interactive communication that is possible today. This also affects the job satisfaction and morale of people in a positive way.

The Army social media center website created many new products available online to reflect the new processes associated with social media: a social media handbook, a library section containing policies and training products, and a U.S. Army I-Phone App, where service members have access to Army news on their smart phone. Another new product created by the Army Social Media Office is a branding tool kit that service members can use in a new process to create their own official unit social media sites using the Army approved graphics. It is the Army's attempt to standardize official sites on social media. The graphics are available to anyone who wants to create a social media site, though soldiers are still required to register all official social media sites with the social media office. This affects people's skill sets required to

[538] Jim Garamone. "Dempsey Addresses Issues During Facebook Town Hall," *American Forces Press Service*, Dec. 5, 2013.

create official social media sites. No formal training is needed to create an official Army site, but self-study is required.[539]

Another example of process change occurred within the Publics Affairs field. According to both Public Affairs officers I interviewed, social media shortened the products and timeline for official DoD press releases due to its users' demand for immediate responses. Releasing official content has become a fluid, on demand type process, in contrast to the static "daily official press conference" of just a few years ago. The public affairs officers claim the shelf life of stories has been reduced. They claim, because of the abundance of stories, a story stays in the news for a lesser period of time before it is overcome by the next viral event.[540] The loss of control was a common sentiment from many of my interviewees. While DoD use to control the narrative coming from the DoD sources, more service members voice opinions on social media with commentary that is not filtered by DoD public affairs offices. DoD also has no control over the spouses of service members who are free to post content at their will. While there are processes in place to contend with a service member posting inappropriate content, there are no processes in place to force family members to post responsible content.

Policy is obviously a factor in the ability of an innovation to move forward to initial operating capability. Figure 4.8 contains what the use of social media in DoD looks like four years post-policy in 2014. Without policy, the organization, processes, people, and policy would not have all matured and caught up with the technology.

[539] http://www.army.mil/create.
[540] Interviews with Public Affairs Officers on 14 Nov 2012 and 26 Oct 2012.

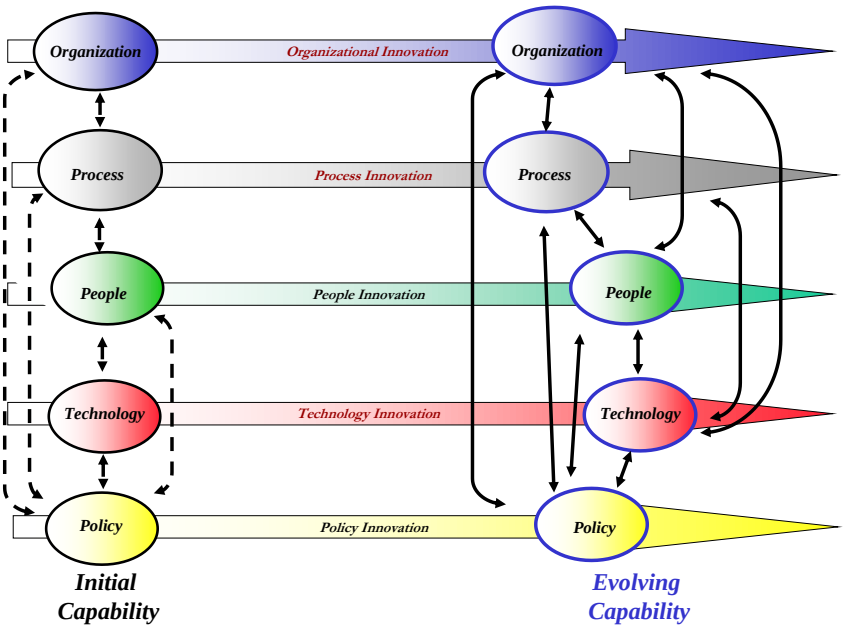

Figure 4.8: Social Media in DoD at Stabilization/Closure

Once the policy stabilized, the organization and processes were able to evolve and mature. The addition of policy to Garstka's innovative capability development model more completely represents how the use of social media evolved within the DoD.

4.5 Chapter Conclusion

This chapter captures the social media policy changes over time, the current views of certain Service network providers since the policy was signed, and the importance of the existence of policy within a framework for capability development. A common thread that weaves through the evolution of the policy change, the attitudes of the current Service network providers, and the proposed conceptual framework is leadership. Leadership is frequently named by service members throughout this project as essential to the success of safely introducing social media to DoD networks. Leaders also have the power to change processes and organizations. However, as seen in the previous section, in DoD, the policy must support the process and organization changes, or they cannot be changed. Therefore, leaders must engage with the policy makers and

provide sound arguments for a policy change, much like the Acting DoD CIO, Dave Wennergren and the ASD for Public Affairs, Price Floyd in their appeal to the Secretary of Defense to overturn the social media policy in 2010. They met much resistance from other senior leaders in DoD, who were entrenched in the current methods. The examination of the situation by the Secretary of Defense and the influence of the discourse surrounding social media allowed them to prevail and the social media policy was changed to allow open access on all DoD networks.

