PENETRATE, EXPLOIT, DISRUPT, DESTROY: THE RISE OF COMPUTER NETWORK OPERATIONS AS A MAJOR MILITARY INNOVATION

by

Craig J. Wiener
A Dissertation Submitted to the Graduate Faculty of George Mason University in Partial Fulfillment of The Requirements for the Degree of Doctor of Philosophy in Biodefense

Committee:

_______________________________________  Gregory Koblentz, Chair
_______________________________________  A. Trevor Thrall
_______________________________________  Stuart Malawer
_______________________________________  Gregory Koblentz, Program Director
_______________________________________  Mark J. Rozell, Dean

Date:  ____________________________________  Fall Semester 2016
George Mason University
Fairfax, VA
Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at George Mason University

By

Craig J. Wiener
Master of Science
George Mason University, 2010
Bachelor of Arts
New York University 1992

Director: Gregory Koblentz, Associate Professor
Schar School of Policy and Government

Fall Semester 2016
George Mason University
Fairfax, VA
Copyright 2016 Craig J. Wiener
All Rights Reserved
DISCLAIMER

Any errors herein are solely those of the author. Additionally, the views expressed herein are those of the author.
DEDICATION

To Betty: I wish you were here.
ACKNOWLEDGEMENTS

I have a tremendous number of people to thank who have helped me throughout my Master of Science and PhD studies, leading to the submission of my dissertation. It literally took a village, and although I cannot thank everyone here, please know the depth of my gratitude is significant and ongoing.

I would like to thank the faculty and staff of the George Mason School of Policy, Government and International Affairs, and the Graduate School of Public and International Affairs for giving me an opportunity to pursue my studies in national security. Specifically, I would like to thank Dr. Rueben Brigarty, the former Director of the Biodefense Department at GMU, who made the decision to allow me into the program after a thirteen-year absence from academia, and who valued the single-minded drive I had to pursue an MS and a PhD. I would like to also thank Dr. Robert Baker for providing me a top-notch education in pathogenic bacteriology, virology and toxicology that forms the foundation of my technical biological weapons knowledge and my friends Mr. Larry Small, Mr. Matthew Moakler and Dr. Jeffrey Curry for encouraging me to pursue my dreams of assisting with US national security.

I would like to thank Dr. Gregory (the beatings will continue until morale improves) Koblentz, my academic advisor and the chair of my dissertation committee, for the entirety of my education at George Mason. Similarly, I would also like to vigorously thank my other committee members Dr. Trevor Thrall, Dr. Stuart Malawer, Mr. Robert L. Dietz, Dr. Allison MacFarlane and my friend and colleague Dr. Daniel Gerstein.

I would like to especially thank my unfailing mentor, General Michael V. Hayden. Over five-plus years, I’ve had the distinct honor of studying under General Hayden as his graduate teaching assistant and, as warranted, class lecturer. Without the General, the fantastic Sandy Stanar Johnson and the invaluable Mr. William Marshall, this dissertation topic could never have been successfully addressed. Furthermore, I would like to thank the Prepublication Review Board and historians at National Security Agency, Central Intelligence Agency and my colleagues at the Department of Energy and National Nuclear Security Administration.

The following individuals turned this journey into a joy, and an invaluable set of senior national security leadership lessons in what it means to serve our nation: General Kenneth Minihan, Mr. Bill Black, Mr. James Gosler, Admiral William O. Studeman, Mr. Glenn Gaffney, Admiral Michael McConnell, Ambassador Linton Brooks, Mr. Chris Inglis, Mr. Rich Haver, the former high-ranking DoD official who still serves his country, the DoD historian, Dr. George Duchak and Mrs. Linda Millis.

Special thanks go to Mr. Charles Durant, Mr. Jon King, Mr. Shawn Sullivan, Mr. Frank Lowery and Mr. Roger Lewis for their support of my efforts on an ongoing basis. I
am indebted to Dr. Michael Warner from the Department of Defense, Mr. Bob Blunden, and Major General Keffer from US Cyber Command for all their help and facilitation, and to my friends Dr. Christopher Ford and Mr. Jamil Jaffer for talking through various aspects of the case study with me over time. Mr. Pat Bomgartner and his entire team were incredibly helpful, and kind beyond words. Thank you!

I appreciate the permission granted by Peter Collins of Internet Live Stats to use a screenshot of one of their graphics.

I would also like to thank the Center for Strategic and International Studies for my time as a Nuclear Scholar in the Project on Nuclear Issues and the members of the Intelligence and National Security Alliance (INSA) for naming me the Sidney Drell Academic Award winner as I strove to complete my doctorate while working my way through school.

My thoughts are with my grandfather Paul Wiener and my uncle Jerome Feldman, and all the members of my family over the last four generations who have served in the US armed forces, not all of whom came home.

I would like to thank my father and mother for teaching me well, encouraging me and ensuring I had all the books I could possibly read when I was a child.

To my wife Rachel, who stands beside me, and whose love, kindness, patience and efforts made my dreams a reality: I love you with all my heart, forever and ever.
SIGNIFICANT CONTRIBUTORS IN ORDER OF APPEARANCE

Admiral William O. Studeman has held positions as the Commanding Officer, Navy Operational Intelligence Center, 1982-84; Director, Long-Range Planning Group, and Executive Director of Advanced Technology Panel of the Chief of Naval Operations Executive Board, 1984-85. He served as the Director of Naval Intelligence, 1985-88 prior to becoming Director, National Security Agency, August 1988-April 1992. Admiral Studeman began his tenure as Deputy Director, Central Intelligence Agency (CIA) on 9 April 1992-3 July 1995 and was Acting Director of Central Intelligence, 21 January-5 February 1993 and 11 January-9 May 1995 respectively.

Vice Admiral John (Mike) McConnell has a 40-year career inside the US National Security establishment. A career Naval Intelligence Officer with 29 years of service, Admiral McConnell has served as Director of Intelligence Pacific Fleet and Seventh Fleet, as well as the Intelligence Officer for Chairman of the Joint Chiefs of Staff, General Colin Powell, and Secretary of Defense Dick Cheney during the First Gulf War. From 1992 to 1996 he served as the Director of the National Security Agency (DIRNSA) under Presidents George H. W. Bush and William J. Clinton prior to entering the private sector. Admiral McConnell returned to direct government service as the Director of National Intelligence from 2007-2009 under George W. Bush.

Ambassador Linton F. Brooks served from July 2002 to January 2007 as Administrator of the U.S. Department of Energy’s National Nuclear Security Administration (NNSA), Deputy Administrator for Nuclear Nonproliferation at NNSA, Assistant Director of the United States Arms Control and Disarmament Agency, Chief U.S. Negotiator for the Strategic Arms Reduction Treaty, Director of Defense Programs and Arms Control on the National Security Council staff, and a number of Navy and Defense Department assignments as a 30-year career naval officer. In addition to his government service, Ambassador Brooks spent eight years as Vice President at the Center for Naval Analyses.

William P. (Bill) Marshall has a broad base of expertise in intelligence and cyber-related matters after nearly 35 years of service at the National Security Agency/Central Security Service (NSA/CSS), where he held a variety of senior leadership, management and analysis positions in support of the U.S. Intelligence Community and Department of Defense. Over the decade of 2000-2010, Mr. Marshall provided leadership in cyber operations and related technology development in three key U.S. Government assignments. From 2008 to 2009, Mr. Marshall served as NSA’s Deputy Chief of Staff for Cyber, a position in which he supported the Director, NSA as the agency’s senior
cyber strategist. In this assignment, he played a central role in coordinating agency-wide planning and preparations in support of the Defense Department’s new U.S. Cyber Command. From 2005 to 2008, as the first Director of the NSA Threat Operations Center (NTOC), he led the development of it from start-up to a widely respected center for cyber security operations in the federal government. The NTOC played a vital role in the delivery of time-sensitive intelligence, warning and response to global threats to U.S. Government information networks. From 1998 to 2002, as Director of the Information Operations Technology Center (IOTC), a joint Intelligence Community and Department of Defense Organization, he led a key interagency activity that produced specialized tools, assessments and operating concepts in support of U.S. Government cyber operations. He successfully led efforts to develop assessments and provide recommendations in support of major Intelligence Community policy and capability decisions designed to improve the collection, production and use of signals intelligence.

Richard L. Haver served on active duty in the U.S. Navy from 1967 to 1973. In 1973, Mr. Haver became a civilian intelligence analyst in the Anti-Submarine Warfare Systems branch at the Naval Intelligence Support Center. In 1976, he was selected as a department head at the Navy Field Operational Intelligence Office (NFOIO), and the next year became the Technical Director of the Naval Ocean Surveillance Information Center. He subsequently held the senior civilian position at NFOIO, serving as Technical Director until assuming the position of Special Assistant to the Director of Naval Intelligence in 1981. He was selected as Deputy Director of Naval Intelligence in June 1985, a position he held until 1989. Mr. Haver was selected by Secretary of Defense Dick Cheney in July 1989 to the position of Assistant to the Secretary of Defense for Intelligence Policy. From 1992 to 1995, he served as the Executive Director for Intelligence Community Affairs. In 1998, he assumed the duties of Chief of Staff of the National Intelligence Council and Deputy to the Assistant Director of Central Intelligence for Analysis and Production. In 1999, Mr. Haver joined TRW as Vice President and Director, Intelligence Programs. He led business development and marketing activities in the intelligence market area for their Systems and Information Technology Group. He also served as liaison to the group’s strategic and tactical C3 business units, as well as TRW’s Telecommunications and Space and Electronics groups. Mr. Haver was selected by Vice President Cheney to head the Administration’s Transition Team for Intelligence and then selected by Secretary of Defense Donald Rumsfeld as the Special Assistant to the Secretary of Defense for Intelligence. He returned to the private sector in 2003.

General Kenneth Minihan retired from the U.S. Air Force on June 1, 1999, after more than 33 years of active commissioned service to the nation. On his final tour of duty he served as the 14th Director of the National Security Agency/Central Security Service, a combat support agency of the Department of Defense with military and civilian personnel stationed worldwide. As Director, he was the senior uniformed intelligence officer in the Department of Defense. He has also served as the Director of the Defense Intelligence Agency. He has over 30 years of experience in national, defense and military information services, information technology development and diverse customer support services.
Glenn Gaffney began his career with the CIA in 1986 as a technical analyst in the CIA Directorate of Intelligence (DI) responsible for the analysis of Soviet space systems and space launch vehicles. His experience in this area led to a position as a senior analyst in the former Office of Scientific and Weapons Research where he was increasingly involved in supporting the Directorate of Science and Technology (DS&T) and the Directorate of Operations (DO) in designing and conducting clandestine technical collection operations to address critical technical intelligence gaps. Gaffney led and participated in a number of DI technical research projects focused on developing and evaluating new collection techniques and approaches in support of the DS&T and the National Reconnaissance Office (NRO). In 1996, the DS&T and the DO established the Clandestine Information Technology Office (CITO); the predecessor to today’s Information Operations Center (IOC). Gaffney was part of a team which laid the foundation for this new office and established its targeting program for DO Information Operations. After joining the DS&T in 1997, Gaffney served CITO and IOC as Chief/Targeting and Analysis, Deputy Chief/Programs, Policy and Resources, and then Chief/Computer Operations. He was appointed Deputy Chief/IOC in October 2002 and Chief/IOC in November 2005. Gaffney served as the Deputy Director for Science and Technology in 2007. In January 2008, Gaffney was named as Deputy Director of National Intelligence for Collection. In this role, Gaffney worked on behalf of the Director of National Intelligence to coordinate and integrate the collection efforts of the 16 intelligence agencies and ensured that Intelligence Community priorities were appropriately reflected in future planning and systems acquisition decisions. In December 2009 Gaffney became the Deputy Director for Science and Technology at CIA, where he served until October 2015.

William (Bill) B. Black Jr. joined the National Security Agency in 1959 as an operational linguist/analyst after three years in the Army Security Agency. While employed at NSA, Mr. Black served as the first Chief of the Office of Military Operations, and after National War College he served as the first chief of Operations and later as both Chief and Deputy Chief of this major field service. As he advanced to the Senior Cryptologic Executive Service, his primary accomplishments were in the area of building new organizations and creating new ways of doing business. Mr. Black completed a wide variety of assignments at NSA including Special Assistant for Information Warfare; Chief, NSA/CSS Representative Europe Office (NCEUR); and Associate Deputy Director for Operations/Military Support. Mr. Black retired from NSA in 1997 and entered the private sector, only to return to government service at NSA as Deputy Director in 2000 at the request of Lt. General Michael V. Hayden, DIRNSA. Mr. Black served as NSA Deputy Director until 2006. After completing this assignment, he served as the Special U.S. Liaison Officer (SUSLO) at the U.S. Embassy in England until 2007. The SUSLO officer is responsible to the Director of National Intelligence and the Director of the National Security Agency for representing the U.S. in all cryptographic relationships with UK policy authorities, including the UK’s counterpart organization, the Government Communications Headquarters (GCHQ) at Cheltenham. Mr. Black retired
once again after his return from England, and continues to consult on various public and private advisory boards to this day.