CHAPTER 5

CONCLUSION

This dissertation explores the origin of the social media policy within the DoD. I concentrated my research on how the DoD came to closure on the decision to first restrict the use of social media; the decision to mandate opening the networks to social media and finally, the debate within the post-closure period over the sufficiency of the policy. I also proposed an amended framework for social media capability development and showed how the absence of policy impeded the development and acceptance of a social media capability for the DoD.

The majority of the existing work on social media and the military was focused on the need for a consistent policy throughout DoD. The DoD initially set a restrictive policy and then suddenly reversed it, to mandate the use of social media on DoD networks. The reasons for this sudden policy reversal were unclear and a discourse analysis assists in clarifying the motive for the policy shift. The main empirical findings are chapter specific and were summarized within chapter two and chapter three: the History of the Decision to Open the DoD Networks to Social Media and a Discourse Analysis of Factors that Impacted the Social Media Decision. This section will synthesize the empirical findings to answer the study's two research questions.

The first question was how have the initial and post-policy debates on social media and the military been shaped by competing discourses of security and privacy risk, sociotechnological inevitability, responsible online behavior and youth? Uniformed senior leaders previously believed the security and privacy risks of social media were so high, that social media should be banned on DoD networks. Initially, the generals in the Tank were successful in banning the use of social media from military networks. There was also a conflict between risk and a service member's desire to contact his or her family and friends. While service members admitted there

were risks involved with using social media, they believed if a person received proper training and exerted self-control, the risks were sufficiently mitigated. Additionally, if a service member did something to put the network at risk, DoD has existing procedures to punish that one service member, not restrict social media for all service members. This discourse influenced the overturn of the social media policy to be more permissive because there was an existing belief in the disciplined nature of service members that made the argument for relying on individual discretion acceptable.

DoD's desire to be technically superior to a potential enemy feeds the sociotechnological inevitability discourse. People expressed fear at being left behind with social media. There was an assumption by DoD leaders and service members that having better technology leads to U.S. victory. However, the Taliban in Afghanistan have inferior communications and weapons technology and after ten plus years at war, are still a viable enemy. Even though there is a current case that disproves sociotechnological inevitability, the DoD continues to strive for technological superiority. It is because of this superiority debate that DARPA has an entire division devoted to social media capability research and development.

The discourse on responsible online behavior show there is evident tension between the stated norms and actual behavior. There is great pressure on service members by the DoD institution and DoD senior leaders to always conduct themselves responsibly. Service members said they took the Code of Conduct seriously, yet many indicated to me that they broke the rules by using social media when it was not authorized or posted something questionable on a social media site. This gap in responsible online behavior is addressed by the emergent discourse of leadership. Leaders monitor service members' actions and address the behavior they deem as irresponsible. The DoD policy and methods to deal with irresponsible behavior already exist as evidenced by

the most recent (2012) version of the social media policy, which is less specific on restrictions and consequences than the original policy was in 2010.

On the other hand, my analysis shows that officers' fears about irresponsible behavior did not always reflect reality. Senior leaders were exceptionally concerned with casualty notification being release on social media before the next-of-kin were properly notified. In reality, these incidents were few and far between. Youth were often blamed for being irresponsible, even though there was no empirical evidence to confirm this as a fact. This discourse of sweeping generalization of youth's irresponsibility definitely impacted the initial policy restricting the use of social media on military networks. DoD policy would be more beneficial if it were based on facts and empirical evidence, not on the whims and guesswork of those in the position to implement change.

Youth are often credited as the reason the social media policy flipped from a restrictive to a permissive policy. There was a general feeling that youth uses social media to communicate and therefore DoD, which recruits from a young demographic, needs to embrace it. The resistance to youth's use of social media for fear they will be irresponsible with it was overcome by the hope and expectation that youth will discover new and innovative ways to utilize social media within DoD.

The second question was what are the relationships among the discourses and how do they affect views of policy? These four discourses often overlapped, portraying the instability of the arguments against social media on DoD networks. The discourses of security and privacy risk were often stated as a concern and a reason for banning social media from military networks, by the service providers, many of them general officers. As the combination of the discourses of youth and their ability to be responsible online grew stronger, the argument for security and

privacy risk diminished in value. The sociotechnological inevitability discourse seemed to foreclose the debate before it concluded. The risk discourse weakened further when the emphasis shifted from security concerns to people slacking off at work and high bandwidth utilization, both of which can be mitigated without eliminating social media. A leadership discourse emerged with a very strong statement about the culture of the U.S. military. Service members believe good leaders make a restrictive social media policy unnecessary. They state there are already standards for responsible behavior and if a service member violates the code of conduct, leaders will take appropriate action. There is a common theme amongst young service members and seasoned veterans that there is no need to punish the masses for the actions of a few individuals.

The current social media policy signed September 11, 2012 seems to be at closure. This study supports the decision that was made to open the DoD networks to social media. By exploring the discourse of security and privacy risk, sociotechnological inevitability, responsible online behavior, and youth, I found the fear that social media use is dangerous to the military was visceral rather than rational. People constructed scenarios that were not supported by empirical evidence as reasons to ban social media on DoD networks. If the social media policy is once again revisited in DoD, researchers should start with these four discourses and also examine the leadership discourse to inform their study as they have proved to be the most influential on the current policy.

The scale of the social media debate is extensive and contains many more opinions than facts. There is no use in revisiting if social media should be used by the DoD or not. To really determine if social media is a useful DoD tool, a study on how DoD is using social media post-

policy should be conducted. This study should look at what units in DoD are using social media and how they are using it. Innovative uses of social media should be shared Department-wide.

To address the strong fears of security and privacy risk that general officers have, a study could be conducted at the classified level on negative incidents involving social media. It would be useful to examine these incidents to see if there are any particular trends or truth behind senior leader distrust of service members' use of social media. Since my dissertation was conducted entirely at the unclassified level, there is a possibility of further evidence existing to support the fear of security and privacy risk. A classified study would be an excellent way to explore this further.

The discourse on social media and the military, particularly that of security and privacy risk, sociotechnological inevitability, responsible online behavior, and youth was significant to the decision to open the DoD networks to social media. Despite the initial fear of risk or irresponsible posting by service members, the use of social media is thriving within DoD under the current policy. Social media is positioned properly today within the DoD if it is chosen to evolve into the powerful platform it have the potential to be. Senior leaders have sufficiently embraced social media and overcome the negative discourse to allow this to happen.

APPENDIX A

Service Member Interview Questions

Do you use social media?

Do you think the military should use social media? If yes, for what purpose?

Did your present or last unit use social media and how did they use it?

Do you think training can overcome your concerns of using a social media site?

The military tried to develop military-only social media sites and most failed. Have you ever used "trooptube" or a similar site? Would you use a social media site that was only open to members of the military?

Do you think social media has changed peoples' behaviors?

Do you know what the DoD policy is on social media? If so, do you think it is adequate?

Risk (Security, Privacy)

Do you have confidentiality concerns relating to service members use of social media?

How secure do you believe your online data is? Who do you think has access to your data?

Are you concerned with the amount of data social media sites retain and access about you?

What do social media companies say about privacy? Is privacy defined well/properly by those companies? Have you ever read the web 2.0 companies' privacy statements?

Is it possible to keep anything on the net private?

Do you use third party applications associated with your social media site?

Are you aware of any incidents where a social media post threatened the security of a service member or unit? If so tell me about it.

Youth

Do you think age makes a difference in how people use social media?

Do you think people in some age groups are more responsible in the use of social media than others?

Are some age groups better than others about controlling the content they post on social media?

Responsible Online Behavior

What guides a service member's (or your) actions on social media?

Should your use of social media use be monitored by your supervisor? Should you monitor the social media activities of your subordinates?

What makes a service member post or not post inappropriate content?

Can you give me examples?

Technological Inevitability

Is the current DoD social media policy reversible?

Do you think DoD would again ban use of social media?

APPENDIX B

Policy Maker Interview Questions

What was your position at the time the social media decision was made in 2010?

Who were the other stakeholders in the decision and how much interaction did you have with them?

Tell me about the last few weeks before the policy was signed?

Who was the most influential stakeholder in the decision?

Were there any words during policy formulation that were widely debated or problematic? What were they and why were they contentious?

Were you for or against opening the DoD networks to social media?

Did you think there was a need for an overarching DoD policy?

Have you changed your views in the few years since the decision was made?

Do you think the current policy is adequate? If not, how would you adjust it?

Are you involved in the current effort to revise the policy? If so, what is your role?

Do you currently use social media?

Do you think youth is irresponsible with social media?

What do you think of service members' current use of social media?

Do you think there is a need for the military to monitor service members' private social media accounts?

Do you think DoD is at risk because of the use of social media? If so, how bad do you think the problem is? If not, why not?

Are there good operational uses for social media?

BIBLIOGRAPHY

Ackerman, Robert and Boland, Rita. "Army Programs Face Daunting Challenges," *Signal*, Nov. 2008. Accessed May 27, 2013 at: http://www.afcea.org/content/?q=node/1754.