**James (Jim) Gosler** is one of the nation’s foremost experts on cybersecurity and information operations. He joined Sandia National Laboratories in 1979, where his early contributions included establishing a performance modeling/simulation program in the data processing operating systems design area and developing attack methodologies for both cryptographic and nuclear weapon systems in the Adversarial Analysis Group. In 1989, Mr. Gosler was invited by the National Security Agency to serve as Sandia’s first Visiting Scientist. During his two-year assignment, he consulted on computer security concerns and established/chaired key information security research working groups. Upon his return to Sandia, he was named Manager of the Software Adversarial Analysis Department. In 1993, he established and directed the Vulnerability Assessments Program and was named Assistant Director of the Systems Assessment and Research Center. In 1995 Mr. Gosler was named director of the Systems Assessment and Research Center. In 1995 Mr. Gosler was named director of the Clandestine Information Technology Office at the Central Intelligence Agency. He served over three decades in various cyber- and nuclear weapon-related positions at Sandia National Laboratories. In 2004, was appointed Sandia’s sixth fellow.

**General Michael V. Hayden,** USAF, served as the Director, National Security Agency/Chief, Central Security Service (NSA/CSS), Ft. George G. Meade, MD, from March 1999 to April 2005. As the Director of NSA and Chief of CSS, he was responsible for a combat support agency of the Department of Defense with military and civilian personnel stationed worldwide. From April 2005 to May 2006 General Hayden served as the first Principal Deputy Director of National Intelligence. In May of 2006, General Hayden was confirmed as Director, Central Intelligence Agency, and served in this capacity until February 2009. The General has served as Commander of the Air Intelligence Agency and Director of the Joint Command and Control Warfare Center, both headquartered at Kelly Air Force Base, TX. He has also served in senior staff positions in the Pentagon; Headquarters U.S. European Command, Stuttgart, Germany; the National Security Council, Washington, DC; and the U.S. Embassy in the People’s Republic of Bulgaria. Prior to his current assignment, the General served as Deputy Chief of Staff for United Nations Command and U.S. Forces Korea, Yongsan Army Garrison.

**Mr. John C. (Chris) Inglis** served as Deputy Director, National Security Agency from August 2006 to January 2014. As the senior civilian at NSA, he was the Agency’s chief operating officer, guiding and directing strategies and policy, and served as the principal advisor to the Director. Mr. Inglis began his career at NSA as a computer scientist within the National Computer Security Center. His NSA assignments included service across information assurance, policy, time-sensitive operations and signals intelligence organizations. Promoted to NSA’s Senior Executive Service in 1997, he subsequently served in a variety of senior leadership assignments culminating in his selection as the NSA Deputy Director. He has twice served away from NSA Headquarters, first as a
visiting professor of computer science at the U.S. Military Academy (1991-1992) and later as the U.S. Special Liaison to the United Kingdom (2003-2006).
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Tables</td>
</tr>
<tr>
<td>List of Figures</td>
</tr>
<tr>
<td>List of Abbreviations/Acronyms</td>
</tr>
<tr>
<td>Abstract</td>
</tr>
<tr>
<td>Chapter 1. Introduction</td>
</tr>
<tr>
<td>The Research Question: Why and How Did Computer Network Operations (CNO) Emerge as a Major Military Innovation (MMI)?</td>
</tr>
<tr>
<td>Defining MMIs</td>
</tr>
<tr>
<td>Computer Network Operations as a MMI</td>
</tr>
<tr>
<td>Significant in Global Scope and Global Impact</td>
</tr>
<tr>
<td>Technology Change and Systems Development</td>
</tr>
<tr>
<td>Vulnerabilities and Methods to Exploit Them</td>
</tr>
<tr>
<td>Operationally Innovative Use</td>
</tr>
<tr>
<td>Some Examples of Computer Network Operations and the Effects They Can Cause</td>
</tr>
<tr>
<td>Spoofing</td>
</tr>
<tr>
<td>Data Deletion Attacks</td>
</tr>
<tr>
<td>Sabotage or Physically Destructive Capabilities: Examples of Physical Objects Being Destroyed</td>
</tr>
<tr>
<td>Significant Organizational Adaptation</td>
</tr>
<tr>
<td>Conclusion</td>
</tr>
<tr>
<td>Chapter 2. Literature Review of MMI Theories</td>
</tr>
<tr>
<td>Civilian–Military Relations</td>
</tr>
<tr>
<td>Interservice Rivalry</td>
</tr>
<tr>
<td>Intraservice Rivalry</td>
</tr>
<tr>
<td>How Do Major Military Innovations Occur?</td>
</tr>
<tr>
<td>Evangelista Model of US Technological Innovation</td>
</tr>
<tr>
<td>Christensen Model of Managing Disruptive Innovation</td>
</tr>
<tr>
<td>Summary of MMI Literature</td>
</tr>
<tr>
<td>Gaps in Main MMI Theories</td>
</tr>
<tr>
<td>Hypotheses</td>
</tr>
<tr>
<td>Civilian–Military Relations Theory as an Explanation for Why CNO Developed as a Major Military Innovation</td>
</tr>
<tr>
<td>Interservice Rivalry Theory as an Explanation for Why CNO Developed as a Major Military Innovation</td>
</tr>
<tr>
<td>Intraservice Rivalry Theory as an Explanation for Why CNO Developed as a Major Military Innovation</td>
</tr>
</tbody>
</table>
The Christensen Model for Creating and Managing Disruptive Technological Innovation as an Explanation for How CNO Developed as a Major Military Innovation ................................................................. 70
Research Design .................................................................................................................. 70
Case Method Selection ........................................................................................................ 70
Method of Analysis .............................................................................................................. 72
CNO Case Study .................................................................................................................. 77
Roadmap for the Rest of the Dissertation ........................................................................... 78
Chapter 3. Prehistory and 1982-1989 .................................................................................. 80
Prehistory ............................................................................................................................... 80
Identification of System Vulnerabilities: 1965 Onward ................................................... 82
A New Type of Special Means in Warfare: 1982-1989 ...................................................... 85
The Joint Strategic Studies Ground (JSSG) and Special Technical Operations (STOs): 1982-1989 ............................................................... 93
CNO MMI Analysis of 1982-1989 ...................................................................................... 105
Civilian–Military Relations Theory 1982-1989 ............................................................... 105
Interservice Rivalry Theory 1982-1989 ........................................................................... 112
Intraservice Rivalry Theory 1982-1989 ........................................................................... 116
Chapter 4. 1992-1996 ......................................................................................................... 121
Introduction ......................................................................................................................... 121
Hackers, Cyber War! and the Digital Explosion: 1995 ...................................................... 142
Minihan Moves Over to Lead NSA: 1996 ........................................................................ 147
NSA and CIA Information Operations Interagency Competition: 1996 ......................... 166
CNO MMI Analysis of 1992-1996 .................................................................................... 170
Interservice Rivalry Theory 1992-1996 ........................................................................... 178
Intraservice Rivalry Theory 1992-1996 ........................................................................... 187
Chapter 5. 1997-2004 ......................................................................................................... 196
Introduction ......................................................................................................................... 196
NSA, CNA Development Authority and the Creation of the Information Operations Technology Center: 1997 ................................................................. 197
ELIGIBLE RECEIVER: 1997 ......................................................................................... 208
Stand-Up of Information Operations Technology Center: 1997 ....................................... 213
SOLAR SUNRISE and MOONLIGHT MAZE ................................................................. 220
NSA and CIA Cooperative Interagency Competition Continues ...................................... 223
Hayden, NSA’s Organizational Transformation and Legitimizing the New Paradigm: 1999-2000 ........................................................................................................... 224
Planning the NSA Transformation .................................................................................... 230
Living on the Net, Industrial Strength Exploitation and Tailored Access ......................... 232
Maturing the IOTC .............................................................................................................. 236
The Sunset of CITO and Stand-Up of the Information Operations Center at CIA: 2000................................................................. 238
Resolving NSA v. CIA Collection Controversy: 2001-2002................................. 240
Transition of IOTC to JFCC-NW and Dual-Hatting the DIRNSA: A Blend of Title 50 and Title 10 Authorities for CNO: 2004-2005................................. 253
CNO MMI Analysis of 1997-2004 .................................................................. 256
Civilian–Military Relations Theory 1997-2004.................................................. 256
Interservice Rivalry Theory 1997-2004............................................................. 265
Intraservice Rivalry Theory 1997-2004............................................................. 275
Chapter 6. 2005-2010.................................................................................. 288
Introduction................................................................................................. 288
Optimizing Cyber Operations at Ft. Meade: 2008............................................ 292
The Creation of US Cyber Command: 2009-2010 .......................................... 294
CNO MMI Analysis of 2005-2010 ................................................................ 297
Civilian–Military Relations Theory 2005-2010................................................ 297
Interservice Rivalry Theory 2005-2010.......................................................... 304
Intraservice Rivalry Theory 2005-2010 .......................................................... 310
Chapter 7. How Major Military Innovations Occur....................................... 317
Chapter 8. Conclusions and Implications .................................................... 328
Introduction................................................................................................. 328
Implications for Future Innovation Efforts ..................................................... 337
The Relationship Between Technology and Doctrine ..................................... 344
Future Research Agenda ............................................................................. 347
Final Thoughts ............................................................................................ 351
Appendix A. The K 7 Organization................................................................. 352
Appendix C. Global Network Infrastructure (GNI).............................................. 369
Appendix D. Sample Information Operations Technology Center (IOTC) Memorandum of Understanding (MOU).................................................. 370
Appendix E. Memorandum of Understanding Between the National Security Agency/Information Assurance Directorate (NSA/IAD) and the Information Operations Technology Center ......................................................... 374
Appendix F. Hayden’s Director’s Message “IOTC Mission Accomplished” ........... 385
Bibliography ............................................................................................... 388
LIST OF TABLES