American Forces Press Service. "Social Media Sites Provide Morale Boost, Official Says," *Armed Forces Press Service*, Washington, DC, March 17, 2010. Accessed September 12, 2012 at: http://www.defense.gov/news/newsarticle.aspx?id=58357.

Associated Press. "Gen. Dempsey Worries Teens' Social Media Use Could Disqualify Them From Military Service," *CBS News*, Washington, DC, Dec. 4, 2013. Accessed Dec. 26, 2013 at: http://washington.cbslocal.com/2013/12/04/gen-dempsey-worries-teens-social-media-use-could-disqualify-them-from-military-service/.

Baym, Nancy K. *Personal Connections in the Digital Age*. Malden, MA: Polity Press, 2010.

Beck, Ulrich. "On the Logic of Wealth Distribution and Risk Distribution," *Risk Society; Towards a New Modernity*, London: SAGE Publications, 1992.

Bonvanie René. "Social Media In The Office: Two Truths And A Lie," *Forbes*, June 10, 2010. Accessed July 29, 2012 at: http://www.forbes.com/sites/ciocentral/2012/06/10/social-media-in-the-office-two-truths-and-a-lie/.

Bronk, Chris. "Marines' Social-Media Ban is Bad for Morale," *Federal Computer Week*, Sept. 17, 2009. Accessed Dec 31, 2012 at: http://fcw.com/Articles/2009/09/21/COMMENT-Chris-Bronk-Marine-ban.aspx?p=1.

Burns, Robert. "William J. Lynn, Deputy Defense Secretary, Will Resign: Top Pentagon Official Plans to Quit by Early Fall," *Huffington Post*, July 7, 2011. Accessed May 27, 2013 at: http://www.huffingtonpost.com/2011/07/07/william-lynn-resign-pentagon_n_892347.html.

Callon, Michel. "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fisherman of St. Brieuc Bay, in J. Law, *Power, Action, and Belief: A New Sociology of Knowledge?* London, Routledge, 1986.

Carden, Michael J. "Cyber Task Force Passes Mission to Cyber Command," *American Forces Press Service*, Sept 7, 2010. Accessed Apr 22, 2013 at: http://ctovision.com/2010/09/jtf-cnd-to-jtf-cno-to-jtf-gno-to-cybercom/.

Chairman of the Joint Chiefs of Staff Instruction, "Joint Capabilities Integration and Development System," CJCSI 3170.01H, Washington, DC, 10 Jan 2012.

Chairman of the Joint Chiefs of Staff Instruction, "Meetings in the JCS Conference Room," CJCSI 5002.01, Washington, DC, 13 Dec 2010.

Chairman of the Joint Chiefs of Staff Memorandum, "Distribution of the Unified Command Plan 2008 (UCP 08)," Washington, DC, Dec. 23, 2008.

Chalmers, Mike. "Social Media Allow Military Families a Deeper Connection," *USA Today*, November 24, 2011. Accessed July 12, 2012 at: http://usatoday30.usatoday.com/news/military/story/2011-11-28/military-deployment-social-media/51349158/1.

Chen, Lisa, Dover, Mike and Geraci, John. *The Generation Gap: Youth as Recognized Authorities*, New Paradigm Learning Corporation, 2006, quoted in Federal CIO Council. *Net Generation: Preparing for Change*.

Chen, Lisa and DaSilva, Ian. *Architecting the Future: Net Gen Career and Talent Management Processes*, Ngera Corp: 2008 quoted in Federal CIO Council. *Net Generation: Preparing for Change*.

Cobain, Ian and Fielding, Nick. "Revealed: U.S. Spy Operation That Manipulated Social Media," *The Guardian*, United Kingdom, March 17, 2011. Accessed on Sept 28, 2011 at: http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks.

Collins, Harry M. *Changing Order*, Chicago, IL: University of Chicago Press, 1992

Cornish, Audie (Host). "All Things Considered," *National Public Radio* Interview, May 21, 2012. Accessed Jul 12, 2012 at: http://www.npr.org/templates/transcript/transcript.php?storyId=153003267.

Cramer, Theresa. "A Case of the Social Military," *www.econtentmag.com* (Apr 2010). Accessed Mar 3, 2011 at: http://www.econtentmag.com/Articles/Editorial/Case-Studies/A-Case-of-the-Social-Military-with-Jive-Clearspace-66002.htm.

DARPA Information Innovation Office. Washington, DC. Accessed Jan 9, 2014 at: http://www.darpa.mil/Our_Work/I2O/Programs/Social_Media_in_Strategic_Communication (SMISC).aspx.

Defense Manpower Data Center. *2011 Demographic Profile of the Military Community*, Washington, DC: Department of Defense, September 2012. Accessed Dec 8, 2013 at: http://www.militaryonesource.mil/12038/.../2011_Demographics_Report.pdf.

Defense News. "Interview with Al Shaffer; Acting U.S. Assistant Secretary of Defense for Research and Engineering," *Defense News Online*, Oct 23, 2013. Accessed Nov 11, 2013 at: http://www.defensenews.com/article/20131023/DEFREG02/310230012.

Department of Defense. *Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)/DoD CIO),* DoD Directive number 5144.1, Washington, DC, May 2, 2005. Accessed Apr 25, 2013 at: http://dodcio.defense.gov/.

Department of Defense. "Department of Defense Personnel Access to the Internet," *Report to Congress* in response to request on page 323 of Senate Armed Services Committee Report Number 110-77, Sept 2007.

Department of Defense. *Dictionary of Military and Associated Terms*, Washington, DC: Chairman of the Joint Chiefs of Staff, Nov 8, 2010 (as amended Feb 14, 2014). Accessed Mar 8, 2014 at: www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Department of Defense Instruction. *DoD Internet Services and Internet-Based Capabilities*, Number 8550.01, DoD Chief Information Officer, September 11, 2012.

Department of Defense Instruction. *DoD Directives Program*, Number 5025.01, Director of Administration and Management, August 30, 2013. Accessed Mar 8, 2014 at: http://www.dtic.mil/whs/directives/corres/pdf/502501.p.pdf.

Department of Defense Instruction. *DoD Personnel Casualty Matters, Policies, and Procedures*, Number 1300.18, Undersecretary of Defense (Personnel and Readiness), August 14, 2009. Accessed: July 15, 2014 at: http://www.dtic.mil/whs/directives/corres/pdf/130018p.pdf.

Department of Defense. *Joint Ethics Regulation*, Washington, DC: Office of the Secretary of Defense General Counsel, Aug, 1993. Accessed Nov 11, 2013 at: http://www.dod.mil/dodgc/defense_ethics/.

Department of Defense. *Joint Operation Planning*, Washington, DC: Chairman of the Joint Chiefs of Staff, Aug 11, 2011. Accessed Nov 10, 2013 at: https://jdeis.js.mil.

Department of Defense. *Standards of Conduct*, DoD Directive 5500.07, Washington, DC: Office of the Secretary of Defense General Counsel, Nov 29, 2007. Accessed Nov 11, 2013 at: http://www.dod.mil/dodgc/defense_ethics/.

Department of Defense. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Washington, DC: Office of the Secretary of Defense, Jan 2012. Accessed Nov 11, 2013 at: http://www.acq.osd.mil/chieftechnologist/areas/guidance.html.

Department of Defense. "The Use of Web 2.0 in the Department of Defense," *DoD CIO and Joint Staff J6*, Washington, DC, July 2009. Accessed Jan 9, 2014 at: http://www.au.af.mil/au/awc/awcgate/dod/use-of-web20-in-dod.pdf.

Department of the Navy. "A Conversation with David M. Wennergren, DoD Assistant Deputy Chief Management Officer, *CHIPS Magazine*, Jan-Mar 2011. Accessed May 27, 2013 at: http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=2308.

Department of the Navy. *Web 2.0-Utilizing New Web Tools*. Chief Information Officer, United States Navy. Washington, DC, October 20, 2008.

Deputy Secretary of Defense. *Directive Type Memorandum 09-026 – Responsible and Effective Use of Internet-based Capabilities*, Department of Defense, Washington, DC: Office of the Deputy Secretary of Defense, February 25, 2010.

Edwards, Paul N. *The Closed World: Computers and the Politics of Discourse in Cold War America.* Cambridge, MA: MIT Press, 1997.

Ellison, Nicole and Boyd, Danah. "Sociology Through Social Networking Sites," in Dutton, W.H., *The Oxford Handbook of Internet Studies*, Oxford: the Oxford University Press, pp. 151-172. Accessed Mar 8, 2014 at: www.danah.org/papers/2013/SocialityThruSNS-preprint.pdf.

Federal Chief Information Officer Council. *Net Generation: Preparing for Change in the Federal Information Technology Workforce.* Washington, DC: Apr 2010. Accessed Jan 27, 2011 at: http://www.cio.gov/Documents/NetGen.pdf.

Ferran, Lee. "Marine Who Urinated on Taliban Dead Says He'd Do It Again," *ABCNEWS*, July 17, 2013. Accessed Dec 31, 2013 at: http://abcnews.go.com/Blotter/marine-urinated-taliban-dead-hed/story?id=19687916.

Floyd, Price. "In Defense of Social Media," *The Washington Times*, March 21, 2011. Accessed April 22, 2013 at: http://www.washingtontimes.com/news/2011/mar/21/in-defense-of-social-media/.