Table 1. How Major Military Innovations (MMIs) Occur ................................................................. 60
Table 2. Why Major Military Innovations (MMIs) Occur ................................................................. 63
Table 3. Civilian–Military Relations Theory MMI Hypotheses......................................................... 67
Table 4. Interservice Rivalry Theory MMI Hypotheses ................................................................. 68
Table 5. Intraservice Rivalry Theory MMI Hypotheses ................................................................. 69
Table 6. Christensen Model for Creating and Managing Disruptive Innovation MMI Hypotheses ................................................................................................................................. 70
Table 7. Civilian–Military Relations Theory 1982-1989 MMI Hypotheses Analysis .................. 111
Table 8. Interservice Rivalry Theory 1982-1989 MMI Hypotheses Analysis ........................ 115
Table 9. Intraservice Rivalry Theory 1982-1989 MMI Hypotheses Analysis ........................ 119
Table 11. Interservice Rivalry Theory 1992-1996 MMI Hypotheses Analysis ........................ 186
Table 12. Intraservice Rivalry Theory 1992-1996 MMI Hypotheses Analysis ......................... 194
Table 13. Civilian–Military Relations Theory 1997-2004 MMI Hypotheses Analysis ........... 264
Table 14. Interservice Rivalry Theory 1997-2004 MMI Hypotheses Analysis ........................ 274
Table 15. Intraservice Rivalry Theory 1997-2004 MMI Hypotheses Analysis ........................ 286
Table 16. Civilian–Military Relations Theory 2005-2010 MMI Hypotheses Analysis ........... 303
Table 17. Interservice Rivalry Theory 2005-2010 MMI Hypotheses Analysis ........................ 309
Table 18. Intraservice Rivalry Theory 2005-2010 MMI Hypotheses Analysis ........................ 315
Table 19. Model for Creating and Managing Disruptive Innovation ....................................... 327
Table 20. Doctrine Development Over Time ................................................................................. 347
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Internet Users in the World.</td>
<td>8</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Supervisory Control and Data Acquisition (SCADA) System General Layout</td>
<td>29</td>
</tr>
</tbody>
</table>
# LIST OF ABBREVIATIONS/ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFB</td>
<td>Air Force Base</td>
</tr>
<tr>
<td>AFEWC</td>
<td>Air Force Electronic Warfare Center</td>
</tr>
<tr>
<td>AFIC</td>
<td>Air Force Intelligence Command</td>
</tr>
<tr>
<td>AFIWIC</td>
<td>Air Force Intelligence Information Warfare Center</td>
</tr>
<tr>
<td>AGIs</td>
<td>Auxiliary General Intelligence Vessels</td>
</tr>
<tr>
<td>AIA</td>
<td>Air Intelligence Agency</td>
</tr>
<tr>
<td>AIS</td>
<td>Automated Information Systems</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ARFORCYBER</td>
<td>Army Forces Cyber Command</td>
</tr>
<tr>
<td>ARPANET</td>
<td>Advanced Research Projects Agency Network</td>
</tr>
<tr>
<td>ASD</td>
<td>Assistant Secretary of Defense</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Model</td>
</tr>
<tr>
<td>ATP</td>
<td>Advanced Technology Panel</td>
</tr>
<tr>
<td>BASIC</td>
<td>Beginner’s Allpurpose Symbolic Instruction Code</td>
</tr>
<tr>
<td>BDA</td>
<td>Battle Damage Assessment</td>
</tr>
<tr>
<td>BIOSG/BIOWG</td>
<td>Bilateral Information Operations Steering and Working Groups</td>
</tr>
<tr>
<td>BM</td>
<td>Battle Management</td>
</tr>
<tr>
<td>BSI</td>
<td>German Federal Office of Information Security</td>
</tr>
<tr>
<td>C2</td>
<td>Command and Control</td>
</tr>
<tr>
<td>C2W</td>
<td>Command and Control Warfare</td>
</tr>
<tr>
<td>C3CM</td>
<td>Command, Control, Communications and Countermeasures</td>
</tr>
<tr>
<td>C3I</td>
<td>Command, Control, Communications, and Intelligence</td>
</tr>
<tr>
<td>C4</td>
<td>Command, Control, Communications, and Computers</td>
</tr>
<tr>
<td>CASE</td>
<td>Computer Aided Software Engineering technology</td>
</tr>
<tr>
<td>CI</td>
<td>Counter Intelligence</td>
</tr>
<tr>
<td>CIA</td>
<td>Central Intelligence Agency</td>
</tr>
<tr>
<td>CIA/DO</td>
<td>Central Intelligence Agency, Directorate of Operations</td>
</tr>
<tr>
<td>CITO</td>
<td>Clandestine Information Technology Office (at CIA)</td>
</tr>
<tr>
<td>CJCS</td>
<td>Chairman of the Joint Chiefs of Staff (at DoD)</td>
</tr>
<tr>
<td>CNA</td>
<td>Computer Network Attack</td>
</tr>
<tr>
<td>CNA&lt;sub&gt;1&lt;/sub&gt;</td>
<td>Computer Network Attack (Data Destruction)</td>
</tr>
<tr>
<td>CNA&lt;sub&gt;2&lt;/sub&gt;</td>
<td>Computer Network Attack (Physical Destruction by Digital Means)</td>
</tr>
<tr>
<td>CNA-OPE</td>
<td>Computer Network Attack Operational Preparation of the Environment</td>
</tr>
<tr>
<td>CND</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>CNE</td>
<td>Computer Network Exploitation</td>
</tr>
<tr>
<td>CNO</td>
<td>Computer Network Operations</td>
</tr>
<tr>
<td>CO</td>
<td>Central Office Switch</td>
</tr>
<tr>
<td>CO</td>
<td>Cyberspace Operations</td>
</tr>
<tr>
<td>COBOL</td>
<td>Common Business-Oriented Language</td>
</tr>
<tr>
<td>COMC</td>
<td>Combatant Commander</td>
</tr>
<tr>
<td>CONOPS</td>
<td>Concept of Operations</td>
</tr>
<tr>
<td>CONPLAN</td>
<td>Contingent Plan</td>
</tr>
<tr>
<td>COS</td>
<td>Chief of Staff</td>
</tr>
<tr>
<td>CRS</td>
<td>Congressional Research Service</td>
</tr>
<tr>
<td>CVEs</td>
<td>Common Vulnerability and Exposures</td>
</tr>
<tr>
<td>DAR</td>
<td>Data-at-Rest</td>
</tr>
<tr>
<td>DARPA</td>
<td>Defense Advanced Research Projects Agency (at DoD)</td>
</tr>
<tr>
<td>DCI</td>
<td>Director of Central Intelligence</td>
</tr>
<tr>
<td>DDI</td>
<td>Directorate of Digital Innovation (at CIA)</td>
</tr>
<tr>
<td>DEC</td>
<td>Digital Equipment Corporation</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DHS/NPPD</td>
<td>Department of Homeland Security, National Programs and Protection Directorate</td>
</tr>
<tr>
<td>DIA</td>
<td>Defense Intelligence Agency</td>
</tr>
<tr>
<td>DIRNSA</td>
<td>Director of the National Security Agency</td>
</tr>
<tr>
<td>DISA</td>
<td>Defense Information Systems Agency</td>
</tr>
<tr>
<td>DIU</td>
<td>Data-in-Use</td>
</tr>
<tr>
<td>DIT</td>
<td>Data-in-Transit</td>
</tr>
<tr>
<td>DNI</td>
<td>Digital Network Intelligence</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOE</td>
<td>Department of Energy</td>
</tr>
<tr>
<td>DOE/NNSA</td>
<td>Department of Energy, National Nuclear Security Administration</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice</td>
</tr>
<tr>
<td>DOS</td>
<td>Disc Operating System</td>
</tr>
<tr>
<td>DOT&amp;E</td>
<td>Directorate of Operational Testing &amp; Evaluation (at DoD)</td>
</tr>
<tr>
<td>DSB</td>
<td>Defense Science Board</td>
</tr>
<tr>
<td>DS&amp;T</td>
<td>Directorate of Science and Technology (at CIA)</td>
</tr>
<tr>
<td>EA</td>
<td>Electronic Attack</td>
</tr>
<tr>
<td>EA</td>
<td>Executive Assistant/Agent</td>
</tr>
<tr>
<td>ECCM</td>
<td>Electronic Combat Countermeasures</td>
</tr>
<tr>
<td>ECM</td>
<td>Electronic Combat Measures</td>
</tr>
<tr>
<td>ELINT</td>
<td>Electronic Intelligence</td>
</tr>
<tr>
<td>EMCON</td>
<td>Emissions Control</td>
</tr>
<tr>
<td>EMP</td>
<td>Electromagnetic Pulse</td>
</tr>
<tr>
<td>EMS</td>
<td>Electromagnetic Spectrum</td>
</tr>
<tr>
<td>ENIAC</td>
<td>Electronic Numerator, Integrator, Analyzer and Computer</td>
</tr>
<tr>
<td>ESC</td>
<td>Electronic Speed Control</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>ESS</td>
<td>Electronic Switching System</td>
</tr>
<tr>
<td>EW</td>
<td>Electronic Warfare</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FLTCYBERCOM</td>
<td>Fleet Cyber Command (US Navy)</td>
</tr>
<tr>
<td>FOA</td>
<td>Field Operating Agency (at US Air Force)</td>
</tr>
<tr>
<td>FOC</td>
<td>Full Operational Capability</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom of Information Act</td>
</tr>
<tr>
<td>FORTRAN</td>
<td>Formula Translator</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accounting Office</td>
</tr>
<tr>
<td>GCC</td>
<td>Geographic Combatant Commander</td>
</tr>
<tr>
<td>GNI</td>
<td>Global Network Intelligence (at NSA)</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface software</td>
</tr>
<tr>
<td>HPSCI</td>
<td>House Permanent Select Committee on Intelligence</td>
</tr>
<tr>
<td>HSPD</td>
<td>Homeland Security Presidential Directive</td>
</tr>
<tr>
<td>HTTP</td>
<td>HyperText Transfer Protocol</td>
</tr>
<tr>
<td>HUMINT</td>
<td>Human Intelligence</td>
</tr>
<tr>
<td>I2W</td>
<td>Information Infrastructure Warfare</td>
</tr>
<tr>
<td>IA</td>
<td>Information Assurance Division (at NSA)</td>
</tr>
<tr>
<td>IBM</td>
<td>International Business Machines</td>
</tr>
<tr>
<td>IC</td>
<td>U.S. Intelligence Community</td>
</tr>
<tr>
<td>ICBM</td>
<td>Intercontinental Ballistic Missile</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control System</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IE</td>
<td>Internet Explorer</td>
</tr>
<tr>
<td>IJSTO</td>
<td>Integrated Joint Special Technical Operations</td>
</tr>
<tr>
<td>IM</td>
<td>Information Management</td>
</tr>
<tr>
<td>INSCOM</td>
<td>Intelligence and Security Command (US Army)</td>
</tr>
<tr>
<td>INFOSEC</td>
<td>Information Security</td>
</tr>
<tr>
<td>IO</td>
<td>Information Operations</td>
</tr>
<tr>
<td>IOC</td>
<td>Information Operations Center (at CIA)</td>
</tr>
<tr>
<td>IOC</td>
<td>Initial Operational Capability</td>
</tr>
<tr>
<td>IOTC</td>
<td>Information Operations Technology Center (IC/DoD)</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IRBM</td>
<td>Intermediate-Range Nuclear Missiles</td>
</tr>
<tr>
<td>ISR</td>
<td>Intelligence, Surveillance, and Reconnaissance</td>
</tr>
<tr>
<td>IW</td>
<td>Information Warfare</td>
</tr>
<tr>
<td>JAG</td>
<td>Justice Advocate General</td>
</tr>
<tr>
<td>JCS</td>
<td>Joint Chiefs of Staff (at DoD)</td>
</tr>
<tr>
<td>JFC</td>
<td>Joint Functional Command</td>
</tr>
<tr>
<td>JFCC-NW</td>
<td>Joint Functional Component Command – Network Warfare (at NSA)</td>
</tr>
<tr>
<td>JIOWC</td>
<td>Joint Information Operations Warfare Command (at NSA)</td>
</tr>
<tr>
<td>JO</td>
<td>Joint Operations</td>
</tr>
<tr>
<td>JSSG</td>
<td>Joint Strategic Studies Group (between NSA and DoD)</td>
</tr>
</tbody>
</table>
JTF-CND  Joint Task Force – Computer Network Defense (at Space Command)
JTF-CNO  Joint Task Force – Computer Network Operations (at STRATCOM)
JTF-GNO  Joint Task Force – Global Network Operations (at NSA)
JC2WC   Joint Command and Control Warfare Center
LANT    Atlantic Command (at Department of Navy)
MARFORCYBER  Marines Forces Cyber Command
MG      Major General
MILDEC  Military Deception
MISO    Military Information Support Operation
MIT     Massachusetts Institute of Technology
MMI     Major Military Innovation
MOP     Memorandum of Policy
MTSO    Mobile Telephone Switching Office
MULTI-INT Multi-Intelligence discipline
NAIC    National Air and Space Intelligence Center
NASA    National Aeronautics and Space Administration
NAWAR   Navigation Warfare
NCSA    National Center for Supercomputing Applications
NFIP    National Foreign Intelligence Program (at NSA)
NIE     National Intelligence Estimate
NIEX    No-Notice Interagency Exercise
NII     National Information Infrastructure
NIPF    National Intelligence Priorities Framework
NMCC    National Military Command Center
NRO     National Reconnaissance Office
NSA     National Security Agency
NSA/CSS National Security Agency, Central Security Service
NSA/IAD National Security Agency, Information Assurance Directorate
NSA/NCSC National Security Agency, National Computer Security Center
NSA/SID National Security Agency, Signals Intelligence Directorate
NSA/TAO National Security Agency, Tailored Access Operations
NSASAB National Security Agency Scientific Advisory Board
NSC     National Security Council
NSFNET  National Science Foundation Network
NSDD    National Security Decision Directive
NSOC    National SIGINT Operations Center
NORAD   North American Aerospace Defense Command
NSPD    National Security Presidential Directive
NTOC    National Security Agency Threat Operations Center (at NSA/CSS)
NWD     Nuclear Weapon Design
OCR     Optical Character Reader
ODCI    Office of the Director of Central Intelligence
OE      Operating Environment
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPDEC</td>
<td>Operational Deception</td>
</tr>
<tr>
<td>OPE</td>
<td>Operational Preparation of the Environment</td>
</tr>
<tr>
<td>OPLAN</td>
<td>Operations Plan</td>
</tr>
<tr>
<td>OPSEC</td>
<td>Operational Security</td>
</tr>
<tr>
<td>OSD</td>
<td>Office of the Secretary of Defense</td>
</tr>
<tr>
<td>P&amp;E</td>
<td>Processing &amp; Extracting</td>
</tr>
<tr>
<td>PAL</td>
<td>Permission Action Link</td>
</tr>
<tr>
<td>PBX</td>
<td>Private Branch Exchange</td>
</tr>
<tr>
<td>PCs</td>
<td>Personal Computers</td>
</tr>
<tr>
<td>PDAS</td>
<td>Planning and Decision Aid System</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller code</td>
</tr>
<tr>
<td>PM</td>
<td>Perception Management</td>
</tr>
<tr>
<td>PSYOPs</td>
<td>Psychological Operations</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>RATs</td>
<td>Remote Access Trojans</td>
</tr>
<tr>
<td>RAND</td>
<td>Research and Development Corporation</td>
</tr>
<tr>
<td>REC</td>
<td>Radio-Electronic Combat</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RF/VHG</td>
<td>Radio Frequency, Volume Holographic Grating</td>
</tr>
<tr>
<td>RIT</td>
<td>Reconnaissance, Intelligence, and Targeting</td>
</tr>
<tr>
<td>ROMO</td>
<td>Range of Military Operations</td>
</tr>
<tr>
<td>ROW</td>
<td>Rest of World</td>
</tr>
<tr>
<td>RSTA</td>
<td>Reconnaissance, Surveillance, Tracking, and Target Acquisition</td>
</tr>
<tr>
<td>RTRG</td>
<td>Real Time Regional Gateway data processing and data mining system</td>
</tr>
<tr>
<td>SAC</td>
<td>Strategic Air Command (at US Air Force)</td>
</tr>
<tr>
<td>SAIC</td>
<td>Science Applications and International Corporation</td>
</tr>
<tr>
<td>SAPs</td>
<td>Special Access Programs</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCM</td>
<td>Security Countermeasures</td>
</tr>
<tr>
<td>SECDEF</td>
<td>Secretary of Defense</td>
</tr>
<tr>
<td>SES</td>
<td>Senior Executive Service</td>
</tr>
<tr>
<td>SIGINT</td>
<td>Signals Intelligence</td>
</tr>
<tr>
<td>SIO</td>
<td>Special Information Operations</td>
</tr>
<tr>
<td>SISIOP</td>
<td>Single Integrated Operating Plan</td>
</tr>
<tr>
<td>SLBM</td>
<td>Submarine Launched Ballistic Missile</td>
</tr>
<tr>
<td>SOO</td>
<td>Senior Operations Officer</td>
</tr>
<tr>
<td>SOSS</td>
<td>Soviet Ocean Surveillance System</td>
</tr>
<tr>
<td>SSG</td>
<td>Special Studies Group (at Department of Navy)</td>
</tr>
<tr>
<td>SSSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>STOs</td>
<td>Special Technical Operations</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocols</td>
</tr>
<tr>
<td>TDM</td>
<td>Tandem switch</td>
</tr>
<tr>
<td>TOPSECRET/NF</td>
<td>Top Secret/No Foreign Nationals</td>
</tr>
<tr>
<td>TSCM</td>
<td>Technical Security Countermeasures</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TTPs</td>
<td>Tactics, Techniques, and Procedures</td>
</tr>
<tr>
<td>UAV</td>
<td>Unarmed Arial Vehicle</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USA</td>
<td>United States Army</td>
</tr>
<tr>
<td>USACOM</td>
<td>United States Atlantic Command</td>
</tr>
<tr>
<td>USAF</td>
<td>United States Air Force</td>
</tr>
<tr>
<td>(US)AFRICOM</td>
<td>United States Africa Command</td>
</tr>
<tr>
<td>(US)CYBERCOM</td>
<td>United States Cyber Command (at NSA)</td>
</tr>
<tr>
<td>USD(I)</td>
<td>Under Secretary of Defense for Intelligence</td>
</tr>
<tr>
<td>USD(P)</td>
<td>Under Secretary of Defense for Policy</td>
</tr>
<tr>
<td>USG</td>
<td>United States Government</td>
</tr>
<tr>
<td>USN</td>
<td>United States Navy</td>
</tr>
<tr>
<td>(US)PACOM</td>
<td>United States Pacific Command</td>
</tr>
<tr>
<td>(US)SOCOM</td>
<td>United States Special Operations Command</td>
</tr>
<tr>
<td>(US)SPACECOM</td>
<td>United States Space Command</td>
</tr>
<tr>
<td>USSR</td>
<td>Soviet Union</td>
</tr>
<tr>
<td>USSS</td>
<td>United States SIGINT System</td>
</tr>
<tr>
<td>(US)STRATCOM</td>
<td>United States Strategic Command</td>
</tr>
<tr>
<td>(US)TRANSCOM</td>
<td>United States Transportation Command</td>
</tr>
<tr>
<td>VADM</td>
<td>Vice Admiral</td>
</tr>
</tbody>
</table>
ABSTRACT

PENETRATE, EXPLOIT, DISRUPT, DESTROY: THE RISE OF COMPUTER NETWORK OPERATIONS AS A MAJOR MILITARY INNOVATION

Craig J. Wiener, Ph.D.

George Mason University, 2016

Dissertation Director: Dr. Gregory Koblentz

This dissertation assesses that computer network operations are a major military innovation (MMI). It examines the role of the US Intelligence Community in the development of computer network exploitation and attack over four discrete time periods spanning approximately 30 years. The study draws upon a range of theories from the field of security studies and disruptive innovation management and a wealth of newly available information due to recently declassified documents and interviews with elite members of the US Intelligence Community. My analysis yields three major findings while providing key additions to the history of computer network attack developmental activities.

First, the case history and associated analysis proves that the US Intelligence Community produced, for the first time, a weapons system that can be considered a MMI. Since existing theories of major military innovation development fail to account for the role of intelligence in the creation of a MMI, and have never addressed a case where the
Intelligence Community actually created a MMI, this finding is significant. Second, Stephen Rosen’s intraservice rivalry theory of MMI development best explains why Computer Network Operations (CNO) emerged as a MMI. Third, substantial elements of Clayton Christensen’s disruptive innovation management model were found to be an operant factor in how CNO developed as a MMI, a related question not covered in dominant MMI development theory.

Several key, historically important findings resulted from this study. The case history reveals an interesting nexus to nuclear weapons activities as key drivers in the development and early doctrinal use of CNO capabilities as a weapon. The early development of CNO grew out of the US desire to disrupt command and control networks through critical node analysis, as part of the US targeting process for strategic nuclear war. The information network penetration capabilities developed during this era, designed to disrupt or deny communications on early Soviet systems, provided key elements for a proof of concept for Information Warfare, the initial nomenclature used for CNO. Similarly, hypothetical studies related to the introduction of subversions in complex hardware and software systems originated as part of adversarial vulnerability assessments for the US nuclear weapons program, influenced the technical approaches taken by the Central Intelligence Agency’s (CIA) Clandestine Information Technology Office, a precursor organization to CIA’s Information Operations Center and newly formed Directorate of Digital Intelligence. Once a full operational capability was developed during the early to mid-2000s, a certain class of Computer Network Attack (CNA) capabilities falling under the US Strategic Command’s use authorities were
treated as special weapons, with use authority approval granted only by the President of the United States or his designee, the Secretary of Defense, the same national command release authority required for nuclear weapons. Furthermore, recently declassified documents show the National Security Agency (NSA) engaged in computer exploitation as early as 1986. A basket of operations, technology and research organizations evolved and merged over time to create Tailored Access Operations, which was established in 1995 as the K 7 organization. CNA tool development was led by NSA through a quasi-independent organization named the Information Operations Technology Center from 1997 until its reabsorption into NSA in late 2004, where CNA and dual-use Computer Network Exploitation (CNE) capabilities were merged.
CHAPTER 1. INTRODUCTION

The Research Question: Why and How Did Computer Network Operations (CNO) Emerge as a Major Military Innovation (MMI)?

Cyberweapons are becoming a key element of US military technological capability. These technologies, however, were not developed by the uniformed military, the traditional drivers of military innovation. Instead, the Intelligence Community played a crucial role in advocating and developing these technologies and led their assimilation into the tools of statecraft. This case poses a challenge for theories of military innovation that focus exclusively on the role of the military in fostering such innovations.

This dissertation answers the question “Why and how did computer network operations emerge as a major military innovation?” This case study provides a unique opportunity to examine the role intelligence agencies played in the development of a revolutionary military technology. There is no scholarly literature on the Intelligence Community’s role in the creation of a major military innovation (MMI). In fact, this is the first known case of the Intelligence Community creating a MMI. The dissertation tests the leading theories on military innovation, none of which have been previously applied to intelligence agencies, to determine which has the greatest explanatory power. This dissertation also critiques and extends those theories by examining the extent to which they fall short of explaining why and how intelligence organizations play a key role in a weapons innovation process traditionally reserved for military organizations.
Finally, the dissertation offers a combinatorial theory that provides more persuasive explanatory power for the case under examination. Thus, this dissertation helps fill both the empirical and theoretical gaps by exploring a MMI in which intelligence agencies played a significant role.

This study explores the nature and extent of the role the U.S. Intelligence Community (IC) played in the successful creation, adoption, assimilation and utilization of CNO and tests this role against explanations offered in existing mainstream academic theories of military innovation. Based on newly available primary sources, including declassified documents and interviews with current and former U.S. government officials responsible for technical and policy aspects of cyberwarfare, a significant portion of the CNO MMI is due to research, development, testing and operational implementation conducted by the US IC. This process consisted of parallel, intertwined and/or discontinuous development with the Department of Defense (DoD) that has evolved over time.¹ The construction of a multidisciplinary explanation that expands on existing theories will be necessary to encapsulate the success of this MMI, and yield distillable lessons that can serve as a roadmap for future success. The outcome of this research will have direct implications for intelligence and military community planning strategies for rapid identification, maturation and implementation of future innovative technologies. Furthermore, these findings can be used to identify and remove organizational deficits in

¹ The Central Intelligence Agency (CIA) has been involved in significant research and procurement efforts such as reconnaissance satellites, manned aircraft such as the U-2, and unarmed aerial vehicles (UAV), but these are all cases of innovation in surveillance and reconnaissance, not combat platforms (Richard A. Best Jr., Intelligence, Surveillance, and Reconnaissance (ISR) Programs: Issues for Congress, No. CRS-RL32508 (Ft. Belvoir, VA: Defense Acquisition University, David D. Acker Library and Knowledge Repository, 2005).
new programs and/or weapon use policy, extending the utility of the relative power advantage that future MMIs might provide our nation.

**Defining MMIs**

By definition, major military innovations are unprecedented. MMIs exemplify significant changes in the conduct of warfare by leading military organizations. Stephen Rosen, a leading thinker in the field, has defined MMIs as:

A change in one of the primary combat arms of a service in the way it fights or the creation of a new combat arm, or a change in the concepts of operation of that combat arm—[MMIs]…also involves a change in the relation of that combat arm to other combat arms and a downgrading or abandoning of older concepts of operation and possibly of a formerly dominant weapon…. Military innovation may not involve behavioral change but the creation of a new technology (i.e. guided missiles, radar and electronics warfare).

A recent composite definition by Adam Grissom states there are three operant factors in a MMI: changes the manner in which military formations function in the field; innovations are significant in scope and impact (consequential); and innovations are tacitly equated with greater military effectiveness that results in a change in operational praxis that produces a significant increase in military effectiveness as measured by battlefield results. Michael Horowitz, drawing on the work of Rosen and Barry Posen, defines MMIs as “major changes in the conduct of warfare relevant to leading military organizations designed to increase the efficiency with which capabilities are turned to

---


power. They are sometimes, but not always, closely related to changes in technology used by military organizations. 

According to Andrew Krepinevich, major military innovations typically involve four key subelements: technology change, systems development, operational innovation, and organizational adaptation. His more nuanced characterization fully embraces Rosen’s observation that the traditional theoretical perspective is clearly more complicated in the field of military technological innovation, concluding that major military innovations occur when the application of new technologies into a significant number of military systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict.

For the purposes of this study I will use a composite definition of MMIs as defined by Rosen with the subelements provided by Krepinevich and Grissom above. Therefore the definition of a MMI shall be:

The creation of a weapons system whose capabilities are shown to be significant in scope and impact (consequential) as a result of technological change and systems development used in an operationally innovative manner, and which causes organizational adaptation significant enough to change the way one of the primary combat arms of a service conducts its operations or results in the creation of a new combat arm.

---


5 Krepinevich discussed these factors in light of ten military revolutions, but in practice this term describes phenomena that are discussed as MMIs in the broader literature, notably by Rosen and Grissom (Andrew F. Krepinevich, “Cavalry to Computer: The Pattern of Military Revolutions,” *The National Interest* 37 (1994): 30-42).


Computer Network Operations as a MMI

Computer Network Operations (CNO) is an umbrella term that incorporates three main components: Computer Network Defense (CND), Computer Network Exploitation (CNE) and Computer Network Attack (CNA). Computer Network Exploitation (CNE) is defined as enabling operations and intelligence collection to gather data from a target’s or adversary’s automated information systems or networks.8 Computer Network Attack (CNA) is defined as the capability to exploit enemy computer networks through intelligence collection, usually accomplished through use of computer code and computer applications, attack and disrupt enemy computer networks, and/or create physical destruction of equipment of facilities as a result of the use of this capability. An alternate definition for CNAs are actions are taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems and networks themselves.9 There are two subtypes of Computer Network Attack: Computer Network Attack 1 (CNA₁) involves digital actions that have a negative digital effect, such as denial of service, destruction of data, and the like. Computer Network Attack 2 (CNA₂) involves

digital actions that have a negative physical effect, such as destruction of critical infrastructure. Computer Network Defense (CND), which will not be discussed further in this dissertation, is defined as actions taken to protect, monitor, analyze and respond to unauthorized activity within information systems and computer networks.

CNO can also be viewed as more than merely a set of tools, techniques or capabilities. Cyber Kill Chain activities, a combinatorial approach to conducting CNO, applies a formalistic approach to targeting and the application of tactics, techniques and procedures, thus facilitating access to previously denied areas to conduct intelligence and/or military operations. It is the combination of targeting capabilities together with the technology changes in malware, the delivery of malware and effects and outcomes generated from that targeting and delivery that constitute the entirety of the MMI.

Computer Network Operations capabilities meet the seven criteria of major military innovations listed above: they are significant in scope and impact, are the result of technological change and systems development, can be or have been used in an operationally innovative manner, and have caused significant organizational adaptation including changing the way one of the primary combat arms of a service conducts its operations and have resulted in the creation of a new combat arm.

12 There are innumerable variants of malicious code injection, Worms/Trojans, or the use of multifunctional Exploit Kits available today, which are increasingly automated or provide a template step-by-step approach for the attacker. Depending on the kind of target, this activity may include information retrieval, information manipulation, application misuse, information exfiltration, denial or service or the creation of physical damage. This is a consolidation of the LM Cyber Chill Chain and European Union Agency for Network and Information Security Cybersecurity Kill Chain descriptors. See William F. Crowe, “Cybersecurity Kill Chain,” Presentation at the ISACA Jacksonville Chapter Meeting, August 13, 2015.
Significant in Global Scope and Global Impact

Cyberweapons operate in and through the domain known as cyberspace which is global in nature and connected to civilian and military infrastructure in virtually every country in the world.

Cyberspace is “formed by the interconnection of information and data transmission systems supporting critical infrastructure, devices that store, process and transmit data and the use of hardware and software applications and includes data, voice and video ‘at rest’ and ‘in motion.’” Furthermore, cyberspace has evolved as “a domain that enables operations across the domains of air, land, maritime and space; [it] transcends commonly defined organizational and geopolitical borders.”13 In the US, utilization of technological capabilities in the cyber domain are seen as a method to “amplif(y) all instruments of national power. In fact, our ability to maneuver in cyberspace is an emerging instrument of power itself.”14 CNA and its interdependent twin CNE are the combined instruments of a significant capability that can be applied by the military within a new crosscutting domain of operations that is entirely manmade and continues to grow.

Today over 3.28 billion people, which is 40% of the global population, use the Internet, and over 975 million websites can be accessed by these users.\(^\text{15}\) It was estimated that 4.9 billion connected “things” were in use in 2015 and the number could reach 25 billion by 2020.\(^\text{16}\) As a result of this technological adoption, potential targets for exploitation or attack have expanded as well, with the ability to reach anywhere on the globe.