Frohmann, Bernd. "Discourse Analysis as a Research Method in Library and Information Science." *Library and Information Science Research* 16 (1994): 119-138.

Fulcher, Dr. Eamon. "What is Discourse Analysis?" eamonfulcher.com, 2012. Accessed July 27, 2012 at: http://www.eamonfulcher.com/discourse_analysis.html.

Garamone, Jim. "Lynn Discusses Social Media at Facebook Headquarters," *American Forces Press Service*, Apr. 28, 2010. Accessed Apr 5, 2011 at: http://www.jointbasemdl.af.mil/news/story.asp?id=123202097.

Garamone, Jim. "Dempsey Addresses Issues During Facebook Town Hall," *American Forces Press Service*, Dec. 5, 2013. Accessed, Dec 27, 2013 at: http://www.defense.gov/news/newsarticle.aspx?id=121285.

Garstka, John. "A Conceptual Framework for Innovation in Capability Development." In *Crosscutting Issues in International Transformation, Interactions and Innovations Among People, Organizations, Processes, and Technology*, edited by Derrick Neal, Henrik Friman, Ralph Doughty, and Linton Wells II, 21-54, Washington, DC: National Defense University, Dec 2009.

Gasser, Urs; Cortesi, Sandra; Malik, Momin; and Lee, Ashley. "Youth and Digital Media: From Credibility to Information Quality," *Harvard University*, Berkman Center for Internet and Society, Pub No. 2012-1, Cambridge, MA: Feb 16, 2012. Accessed Dec. 8, 2013 at: http://ssrn.com/abstract=2005272 or http://dx.doi.org/10.2139/ssrn.2005272.

Gentzkow, Matthew and Shapiro, Jesse M. "What Drives Media Slant? Evidence from U.S. Daily Newspapers," *Econometrica*, Vol. 78, No. 1, Jan 2010, pp 35-71. Accessed May 27, 2013 at: http://faculty.chicagobooth.edu/jesse.shapiro/research/biasmeas.pdf.

Gertz, Bill. "Inside the Ring: Taliban Infiltrate Social Media," *Washington Times*, Washington, DC, August 22, 2012. Accessed September 28, 2012 at: http://www.washingtontimes.com/news/2012/aug/22/inside-the-ring-taliban-infiltrate-social-media/?page=all.

Ginsberg, Wendy R. *The Obama Administration's Open Government Initiative: Issues for Congres*s. Washington, DC: Congressional Research Service, August 17, 2010.

Gould, Joe. "Army Expands Warnings on Social Networking," *Army Times*, September 26, 2011. Accessed September 30, 2011 at: http://www.armytimes.com/news/2011/09/army-expands- warnings-on-social-networking-092511w.

Gould, Joe. "Social Media Complicate Army's Death Notifications," *Army Times*, May 6, 2012. Accessed June 2, 2013 at: http://usatoday30.usatoday.com/news/military/story/2012-04-28/social-media-death-notifications/54607350/1.

Harkins, Gina. "Marines Seek Guidance on Social Media After Anti-Obama Posts," *Marine Corps Times*, April 7, 2012.

Hoover, J. Nicholas. "DoD Loosens Social Media Restrictions," *Information Week*, Feb 26, 2010. Accessed Sept 23, 2013 at: http://www.informationweek.com/government/policy/dod-loosens-social-media-restrictions/223100879?cid=RSSfeed_IWK_News.

Hughes, Thomas P. "The Evolution of Large Technological Systems, " in *The Social Construction of Technological Systems*, ed. Weibe E. Bijker, Trevor Pinch, and Thomas P. Hughes. Cambridge, MA: MIT Press, 1987.

Hungerford, Harold; Volk, Trudi L; and Ramsey, John. "Instructional Impact of Environmental Education on Citizenship Behavior and Academic Achievement," Paper presented at the *North American Association for Environmental Education Conference*, South Padre Island, TX, Oct. 21, 2000. Accessed Dec 8, 2013 at: http://www.cisde.org/.../IEEIA%20%2020%20Years%20of%20Researc.pdf.

Kaplan, Stephen. "Human Nature and Environmentally Responsible Behavior," *Journal of Social Issues*, Vol 56, No. 3, 2000, pp. 491-508. Accessed Dec 8, 2013 at: https://www.stanford.edu/.../kaplan_2000_9_selfmotivatedaction_c.pdf

Kruzel, John, J. "Pentagon Weighs Social Networking Benefits, Risks," *Armed Forces Press Service*, Washington, DC, August 4, 2009. Accessed September 12, 2012 at: http://www.defense.gov/news/newsarticle.aspx?id=55363.

Kruzel, John J. "Officials Look to Solve Social Network Risks Without Ban," *American Forces Press Service*, Washington, DC, August 6, 2009. Accessed June 3, 2013 at: http://www.defense.gov/news/newsarticle.aspx?id=55399.

Lubold, Gordon. "Marines Retreat from Facebook, Will Pentagon Follow?" *Christian Science Monitor*, Boston, MA, August 5, 2009.

Lubold, Gordon. "Military Brass Joins Wired Troops." *Christian Science Monitor*, Boston, MA, January 21, 2009. Accessed April 26, 2013 at: http://www.highbeam.com/doc/1G1-192364675.html.

Lundquist, Edward. "Crisis Tool: Social Media Can Provide Situational Awareness During Disasters…In 140 Characters or Less," *Sea Power*, February 2011, pp. 10-14.

Lynn, William J. "Defending a New Domain," *Foreign Affairs*, Council on Foreign Relations, September/October 2010.

Marshall, Cory. "Intel Training: 90YS Goes Inside Ft. Huachuca's Military Intelligence Training, *KGUN9 News*, Ft. Huachuca, AZ, Nov. 8, 2013. Accessed Dec 27, 2013 at: http://www.jrn.com/kgun9/news/Ft-Huachuca-intelligence-training-231203341.html.

Mayfield, Thomas D. III. "A Commander's Strategy for Social Media," *Joint Forces Quarterly*, Issue 60, 1st Quarter, 2011. Accessed April 26, 2013 at: http://www.ndu.edu/press/commanders-strategy-social-media.html.

McCaney, Kevin. "Pentagon to Update Rules for Using Commercial Social Media Sites," *Government Computer News*, May 29, 2012. Accessed Jan 9, 2014 at: http://gcn.com/Articles/2012/05/29/DOD-social-media-policy-no-dot-mil.aspx?Page=1

Miles, Donna. "Gates, Mullen: Communications Technologies 'Strategic Asset' for United States," *American Forces Press Service*, Washington, DC, June 18, 2009. Accessed: June 3, 2013 at: http://www.defense.gov/news/newsarticle.aspx?id=54834.

Miles, Donna. "New Policy Authorizes Social Media Use With Caveats," *American Forces Press Service*, Washington, DC, Feb 26, 2010. Accessed April 25, 2013 at: http://www.defense.gov/news/newsarticle.aspx?id=58117.

Miles, Donna, "New Public Affairs Chief Sets Out to Transform Communications Processes," *American Forces Press Service*, Washington, DC, June 15, 2009. Accessed June 2, 2013 at: http://www.defense.gov/news/newsarticle.aspx?id=54779.

Mueller, Milton. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010.

Nolan, Steve. "U.S. employees set to be forced to give bosses their Facebook PASSWORDS," *Daily Mail Online*, United Kingdom, April 23, 2013. Accessed April 26, 2013 at: http://www.dailymail.co.uk/news/article-2313367/CISPA-Amendment-US-cyber-attack-law-banning-employers-asking-Facebook-passwords-blocked.html.

O'Keefe, Ed. "Transcript: Interview with 'Don't Ask Don't Tell' Report Co-authors." *Washington Post online*, December 20, 2011. Accessed June 30, 2012 at: http://voices.washingtonpost.com/federal-eye/2010/12/transcript_interview_with_dont.html

Perry, Chondra. "Social Media and the Army," *Military Review* 90 (Mar-Apr 2010).

Pinch, Trevor J. and Bijker, Wiebe. "The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other," in *The Social Construction of Technological Systems*, ed. Weibe E. Bijker, Trevor Pinch, and Thomas P. Hughes. Cambridge, MA: MIT Press, 1987.

Price, Floyd. "In Defense of Social Media; How Public and Private Sectors of DoD Opened Doors to the Network," *The Washington Times*, March 22, 2011. Accessed March 22, 2011 at: http://www.lexisnexis.com/lnacui2api/delivery/PrintDoc.do?jobHandle=1843%3A275766.

Potter, Jonathan. *Representing Reality: Discourse, Rhetoric and Social Construction*, Thousand Oaks, CA: SAGE Publications, 1996.

Qiu, Jack Linchuan. *Working-Class Network Society: Communication Technology and the Information Have-Less in Urban China*. Cambridge, MA: MIT Press, 2009.

Reilly, Corinne. "Captain Who Made Racy Videos to Retire From the Navy," *Virginia Pilot*, January 28, 2012. Accessed April 27, 2013 at: http://hamptonroads.com/2012/01/captain-who-made-racy-videos-retire-navy.

Rodewig, Cheryl. "Geotagging Poses Security Risks," *US Army*, Ft Benning, GA, March 7, 2012. Accessed April 26, 2013 at http://www.army.mil/article/75165/.

Rodewig, Cheryl. "Social Media Misuse Punishable Under UCMJ," *U.S. Army*, Ft Benning, GA, Feb 9, 2012. Accessed June 12, 2012 at: http://www.army.mil/article/73367/.