![Internet Users in the World](http://www.internetlivestats.com/internet-users/)


Clearly the United States is not alone in believing cyberspace operations are essential. The world is now witnessing a “full-blown war zone as governments across the

\(^{15}\) An Internet User is defined as an individual who has access to the Internet at home, via computer or mobile device (Internet Live Stats, “Number of Internet Users (2016) – Internet Live Stats,” accessed August 27, 2016, http://www.internetlivestats.com/internet-users/).

globe clash for digital supremacy in a new, mostly invisible theater of operations.” The recognition, adoption and diffusion of this newly emerging intelligence and military capability highlights its significance in scope and impact. Traditionally, MMIs are displayed on the battlefield during kinetic warfare, and lead to emulation and adoption by nation-state competitors; however, in some instances, a significant capability revelation can occur during peacetime and trigger an international response to and adoption of a new capability or warfighting paradigm, without display of the entirety of the capability at first. As of 2011, the Center for Strategic and International Studies publicly identified 33 nation-states that have adopted the use of Computer Network Operations in their military planning. These elements will typically include using CNO as a reconnaissance tool, intelligence gathering function, and/or for cyberattack capability and capacity building, either as standalone elements or in combination with traditional electronic warfare or information operations.

Computer Network Operations capabilities offer the ability to conduct espionage, sabotage or warfare in a manner which is scalable, instantaneous, can be focused on one or one thousand simultaneous locations or more at the discretion of the attacker, remotely executed from anywhere on the planet, and are not necessarily attributable nor traceable at close to the speed of light. No intelligence or military capability like it has ever been

---

developed. As early as 1997, the National Security Agency (NSA) recognized that the development of computer network attack capabilities, facilitated by computer network exploitation, presents a method for “incredibly accurate strikes on infrastructure targets by means of cyber-attacks on the information infrastructure needed to operate it.”

Indeed, the efficacy of this weaponized technology may become the key to success or failure in future conflicts. According to a Defense Science Board Report in 2013, if the US became engaged in a “full-scale conflict with a peer adversary, attacks would be expected to include denial of service, data corruption, supply chain corruption, traitorous insiders, kinetic and related non-kinetic attacks at all altitudes from underwater to space.” The report predicted reasonably foreseeable cascading second and third order effects for the civilian populations, akin to the second and third order effects experienced by civilian populations in traditional armed conflicts, including the “disruption of electricity, monetary systems, communications, and electrically pumped fuel. Depending on the nature of the attack, the effects could last from a few days to months or more to reestablish basic infrastructure operations.”

Specific types of computer network operations attacks against critical infrastructure are a continuing concern. Critical infrastructure is defined in the US as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on

---

security, national economic security, national public health or safety, or any combination of those matters.\textsuperscript{23} In November 2014, Representative Michael Rogers, Chairman of the House Permanent Select Committee on Intelligence (HPSCI), stated in public that certain nation-state entities are probing Americans’ critical infrastructure networks and in some cases have gained access to industrial control systems through the use of trojan horse malware that can be used to shut down oil and gas pipelines, power transmission grids and water distribution and filtration systems.\textsuperscript{24} NSA Director Mike Rogers, who was a witness in front of the HPSCI, stated that “there are nation-states and groups out there [outside the US] that have the capability to enter...[US] industrial control systems (ICS), and to shut down...our ability to operate our basic infrastructure.”\textsuperscript{25} In July of 2014, the US Department of Homeland Security Industrial Control System Computer Emergency Response Team (ICS-CERT) discovered an ICS-focused malware campaign that used multiple infection vectors to compromise systems, including phishing emails, redirects to compromised web sites and Trojanized update installers.\textsuperscript{26} Moreover, ICS-CERT released preliminary notification documents in December 2014 warning critical infrastructure owners about a different ongoing malware campaign that compromised

numerous industrial control systems (ICS) environments, had the ability to manipulate these systems and apparently was active since at least 2011.  These public statements were likely in response to the recently discovered Black Energy and Havex malware campaigns, which will be discussed briefly later on in this chapter.

**Technology Change and Systems Development**

The move from standalone computers to network computers, transistor and microprocessor development and miniaturization have led to an explosion of affordable personal computer systems. The expansion of computer languages, software development and graphical user interfaces have simplified the use of computers for the entire world; the development of the Advanced Research Projects Agency Network (ARPANET) and later the commercial Internet and the global adoption of this system were only possible through the development of massive switches, routers and fiber optic cables. The development of high-speed Internet connections, broadband and wireless technologies all build from these changes as well. This in turn facilitated decisions to develop highly networked and interdependent information systems to control information and critical infrastructure functionality. The continuous integration of these components led to the widespread automation of industrial system processes and facilitated centralization and remote access control of these systems. As a result, the world is dependent upon unprecedented speed of information flows enabled by fiber optic cables that can literally transmit information and remotely provide instructions to these systems at close to the

---

speed of light. Some key examples of these technology changes and systems developments are discussed in this section.

The development of accessible and affordable computer hardware, operating systems and software underpins the entirety of technology changes and systems development for the emergence of computer network operations as a major military innovation. Today it is estimated that there are over two billion personal computers in the world. This is due to the invention of the microprocessor in the early 1970s which led to building personal use computers (PCs). The development of operating systems for these machines, as well as programs for word processing, accounting and databases for storing and organizing information for recall and analysis soon followed. IBM entered the PC market in 1980, which led to an explosion in the adoption of computer technology throughout the United States and the world. The Disc Operating System (DOS) and the creation of a graphical user interface simplified the use of the systems, while marketing “prepackaged” software applications provided sophisticated capabilities at an affordable price, further expanding the distribution of these integrated systems.

---

Advanced connectivity capabilities, which started during the 1970s, paralleled the ongoing development of sophisticated personal computers and ultimately resulted in a revolutionary convergence that has directly facilitated the development of Computer Network Operations as a major military innovation. The rise of the Internet, an incredibly complex system of systems integration, is the key enabler of computer network operations. This system began to develop in 1961 as a result of the writings of Leonard Kleinrock, a Massachusetts Institute of Technology (MIT) researcher, and resulted in the creation of ARPANET in 1969. ARPANET demonstrated the possibilities of computer networking based on a variety of packet-switching technologies. More specifically, telecommunications switches, which are the “brains” of interconnected communications, parse incoming voice or data signals to determine the desired destination address and create a transmission path between incoming and outgoing physical communications ports and links. These transmissions are accomplished through the use of a circuit switch (voice) or packet switch (data - router). These switches digitize, encode and transmit speech or data which is reconstructed upon arrival at its destination end point, a functionality that is only made possible by specialized computers called servers. The creation of the multiprotocol router in 1980 advanced connectivity for network-based

36 The 4ESS switch was a key to the rise of fiber-optic transmissions of information. This switch, together with new data transmission formats such as packet switching, frame relay, asynchronous transfer mode (ATM) and Internet protocols, combined to facilitate the telecommunications revolution (AT&T, “History of the AT&T Network: History of Network Switching,” accessed August 27, 2016, http://www.corp.att.com/history/nethistory/switching.html.
data transmission between servers as well. In 1982 Transmission Control Protocols (TCP) and Internet Protocols (IP) emerged as the connecting mechanisms for various smaller networks and led to computers on a network to be given a unique identifying number, know as an IP address. Soon after, in 1983, the Domain Name System (DNS) was created and established a common protocol for defining various Internet communities as well as a Uniform Resource Locator (URL) system, which ascribes a “unique address for a file that is accessible on the Internet.” In 1989, additional innovations were created, including a new computer language called HyperText Markup Language (HTML), a communications protocol called HyperText Transfer Protocol (HTTP) and the design of a Uniform Resource Identifier, which is a unique address to identify each location on the Internet. Furthermore, the first “point and click browser/editor” software was developed, which was called the World Wide Web (WWW).

The adoption and integration of fiber-optic cables, which use rapid pulses of light traveling on fibers of ultra-pure glass to facilitate the transmission of digital (information, text, images, video) data across long distances, further expanded the Internet’s connectivity and capacity. Fiber-optic cables provide a high-speed, reliable, and scalable transmission medium, enabling the Internet to continue growing and evolving to meet the constantly increasing demands of users worldwide. It is worth noting that Jim Duffy’s article “Evolution of the Router” provides an in-depth overview of the evolution of routers and their role in the Internet’s infrastructure. Similarly, Jeff Tyson’s work on “How Internet Infrastructure Works” offers a comprehensive look at the various components and protocols that underpin the Internet. While Kim Zimmermann’s “Internet History Timeline: ARPANET to the World Wide Web” offers a historical perspective on the development of the Internet, Margaret Rouse’s definition of URL from WhatIs.com clarifies the importance of Uniform Resource Locators in the Internet’s operation. The World Wide Web Foundation’s timeline, “History of the Web,” illustrates the key milestones and innovations that have shaped the development of the World Wide Web. Finally, Michael L. Dertouzos’s book “Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its Inventor” and John Impagliazzo’s “History of Computing in Education: IFIP 18th World Computer Congress, TC3/TC9, 51st Conference on the history of computing in education, 22-27 August 2004, Toulouse, France, Vol. 145” offer valuable insights into the broader context of computing education and the history of computing.
visual and voice) data, transformed the speed at which sending and receiving of information could be accomplished, and in effect was the establishment of an “entirely new system” for telecommunications.\(^\text{42}\) For example, in the mid-1980s, ARPANET operated with 56 Kilobits (a kilobit is 1000 bits per second, abbreviated as Kbps) circuits. Once fiber-optic technology was used to create the first high-speed backbone in 1987, called the National Science Foundation Network (NSFNET), speeds on intragovernment systems increased to 1.5 MBps in 1988\(^\text{43}\) and to 45 megabits (a megabit is one million bits per second, abbreviated as MBps), an order of magnitude larger by 1991. These significant increases in capability and capacity were due to the adoption of fiber optic technology. Fiber-optic technology adoption spread, and accelerated connectivity speeds and worldwide Internet access as a whole beginning in the late 1990s.\(^\text{44}\) The development of gigabit networks, which are broadband networks that can transmit data at one billion bits per second or more via fiber optic lines, represented a significant leap forward in connectivity speeds, and faster data transmission followed over time.\(^\text{45}\) As a result, high-speed Internet connectivity grew from 2.8 million connections in December 1999 to 243 million as of June 30, 2012.\(^\text{46}\)


The development of information and communications technology (ICT), which is characterized by accessibility, connectivity and speed, is now ubiquitous and is increasingly intertwined in industry as well as military and civilian life. However, the development of these systems created a tremendous range of vulnerabilities which have become more pronounced over time.

**Vulnerabilities and Methods to Exploit Them**

The co-development of personal computers, software and hardware such as routers and switches, which we call the Internet, and its function as an interconnected delivery mechanism, did not substantially take into account security-related measures as a part of its inherent functionality, and is actually comprised of an ad hoc system of systems that continues to mature over time. As a result of this ad hoc and decentralized systems development, which has radically exceeded all initial utilization expectations, a vast number of information security vulnerabilities have developed. The possibilities for exploitation are further compounded by the complexity of the software controlling the functions of the hardware itself, which creates exponentially larger attack surfaces. Richard Danzig cites, for example, the Linux operating system which has grown from 176,000 lines of code when introduced 20 years ago to over 15 million lines of code in 2011, and reports that there will be approximately 8.6 million lines of code in the Pentagon’s new Joint Strike Fighter aircraft and an estimated 50 million lines of code in
Microsoft’s Vista operating system. This leaves ample opportunity for unintentionally created and inherent vulnerabilities to be discovered.

Information security vulnerabilities are mistakes in software that can be directly used by an attacker to gain access to a computer system (or a set of systems). These vulnerabilities, at a minimum, allow an attacker to execute commands as another user, access data contrary to the specific access restrictions for that data, pose as another entity or to conduct a various denial of service, data manipulation, deletion or physically destructive attacks. A global tracking system for common vulnerability and exposures (CVEs) was developed, and has catalogued over 73,258 CVEs since 1999. Computer Network Operations typically rely on leveraging CVEs, each of which was once an unknown vulnerability, as part of the interdependent computer network attack process. The first use of an unknown and unmitigated vulnerability, which is also known as a “zero day,” provides a significant advantage to an attacker, since this type of exploitation

48 The process of finding and exploiting vulnerabilities to gain system or network access is integral to the ability to conduct destructive operations, and will be described in the Operationally Innovative Use subsection.
50 CVEs are composed of two possible categories: vulnerabilities, described above, and exposures. Exposures are not vulnerabilities, but provide an important component of a successful attack that allows an attacker to conduct information-gathering activities, hide activities, or provide primary points of unauthorized entry into a computer or network MITRE Corporation, “CVE – Terminology,” Common Vulnerabilities and Exposures, accessed August 27, 2016, https://cve.mitre.org/about/terminology.html).
is difficult to discover. According to FireEye “it often takes not just days but months and sometimes years before a developer learns of the vulnerability that led to an attack.”

As a result, in an almost co-evolutionary manner we have seen the emergence and development of malicious software, or malware, which is defined as “any program that works against the interests of the system’s user or owner, usually without the owner’s informed consent.” The most common forms of malware are viruses, worms and remote access Trojans (RATs), which are explicitly designed to exploit specific information security vulnerabilities, including zero days, and their capabilities are becoming exceedingly complex.

A computer virus is a small software program that spreads from one computer to another through a variety of means, and can interfere with computer operations. Viruses can also “infect” other programs by modifying them and can spread throughout a computer system or network. As early as 1985 NSA recognized that the “threat of computer virus attack is very real,” and the application of malicious code in the form of computer network attack fell into three major forms: “compromise, spoofing and denial of services.” Viruses could be employed to mount “denial of service attacks” (defined as “the unauthorized use of system resources to the exclusion of authorized users”) that

---

55 National Security Agency, redacted author, “Computer Virus Infections: Is NSA Vulnerable?” Cryptologic Quarterly 4, no. 3 (Fall 1985); the author also recognized the existence of “trojan horses…computer program[s] which, in addition to performing a desired function, causes a malicious side effect when run by an unsuspecting user…and whose identification is difficult.”

could bring a computer system to a halt.\textsuperscript{56} This acknowledgement is likely due, at least in part, to an article authored by doctoral student Fred Cohen entitled “Experiments with Computer Viruses,” which cites the development of the first virus in 1983, just two years after the introduction of the first mass-market IBM personal computer.\textsuperscript{57} Similarly, the “first computer worms were created in the labs of John Shock and Jon Hepps of Xerox’s Palo Alto Research Center in the early 1980s”\textsuperscript{58} (although a “creeper program” to provide systems updates across ARPANET was already created by computer scientists a decade earlier). A trojan horse (program), described as “a computer program that appears to the user to perform a legitimate function but in fact carries out some illicit function that the user of the program did not intend,” is a term attributed to NSA employee Dan Edwards.\textsuperscript{59}

Most viruses simply replicate or display messages; however, some viruses have a portion of code designed to deliver a payload that can “corrupt programs, delete files, reformat a hard disk, or crash a network.”\textsuperscript{60} There are various types of viruses, including simple viruses, outlined above; encrypted viruses, which are designed to avoid technical “signature” detection by obfuscating the virus, making it unrecognizable to antivirus software; or polymorphic viruses which include a mutation engine that generates

\textsuperscript{57} Fred Cohen, “Computer Viruses” (PhD diss., University of Southern California, 1985).
randomized decryption routines that change each time a virus infects a new program, to further obfuscate its presence. Similarly, a computer worm is a type of computer virus that can spread without human interaction. Worms usually propagate through opening an email attachment and spread automatically through email messages, networks or operating system vulnerabilities. Worms steal and utilize information from the infected computer to spread, and can overwhelm computer systems quickly. Worms are not always destructive to computers, but at a minimum, they usually cause computer and network performance stability problems. Remote Access Trojans (RATs) are a more evolved form of malicious trojan horse malware, and today RATs are considered more dangerous than most all other types of malicious code. RATs permit an intruder to control the totality of a computer’s operations. The various functions include the ability to delete and modify files, format or reformat hard disks, upload and download files with additional malicious functionality. The use of RATs can allow an attacker to spread throughout associated or interconnected networks, and gather technical characteristics from the infected systems, a process known as enumeration. RATs create a permissive operating environment for extensive exploitation, exfiltration or destruction of the

---

functionality of these systems, rendering them useless, with associated second order or third order effects.65

Malware capabilities are becoming more sophisticated and complex in nature, yet the process to use and customize malware is becoming more simple and widespread. Technology development and maturity levels for malicious code such as a Remote Access Trojans now make the automated creation of polymorphic malware tools possible. Similarly, automated attack capabilities are now launched at machine speed and the ability for nation states and even individuals to attack on a widely distributed basis across multiple systems simultaneously is being observed as a result of innovations in Internet-enabled command and control mechanisms and vast networks of infected and enslaved computers known as botnets.66

Operationally Innovative Use

As early as 2006, the Chairman of the Joint Chiefs of Staff called “operations in cyberspace a critical aspect of our military operations around the globe.”67 The US military defines cyberspace as a separate and distinct domain of military operations to the

---


traditional military battlespace domain areas on land, sea, air and space. States conduct computer network operations to achieve a variety of political, economic or military objectives, which can be either tactical or strategic in nature, or both. The applications of these methodologies allow flexible espionage, sabotage or warfighting goals to be realized. Cyber attacks offer reduced costs compared to conventional strikes with greater efficiency; the asymmetric nature of cyber attacks makes them difficult to defend against; the anonymous nature of their offensive capabilities allows an attacking government to circumvent approval by the world community to a military offensive. There is the ability to conduct cyber attacks in peacetime for immediate geopolitical ends, as well as to prepare for possible future kinetic attacks or wartime use as a standalone or integrated capability. The nature of computer network operations can be patent and overt, or in the alternative, provide plausible deniability to the perpetrator or facilitate the misattribution of the activity to another actor when this is seen as politically desirable. Other motivations, which are closely related to political, economic or military goals, would include a desire to deny an adversary their existing capabilities, and/or close traditional technological or military superiority gaps by degrading the networked informational foundations upon which these capabilities depend. This type of degradation could include the disruption or destruction of command, control, communications and intelligence-gathering functions or possibly the actual functioning of advanced, interconnected software- and hardware-dependent weapons systems or platforms. The applications of

---

computer network operations seems only limited by the imagination and technical prowess of the analysts, targeters, designers and operators behind the creation and use of these tools.

**Some Examples of Computer Network Operations and the Effects They Can Cause**

**Spoofing**

According to the UK Register, in 2007 Israeli forces were able to shut down Syrian air defense systems through the use of an airborne network attack system developed by BAE Systems capability called SUTER. SUTER allows users to invade communications networks, see what enemy sensors see, and even take them over as systems administrators to manipulate sensors into positions so that approaching aircraft cannot be seen.\(^69\)

**Data Deletion Attacks**

There are two recent, significant data deletion attacks accomplished through the use of computer worms with data deletion capabilities which are prominent examples of CNA\(_1\): the Saudi Aramco and Sony Pictures incidents. While these would not generally be considered military-grade computer network operations tools, they highlight the types of capability development occurring in CNO.

**Saudi Aramco Attack**

According to publicly available reports, in late October 2012, Aramco, a Saudi state-owned oil company, experienced a destructive data attack after malware was introduced into its computer systems, which “erased documents, spreadsheets, e-mails,

and files on approximately 30,000 systems.” As a result of the attack, the firm shut down internal corporate networks, and disabled e-mail and Internet access in order to stop the virus from spreading. This malware, later named Shamoon, was a computer worm “designed to replace the data on hard drives with an image of a burning American flag and report the addresses of infected computers.” The code included a timing mechanism set for the exact time the attackers wanted the data deletion to commence, known as a kill switch. Specifically, Shamoon corrupted files on the infected computers and overwrote the Master Boot Record (MBR) in an effort to render a computer unusable. McAfee, a US antivirus firm, indicated that the “worm may be spread by infected removable drives…., be installed by visiting a malicious web page (either by clicking on a link), or by the website hosting a scripted exploit which installs the worm onto the user’s system with no user interaction.” The US Department of Homeland Security indicated the malware was designed for information stealing with a highly destructive data deletion module that spread via network shares to infect additional machines after the initial

infection, and could result in operational impacts including loss of intellectual property and disruption of critical systems.\(^{74}\)

*Sony Pictures Attack*

In late November 2014, Sony Pictures Entertainment (SPE) experienced a cyber attack that destroyed computer systems and stole large quantities of personal and commercial data through the deployment of destructive malware, rendering thousands of SPE’s computers inoperable.\(^ {75}\) According to the United States Computer Emergency Readiness Team (US-CERT) the attackers used a Server Message Block (SMB) Worm Tool to conduct the attacks. The attack tool was equipped with five components, including a Listening Implant, Lightweight Backdoor, Proxy Tool, Destructive Hard Drive Tool, and Destructive Target Cleaning Tool.\(^ {76}\) The tool possessed a sophisticated multifunction capability designed to confirm initial remote access, defeat firewalls, discover and exploit network infrastructure, identify specific machines, run remote commands, transfer files, destroy data past the point of recovery and render the computer systems it infected non-operational with irrecoverable data while spreading this destruction throughout the entire network. The malware also had a self-reporting damage


assessment function. US-CERT assessed that this malware could result in operational impacts including loss of intellectual property and disruption of critical systems.77

**Sabotage or Physically Destructive Capabilities: Examples of Physical Objects Being Destroyed**

CNA can be used to destroy physical objects connected to a computer. Typically this can be accomplished through the manipulation or data wiping of industrial control system software, but there are other possibilities as well.

Industrial control systems (ICS) include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system components such as Programmable Logic Controllers (PLC) which are in widespread use by industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, automotive, aerospace, and durable goods. ICS are often highly interconnected and mutually dependent systems and the US Government considers them to be vital to the operation of America’s critical infrastructures.78 Similarly, the use of ICS is worldwide. According to the NIST, affecting the programming logic running ICS has a direct effect on the physical world, and could result in significant risk to human health and safety,

---


78 SCADA systems are typically used for centralized control of dispersed machinery. DCS can be used to control production systems within a local area while PLCs control specific applications (Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, *Guide to Industrial Control Systems (ICS) Security*, Preprint, NIST Special Publication 800, no. 82, rev. 2 (Gaithersburg, MD: 2015), accessed August 28, 2016, http://dx.doi.org/10.6028/NIST.SP.800-82r2).
damage the environment, and/or cause serious financial issues that negatively impact a nation’s economy.  

Internet-connected ICS systems are vulnerable to remote computer network operations, as exemplified by the Black Energy and Havex malware campaigns described earlier in this chapter. These types of operations are now possible due to systems development. Traditionally, ICS were physically and logically isolated, not Internet connected, used proprietary operating instructions, and consisted of specialized hardware and software components. With the changes in information technology and the expansion of the Internet, ICS are becoming integrated with business information technology (IT) systems, are no longer physically or logically isolated, use commercially available operating systems and are becoming highly standardized. Furthermore, ongoing integration efforts are increasing the use of wireless technologies, which places these systems “at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment.”

Interference with the operations of ICS can include: blocking or delaying flow of information through ICS networks; unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life; causing inaccurate information to be sent to system operators, to disguise unauthorized changes, or to cause the operators to

---


initiate inappropriate actions, which could have various negative effects; modifying ICS software or configurations or introducing malware infections, which could have various negative effects; interference with the operation of equipment protection systems, which could damage equipment; or interference with the operation of safety systems, causing systems failures which could endanger human life.

Figure 2. Supervisory Control and Data Acquisition (SCADA) System General Layout. Note: WAN = Wide Area Network; MTU = Master Terminal Unit (server for SCADA system); IED = Intelligent Electronic Device; RTU = Remote Terminal Unit. Source: Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, Guide to Industrial Control Systems (ICS) Security, Preprint, NIST Special Publication 800, no. 82, rev. 2 (Gaithersburg, MD: 2015), accessed August 28, 2016, http://dx.doi.org/10.6028/NIST.SP.800-82r2.

While not specifically an ICS attack, although operating on the same principles, the Project Aurora Test, performed in 2007 at Idaho National Laboratory, provided a live demonstration of how a cyber attack could destroy a 27-ton diesel generator by over-

Similarly, the publically reported deployment of Stuxnet, the first malware known to specifically target a control system, coupled intelligence, surveillance and reconnaissance (ISR) functionality with a capability to exploit programmable logic controllers (PLC) and human machine interface software (HMI). This malware is an example of the combination of precise targeting and the creation of kinetic effects in the
physical world, reportedly causing mass-scale equipment destruction while inducing the appearance that all systems were perfectly functional. This was reportedly accomplished by malware that modified a PLC code while engaged in a sophisticated evasion technique that was successfully hidden from the operator. The worm and its payload only impacted control systems operating a specific variable frequency drive, with tailored destructive effects limited specifically to the target the malware was designed to find.\textsuperscript{85}

How, or if, this activity translated to the creation of an alleged covert US program that included experimental methods to undermine electrical systems, computer systems and other networks on which Iran relies is open to speculation.\textsuperscript{86} Regardless of the name of the program or the name of the worm, what came to be called Stuxnet is by far the most sophisticated attack code uncovered to date. The Stuxnet worm repeatedly sought to infect five industrial facilities in Iran over a 10-month period. The advanced worm recorded information on the location and type of each computer it infected.\textsuperscript{87} Half a million bytes long, Stuxnet was designed to propagate via thumb drives and other removable media. It targeted a single, specific type of highly specialized industrial control system at one location, Iran’s Natanz uranium processing facility.\textsuperscript{88} Researchers

at Symantec were able to build a model of the spread of the infection; they determined that 12,000 infections could be traced back to just five initial infection points.\(^8^9\)

Stuxnet represents the first of many milestones in malicious code history: It is the first worm to exploit four 0-day vulnerabilities, compromise two digital certificates, inject code into industrial control systems, and hide the code from the operator.\(^9^0\) Stuxnet highlighted a new reality in CNA history: Direct-attack attempts on critical infrastructure and the ability to cause physical destruction through the use of binary digital code are now reality. The New York Times declared that Stuxnet appears to be the first time a nation-state repeatedly used cyberweapons to cripple another country’s infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives.\(^9^1\) Recently, Symantec research published a white paper citing evidence to buttress its claim that a beta version (the so-called “0.5”) of what came to be called Stuxnet was in “development as early as November 2005.” This beta version was previously flagged by malware researchers as


\(^9^1\) “Cyberattacks on Iran — Stuxnet and Flame,” *New York Times*, accessed August 30, 2016, http://www.nytimes.com/topic/subject/cyberattacks-on-iran-stuxnet-and-flame. Perhaps more importantly, according to experts at Symantec, “The technical novelty of the individual components of the Stuxnet worm is not astonishing. What is more interesting is the way those different parts are combined with each other to result in a powerful targeted threat against control systems used in nuclear facilities. In fact, Stuxnet is highly modular, and this feature allows sophisticated attackers to build a targeted attack from various pieces of code, similar to the way carmakers build new cars from available parts. This modularity also means a new era for malware developers, with a new business model pointing towards distributed labor where malware developers can work simultaneously on different parts of the system” (Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier* (Cupertino, CA: Symantec Corp., 2011), accessed August 30, 2016, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
early as November 2007. This revelation, the result of ongoing forensic analyses related to CNA₂, indicates a robust CNA₂ capability may have existed much earlier than originally known. James Andrew Lewis observed that “the use of network technologies and the exploitation of cyberspace for intelligence and attack has become a normal part of military activity…. We can now go beyond the disruption of networks and information to ascribe a kinetic effect to cyber weapons—the ability to inflict physical damage through cyber-attack.” General Michael V. Hayden recently summed up the emergence of a new CNO MMI.