Sargent, John F., Jr. "Federal Research and Development Funding," *Congressional Research Service*, Washington, DC, Dec. 5, 2013. Accessed Jan 17 at: https://www.fas.org/sgp/crs/misc/R42410.pdf.

Senate Armed Services Committee. "National Defense Authorization Act for Fiscal Year 2008," U.S. Government Printing Office, Washington, DC, June 5, 2007. Accessed Sept 24, 2013 at: http://www.gpo.gov/fdsys/pkg/CRPT-110srpt77/html/CRPT-110srpt77.htm.

Shapin, Steven and Schaffer, Simon. Leviathan and the Air Pump: Hobbes, Boyle and the Experimental Life. Princeton, NJ: Princeton University Press, 1985.

Shirky, Clay. *Here Comes Everybody*. New York: The Penguin Press, 2008.

Stewart, Joshua. "Limited Online Access Stresses Sailors at Sea," *Navy Times*, April 15, 2012.

Takai, Teresa M. "Improving Management and Acquisition of Information Technology Systems in the Department of Defense," *Statement for the Record, House Armed Services Committee on Emerging Threats and Capabilities*, Washington, DC, April 6, 2011.

Talja, Sanna. "Analyzing Qualitative Interview Data: The Discourse Analytic Method," University of Tampere, Finland.

Tapscott, Don and Gilles, Bill. The 8 N-Gen Norms: Characteristics of a Generation, p. 13, quoted in Federal CIO Council. *Net Generation: Preparing for Change.*

Techweb. "Air Force Seeks Fake Online Social Media Identities," *TECHWEB*, Feb 22, 2011. Accessed March 22, 2011 at: http://www.lexisnexis.com/lnacui2api/delivery/PrintDoc.do?jobHandle=2861%3A275767.

Threat Center Live Blog. "Foxsports.com Used to Serve Malware," October, 2, 2009. Accessed April 24, 2013 at: http://threatcenter.blogspot.com/2009/10/foxsportscom-used-to-serve-malware.html.

Trainor, Bernard E. "Washington Talk: Joint Chiefs of Staff; Inside the 'Tank': Bowls of Candy and Big Brass," *New York Times*, Jan 11, 1988. Accessed April 1, 2013 at: http:www.nytimes.com/1988/01/11/us/Washington-talk-joint-chiefs-staff-inside-tank-bowls-candy-big-brass.html.

United States Air Force Public Affairs Agency. *Social Media and the Air Force*, Washington, DC, November, 2009. Accessed February 5, 2014 at: https://www.24af.af.mil/.../media/.../AFD-091210-043.

United States Army. "Public Announcement on the Army's Guidance on Accessing Social Networking Sites (SNS)," *ALARACT 228/2009*, Washington, DC, August 14, 2009. Accessed February 5, 2014 at: http://www.ajrotc.us/website_datacall/ALARACT_228_2009_army guidance_social_networking_sites_14aug09%255B1%255D.pdf+&cd=4&hl=en&ct= clnk&gl=us.

United States Marine Corps. "Immediate Ban of Internet Social Networking Sites (SNS) on Marine Corps Enterprise Network (MCEN) NIPRNET," *MARADMIN 0458/09*, Washington, DC, August 3, 2009. Accessed Apr 7, 2013 at: http://www.marines.mil/News/Messages/MessagesDisplay/tabid/13286/Article/ 112458/immediate-ban-of-internet-social-networking-sites-sns-on-marine-corps-enterpris.aspx.

United States Office of Personnel Management. *Sizing Up the Executive Branch of the Federal Government: Fiscal Year 2012*, Washington, DC: Jan 2013.

Wells, Linton II and Drapeau, Mark. *Social Software and National Security, An Initial Net Assessment*, Washington, DC: National Defense University, April 2009.

Westlake, E.J. "Friend Me If You Facebook; Generation Y and Performative Surveillance," *The Drama Review*, Volume 52, No. 4(T 200) Winter 2008, pp 21-40. Accessed March 22, 2011 at http://muse.jhu.edu/journals/tdr/summary/v052/52.4.westlake.html.

The White House. "Transparency and Open Government." *Memorandum from President Barack Obama*. Jan. 21, 2010. Accessed Dec. 7, 2010 at: http://www.whitehouse.gov/ the_press_office/Transparency_and_Open_Government/.

The White House. "Remarks By the President on Securing Our Nation's Cyber Infrastructure," *Office of the Press Security*, May 29, 2009. Accessed: Sept 15, 2010 at: http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

Winner, Langdon. "Social Constructivism, Opening the Black Box and Finding It Empty," Conference Proceedings, *Biennial Conference of the Society for Philosophy and Technology*, Mayaguez, Puerto Rico, March 1991.