By mid-2010, though, a little more than a year after I left government, there was little doubt that cyber weapons had come of age. Someone, almost certainly a nation state (since this was something too hard to do from your garage) used a cyber weapon that was popularly labeled STUXNET to disable about 1000 centrifuges at the Iranian nuclear facility at Natanz. When the fact of the attack became public, I commented that—although this did not compare in any way in destructive power—it felt to me a little bit like August, 1945. Mankind had unsheathed a new kind of weapon. Someone had crossed a Rubicon. A legion was now permanently on the other side of the river. We were in a new military age. What had been concept and anticipation only two decades earlier in Texas was now reality.

A new reality, indeed. Recently, a second physically destructive cyber event has been reported by the German government and the U.S. press. According to a combination of reports by the German Federal Office of Information Security (BSI) in late 2014, and another in late 2015 by Bloomberg News, a targeted attack on the computer network of a steel mill owned by ThyssenKrupp AG, Germany’s largest steelmaker, caused “the

---

uncontrolled shutdown of a blast furnace, leaving it in an undefined state and resulting in massive damage.\textsuperscript{95} The attackers, according to the reports, used “spear phishing e-mails and sophisticated social engineering to gain access to the steel mill’s office and production networks…and developed or possessed detailed technical knowledge of the ICS and production processes being used.” Bloomberg News stated that over the course of weeks, the “attacker(s) inserted malware, took control of a computer that operated digital controls for the blast furnace, tampered with temperature sensors and motors that controlled gas flow and remotely disabled the furnace’s ability to shut down…which apparently caused the machine to overheat and melt down.”\textsuperscript{96}

**Significant Organizational Adaptation**

NSA, CIA and DoD have all implemented organizational adaptations in response to changes in the technological and operational environments around the world. Furthermore, the Department of Defense has formalized military computer network operations warfighting capabilities. These changes highlight the importance of computer network operations as a driving force for modern warfare and an emerging MMI.

NSA had primary responsibility for the collection and analysis of signals intelligence and was also responsible for protecting information systems security of U.S.


government agencies. NSA, however, faced increasing technical challenges to SIGINT collection in that as early as 1982, NSA recognized that:

As computers become more tightly integrated into telecom nets, the central problems facing SIGINT will become what to target and how. The most useful data, from an intelligence or a SIGINT viewpoint, may be resident in the system in a computer memory, rather than passing over a communication channel. SIGINT, instead of waiting for data to be transmitted and then passively collecting and exploiting them, will have to penetrate into the nets, find what is there, and extract it.  

According to the Congressional Research Service, changes at NSA were due, at least in part because data transmission contents in fiber optic cables could not be “readily intercepted…without direct access to the cables themselves…and…affect requirements for expensive SIGINT satellites since transmissions over fiber optic cables cannot be intercepted from space-based platforms.” Significant internal realignments occurred, in part to address these concerns, starting in 1996 when General Ken Minihan took over the reins at NSA to address the challenges of scaling up computer network exploitation and was tasked with the mission to develop computer network attack capabilities as early as 1997. Achieving the wholesale development of these capabilities, however, required significant organizational adaptation over time. This adaptation included closing the largest SIGINT element at NSA, called A group, to reallocate operational funds and refocus NSA’s mission into CNE. Soon after, the creation of a special interagency

---

organization housed at NSA called the Information Operations Technology Center (IOTC) to develop computer network exploitation and attack tools was an especially important organizational adaptation during this time period. This organization was charged with the responsibility for creating, gathering and validating CNA tools for the whole of the Intelligence Community as well as DoD.\textsuperscript{100} Furthermore, in 1999, the concept of “Digital Network Intelligence” was identified as a new SIGINT paradigm, defined as the intelligence from intercepted digital data communications transmitted between, or resident on, networked computers,\textsuperscript{101} and by definition shows that NSA repositioned itself to exploit computer-to-computer communications. This paradigm change provides strong evidence of an organizational adaption from traditional radio frequency (RF) interception capabilities to digital interception. Indeed, this paradigm change drove additional recommendations of “enabling taxonomies,” or flexible nomenclatures and methods to meet this new technical approach, including deployment strategies, mission management, functional capability needs, skill sets, system needs, organizational needs and resource requirements.\textsuperscript{102} This was apparently driven, at least in part, by global technology changes and interconnectivity in communications such as

\textsuperscript{100} The Title 10-Title 50 debate is essentially a debate about the proper roles and missions of U.S. military forces and intelligence agencies. “Title 10” is used colloquially to refer to DoD and military operations, while “Title 50” refers to intelligence agencies, intelligence activities, and covert action. See: Andru E. Wall, “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities and Covert Action,” Harvard National Security Journal 3 (2011): 85, accessed August 31, 2016, http://www.soc.mil/528th/PDFs/Title10Title50.pdf.


satellite, satellite gateways, public access Internets and intranets, cellular communications, digital switches, etc.\textsuperscript{103}

Similarly, CIA created a new organization to focus on computer network exploitation and other related human intelligence (HUMINT) technical operations\textsuperscript{104} in 1995 called the Clandestine Information Technology Office (CITO), a response to CIA’s concern that it “might not be ready to exploit the rapid expansion and utilization of advanced technology in various target domains and ‘seize’ the collection opportunities in the rapidly emerging high tech environment.” The creation of CITO led to an “advent of espionage in cyberspace [that] was nearly instantaneous…its rapid growth and impact on (CIA’s) operations was stunning and even revolutionary.”\textsuperscript{105} CITO eventually morphed into a full-spectrum computer network operations entity called the Information Operations Center housed in the Directorate of Operations in 2001, with portions of its initial mission transferred to the Office of Technical Collection.\textsuperscript{106} In 2015, CIA announced the start of a massive new reorganization, creating the Directorate of Digital


\textsuperscript{104} According to the House Permanent Select Committee on Intelligence, “A clandestine service does much more than simply collect ‘HUMINT’ clandestinely…it also works in liaison with other spy services to run all types of operations; it taps telephones and installs listening devices; it breaks into or otherwise gains access to the contents of secured facilities, safes, and computers; it steals, compromises, and influences foreign cryptographic capabilities so as to make them exploitable by US SIGINT; and it clandestinely emplaces and services secret SIGINT and MASINT sensors” (United States Congress. House Permanent Select Committee on Intelligence, “IC21: The Intelligence Community in the 21st Century: Clandestine Service Executive Summary,” 104\textsuperscript{th} Congress, Second Session, Chapter IX (1996), accessed August 31, 2016, https://www.gpo.gov/fdsys/pkg/GPO-IC21/html/GPO-IC21-9.html.


37
Innovation (DDI), the first time in more than 50 years that the organization has formed a new directorate, “designed to accelerate the infusion of advanced digital and cyber capabilities across the agency” and consolidating the “CIA’s digital operations — from cyberespionage to data warehousing and analysis.”

In contrast to the IC, at first it appears that DoD’s broader non-cryptologic and intelligence component interests in CNO were initially focused on CND for its own networks. In 1998, Joint Task Force—Computer Network Defense (JTF-CND) was created under the auspices of the U.S. Space Command. This was likely driven by the fact that the US was experiencing the effects of computer network exploitation itself. For example, CIA was “detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber warfare programs in other countries,” although this organization alignment would prove itself to be suboptimal. However, By April 2001, JTF-CND’s mission expanded to include computer network attack, and it was renamed Joint Task Force—Computer Network Operations (JTF-CNO). The task force became part of the US Strategic Command (USSTRATCOM) in October 2002. The US formalized authorities for militarily significant CNE and CNA capabilities as early as

---

February 2003 through National Security Presidential Directive (NSPD)-16, which “provided guidance to determine how and when the United States would launch a Computer Network Attack (CNA) against foreign systems, and who would be authorized to conduct such operations.”¹¹² The issuance of this type of national security directive implied a robust capability that will likely expand over time. By 2004, JTF-CNO was renamed Joint Task Force—Global Network Operations (JTF-GNO), although the network attack mission transferred in 2003 to a new organization, which evolved into the Joint Functional Component Command—Network Warfare (JFCC-NW) in January 2005, led by the Director of NSA, who was given specific CNA authorities via a delegation process¹¹³ which provided a specific, seminal convergence of intelligence capabilities with military authorities for computer network operations. A sophisticated computer network exploitation intrusion (commonly referred to today as BUCKSHOT YANKEE, although this is the name of the remediation operation)¹¹⁴ led to a further restructuring and recombining of US offensive and defensive computer network operations resulting in the establishment of U.S. Cyber Command in May 2010, effectively a National Security Agency/US Cyber Command (NSA/CYBERCOM) hybrid under a single dual-hatted commander who was now authorized to and capable of executing both the CNE and CNA, and CND missions under two sets of legal authorities. This significant

consolidation of authorities allows for a large degree of flexibility to engage in a variety of highly informed operational environments, during peacetime, times of heightened tensions, or during warfare. Dual-hatting, while not in and of itself unusual, is particularly important in the case of CNO as a MMI, and according to the White House, “keeping the positions of NSA Director and Cyber Command Commander together as one, dual-hatted position is the most effective approach to accomplishing both agencies’ missions.”\textsuperscript{115} According to the \textit{Washington Post}, which provided analysis of the mechanism and effects of this dual-hatted arrangement, US personnel “who operate under intelligence legal authorities, may switch to a military authority when they are ordered to conduct a computer attack under an execute order by the president and the defense secretary. The process is documented. ‘You can be doing intelligence-gathering one second and then pull the trigger on an offensive op the next,’ a former intelligence official said.”\textsuperscript{116}

\textbf{Conclusion}

Computer network attack and computer network exploitation (CNA/CNE), as a subset of CNO, is a prominent example of a MMI in the 21\textsuperscript{st} century. CNO came into being as a result of technology changes, systems development, operational innovations and organizational adaptation. Technological changes, including the development of accessible and affordable computer hardware, operating systems and software underpin


the entirety of today’s modern world. A series of worldwide integrations between computing systems and telecommunication capabilities connected by high-speed transmission lines is now used by at least 40% of the world’s population. However, this same supersystem has inherent vulnerabilities, and exploitation of this supersystem is now routine and increasingly dangerous. Operational innovations designed to exploit these systems from thousands of miles away, many times anonymously, run the gamut from denial of use to espionage and various levels of physical destruction. Significant organizational adaptation has occurred over time in the US Intelligence Community to create this MMI and provide a highly effective new capability for the Department of Defense, which itself has undergone significant organizational adaptation to ensure it can make effective use of the tools. Broadly speaking, CNO has caused organizational adaptation and changes at NSA, CIA and DoD in the way the organizations “fight,” and in each instance caused the creation of a new combat arm, in addition to a change in the concepts of operation of that combat arm, with a new type of fully integrated intelligence-gathering and warfighting capability. This new instrument of power is still in the process of being incorporated and refined in an iterative cycle of technology change, systems development, operational innovation, organizational adaptation and doctrinal development, both in the US and worldwide.
CHAPTER 2. LITERATURE REVIEW OF MMI THEORIES

The literature on military innovation has largely focused on three main theoretical explanations: civilian–military relations, intraservice politics and interservice politics. Each of these theoretical explanations will be used to determine their level of explanatory power as to why computer network operations have emerged as a major military innovation.

Civilian–Military Relations

Most discussions of US military innovations start with civilian–military relations as a framing theory. According to Barry Posen, MMIs are primarily the result of “civil–military dynamics that determined whether interwar militaries would innovate.” Posen’s theory implicitly identifies the phenomenon of military bureaucratic conservatism and its inclination toward slow incremental change or, in the worst cases, “routine” intransigent failure to adapt, resulting in the routine suboptimization of strategic initiatives.\(^\text{117}\) Posen observed that a military bureaucracy’s interest in reducing uncertainty will keep it resistant to change and locked into “standard operating procedures.”\(^\text{118}\) Furthermore, Posen posited that a typical military bureaucracy structure, which by its very nature is resistant to change, wants to ensure autonomous action from civilian control and will


therefore structure doctrine “in such a way as to make it inaccessible to political tinkering…and will keep doctrine from responding to changes in political goals.”

Posen observed that even the most successful military organizations require a good “kick in the pants” from external authorities who perceive a threatening external strategic environment if they are to innovate. Posen’s conclusion is that innovation will only occur if statesmen (civilians) intervene in military service doctrinal development, preferably with the assistance of maverick officers from within the service. This highlights the requirement that top-down external executive-level intervention is necessary to induce mission-based problem solving that will ultimately create a major military innovation. The international, grand strategy level of analysis in Posen’s work is focused on how macro-level domestic and international variables interact and the degree to which military organizations respond to top-down directed change based on civilian political goals. This concept can be clarified as the manner in which American political leaders responsible for national security policy can shape or direct the military to meet the country’s evolving security needs. Posen does not examine the underlying foundational technologies that facilitate major military innovation, nor consider a bottom-

up or organizational approach to their creation. One point that Posen makes that will require further examination is his position that new technology is often grafted on to old doctrine. The case study process trace will test this assertion for validity.

There are two variants of Posen’s theory based on the works of Deborah Avant and Kimberly Zisk. Posen, Avant and Zisk agree that doctrine is a result of mixing international and domestic variables. Each of them believes that civilian intervention plays a role in the development of military doctrine, although the level of influence civilians possess and the source of the change to military doctrine varies by writer. These authors do implicitly agree that the threat environment plays an important role in the development of doctrine, but disagree as to level of autonomy the military possesses when instituting innovative doctrinal change.

Deborah Avant succinctly summarizes the inapplicability of Posen’s theory to directly explain the development of major military innovations by identifying Posen’s underlying assumption that the driving factors for MMIs are “balance-of-power crises [which] invoke the top political leadership’s attention, and trigger a rational updating of strategies in conformance with realpolitik…and the assumption that a determined civilian leadership can redirect the military.” Avant examines Posen’s conclusions that military

---


organizations should prefer offensive-style doctrine and should be reticent to change, absent civilian intervention. She also reviews Posen’s belief that civilian leaders are more attuned to international-level threats and intervene to force changes in military doctrine during times of crisis. Avant finds, however, that despite sustained intervention by civilian leaders, minimal doctrinal changes occurred in the US Army during Vietnam.\textsuperscript{126} Avant focuses on the impetus for doctrinal innovation being derived from domestic institutional structures (what she calls the institutional model) which are driven by both the short- and long-term political interests of civilian actors which influence or color the way in which they understand the external strategic threat environment and thus, under the right conditions, directly affects doctrinal innovation.\textsuperscript{127} Avant offers an alternative explanation by examining “the delegation of power between the governing [superior civilian authorities], and the specialized subordinate [the military organization] and attributing success or failure to [innovate] adapt in response to similar threats.” She concludes that the success or failure of civilian intervention can be explained by the strength of undivided civilian institutional control [both presidential and congressional] and its effect on the development of military organization. “When civilian institutional actors are divided in their approach or assessments of what the military should change, the attempts at changing the military’s doctrine will fail.”\textsuperscript{128} By this logic, major military innovations would be driven by the domestic political deliberations of US civilian

authorities, the short-term threat they perceive at the international system level, filtered through the lens of domestic institutions and the US system of checks and balances which drives the nature of the changes ultimately imposed on the military. This research does not address the knowledge gap within the literature relative to Intelligence Community-generated major military innovations, nor does it provide explanatory power regarding the development of the innovation itself.

Kimberly Zisk is critical of Posen and the earlier scholars on civilian–military relations, who view “militaries as hidebound bureaucratic actors, inert unless pushed, and oriented above all toward domestic political competition and organizational predictability.” Zisk hypothesizes that “perhaps it is not that military officers are resistant to innovation in general, but merely to innovation that they believe will damage their bureaucratic and institutional interests.” This hypothesis would indicate that, at least in some instances, military organizations are likely to develop innovative doctrines on their own, in the absence of civilian intervention. Zisk analyzes this dynamic in light of how military officers may respond “when they interpret a foreign doctrinal shift as a threat to the success of their current war plans.” Her analysis embeds a reactive countermove component as the impetus for internally generated (within the military bureaucracy) doctrinal changes as opposed to a domestically based, external intercession by civilian authorities or elites. To her credit, Zisk recognizes that military officers are

genuinely concerned about ensuring the protection of national security during changes in the threat environment and will innovate while straddling the line between bureaucratic self-interest and the importance they place on “policy continuity and institutional stability.” While this research recognizes that military institutions may develop innovative doctrines on their own, it posits that doctrine comes first, and does not flow from technological change. Zisk believes that technology is created over time and then incorporated into a MMI as part of an overall process. Furthermore, Zisk focuses on the international threat environment as a significant driver for this change, which does not readily address peacetime innovation or innovation that occurs during times of low-intensity conflict or so called “small wars.” It must be stated that within the Civilian–Military literature there is an entire area of analysis that focuses on operant factors related to civilian control of the military, which, while interesting as a subtopic, is not on point for this analysis and will not be reviewed in this dissertation.

Interservice Rivalry

In contrast to the Civilian–Military model which has not been widely applied to MMI case studies, the literature on Interservice rivalry is vast and focused directly on the

---


role of bureaucratic politics in generating MMIs. According the Interservice rivalry model of military innovation, the key catalyst for innovation is competition between military organizations as a result of resource scarcity. Under this theory, innovation is an outgrowth of competition between the various armed services within a nation-state who are seeking to maintain their budget authority and end-strength, and thus maintain control over their traditional missions to ensure their ongoing relevance. This type of rivalry “occurs when the services, each following its own interests and ideology, compete within DoD [or the IC] for peacetime roles and wartime missions—and thus for resources—that they believe accrue to their unique strategic approach to war fighting.”

Interservice rivalry becomes most prominent when a new mission area emerges in which none of the services have a dominant advantage, or an old mission may be

---


reopened for competition between the services. According to this model, innovation is not attributable to any external factors—instead it is an internally generated phenomenon through competition over scarce resources or future potential funding. New missions, technologies and threats create new sources of funding, and generate new imperatives to develop a program that fulfills that new need. To Jack Snyder, Interservice rivalry is also identifiable through the doctrinal choices made by military institutions that best serve military interests in bureaucratic battles over resources or organizational prestige.

Furthermore, according to Zisk, who straddles Interservice rivalry theories in her writing, “Routine” innovations (within-paradigm incremental improvements to existing military technology or tactics) are valued by military bureaucracies because they typically assure an increase in military budget and the continued importance to the state of military expertise and the military instrument in international affairs. The leading studies in the area are attributed to Harry Sapolsky, Henry Armacost and Owen Cote Jr., each of whom focused on the development of strategic weapon systems.

Harry Sapolsky concludes that the competition between the services regarding the development of nuclear ballistic missiles resulted in more rapid innovation. Sapolsky examined the development of intercontinental ballistic missiles (ICBMs) during the Cold

137 This restatement of Interservice rivalry theory is drawn from Nina A. Kollars, “By the Seat of Their Pants: Military Technological Adaptation in War” (PhD diss., The Ohio State University, 2012).
War—specifically how the US Navy’s Polaris submarine-launched ballistic missile (SLBM) system development and fielding was influenced and managed as a result of competition with the US Air Force’s Minuteman ICBM. Sapolsky recognized that nuclear missile systems were in some ways “green field,” and outside of each of the services’ core competencies but within the perceived, organic extension of its mission area, which drove competition. The weapons system development schema was indicative of incremental innovation.141

Henry Armacost identified a specific alignment of external advocates and politically driven bureaucratic dynamics that drove the pursuit of differing strategies adopted by the Air Force and the Army in their development of the Thor and Jupiter intermediate-range nuclear missiles (IRBMs).142 Each service branch pursued a separate strategy to achieve nuclear mission area dominance while developing a within-paradigm incremental technological innovation. Armacost describes how the Army sought to accelerate its Jupiter technological development program, delay an interservice decision as long as possible, and develop a doctrine for using nuclear weapons in tactical and operational roles. The USAF, in response, also accelerated its Thor missile program and attempted to achieve bureaucratic dominance over the entirety of nuclear weapon platforms through centralized control.143

---

Owen Cote Jr. examined the sources of military doctrine and concluded that regardless of where doctrinal change originated (whether through civilian intervention or an internally derived process), ultimately doctrinal choices are made because they best serve military interests in bureaucratic battles over resources or organizational prestige.\textsuperscript{144} Cote examined issues of military innovation by conducting a case study related to the development of Polaris and Trident II Submarine-launched ballistic missile (SLBM) programs over several administrations. Cote argued that interservice rivalry can “accelerate doctrinal change begun as a result of civilian interventions or [emphasis added] emerging new combat arms within the services.” Additionally, Cote identified that Interservice rivalry can act alone and independently to cause the creation of innovative doctrine.\textsuperscript{145} Cote compared and contrasted Posen and Stephen Rosen’s writings, and in many respects splits the difference between the two theories. Cote notes that neither Posen nor Rosen address “the potential explanatory power of different patterns of interservice relations as an independent or intervening variable.” He identifies interservice rivalry (conflict) as a separable independent variable, whereas it was treated as an intervening variable by Rosen. Furthermore, Cote notes that there are both cooperative and competitive patterns of interservice relations, and the source of these different patterns may be attributable to external systemic pressures or internal organizational dynamics. Cote also allows for instances where civilian influence on the


manner in which innovative doctrine is ultimately created can be impacted by a domestic political level of analysis.\textsuperscript{146}

**Intraservice Rivalry**

The Intraservice model of military innovation focuses on the internal competition between branches of the same military service and new branches that embrace new military capabilities.

The leading proponent of the intraservice rivalry model is Stephen Rosen, who observed that the pathway to innovation begins when senior leadership develops “a new theory of victory, an explanation of what the next war will look like and how officers must fight if it is to be won.”\textsuperscript{147} Rosen argues that military innovation is a slow internal process, stretching across a generation, as young officers align with protective mentors and work their way up the hierarchy to assume senior positions and foment desired change.\textsuperscript{148} This theory directly rebuffs the civilian–military theory, which cites a variety of drivers for innovation, including previous defeat in wartime, civilian intervention or the overall threat environment, which according to intraservice rivalry is not necessary to produce innovation in a military organization. Even predoctrinal choices are not made explicitly for bureaucratic purposes: Instead, what might be taken as predoctrine is actually one or more senior leaders developing a new theory of victory, what it will look like and how it would need to be fought that generates a coupling between newly


emerging military capabilities and the new theory of victory. This theory also challenges the assumption of the Interservice model that each service behaves as a unitary actor.

According to Rosen’s analysis, the creation, adoption, utilization and assimilation of an innovation “requires a very specific alignment of service leaders, mid-level officers, and institutional arrangements” to be successful. These innovational concepts typically result in an internal, ideological struggle within the service that ultimately requires advocates, allies and resources to become a reality.149 Rosen observes that an internal organizational struggle which leads to innovation may require a new promotional pathway to senior ranks to ensure incorporation of new skills (e.g., people with a technical specialty who might not typically make general officer). Posen’s mavericks do not have this power and civilians are not entirely seen as legitimate enough to influence these decisions according to Rosen, although civilians can protect military innovators against some internal and external opposition.150

Rosen’s theory is typically referred to as a two-step process innovation model. His analysis separates innovation into peacetime, wartime and technological typologies within the intraservice rivalry theory. Rosen’s work investigates a “new way of war, with new ideas of how the components of the organization relate to each other and to the enemy, and new operational procedures conforming to those ideas. They involve changes

in the critical military tasks, the tasks around which warplans revolve.” Rosen does not specifically address how technological innovation occurs within his analysis.

**How Do Major Military Innovations Occur?**

In the previous section, the examination of mainstream theories and the associated case studies provide explanations as to why MMIs are created. However, the previously discussed theories do not examine the details of how these innovations actually occurred. Traditional MMI literature simply does not explain the details of how a MMI is created, nor do they satisfactorily address the product, processes and operational advancements necessary to create a major military innovation. Product innovations involve making changes to create a new, redesigned or substantially improved good or service that incorporate new components, materials or desirable functions into an existing product. Process-based innovations, which are changes in management techniques and organizational structures, are also essential to explaining MMI development, as are operational innovations, which refer to changes in employment techniques for new and/or existing technologies. These explanatory elements are also somewhat similar to the definition of a MMI offered by Krepinevich, which involve technology change, systems development, operational innovation and organizational adaptation discussed in Chapter 1.

The managerial science and revolution in military affairs bodies of literature have recently focused on the management of sustaining innovations and disruptive

---


innovations. Sustaining technologies are innovations that incrementally improve performance of established products. Disruptive technologies are innovations that result in worse product performance, at least the near term, because they have a different value proposition that initially underperforms established products until they eventually become the dominant technology over time. Two frameworks that address the management of technological innovations will be used to examine and test certain hypotheses related to how computer network operations developed as a MMI. One framework will address an approach to sustaining innovations, while the other will address the approach to disruptive innovations.

**Evangelista Model of US Technological Innovation**

Matthew Evangelista applies the mechanics of Rosen’s two-step innovation process to explain how major military innovations occur within an organization. Technological innovations involve weapons “that portend major organizational changes, reallocation of resources, possible diminished organizational autonomy, [or] significant changes in strategy.” Evangelista’s model of the U.S. technological (weapons) innovation is a four- to five-stage internal process: (1) technocratic initiative (innovation), (2) consensus building (within the community), (3) promotion (within the armed services, Congress and the Executive branch), (4) open windows (leveraging of external threats) and (5) high-level endorsement from within the military coupled with funding. Evangelista observes that the innovation adoption process will be smooth if the technology is within the traditional mission space of the originating organization, but if

the technology is disruptive to a traditional mission view, internal opposition may develop. Evangelista further argues that when these internal difficulties occur it is necessary for a military service to point to external events (changes on the international stage) to justify adoption and utilization of the new system or technology.\textsuperscript{154} While Evangelista’s model and case study analysis are helpful to broadly describe distillable elements for sustaining innovation development, they are not sufficiently useful for casual analysis, and will not be analyzed in Chapter 7. His model is instead compared against Hayden’s Christensen’s work in Table 1 in the section below to highlight the differences between the predictive elements of sustaining innovation and disruptive innovation.

\textit{Christensen Model of Managing Disruptive Innovation}

Christensen identified three ways successful managers facilitate the creation and/or development of disruptive technologies: (1) Acquire a new organization whose processes and values are a close match with a new task.\textsuperscript{155} (2) Try to change processes and values of current organization. (3) Separate out an independent organization and develop new processes and values required to solve a new problem.\textsuperscript{156}


\textsuperscript{155} Since acquisition of a new organization whose processes and values are a close match with a new task is highly unlikely to be applicable to the US government, this method will not be addressed any further.

Christensen concludes that changing organizations locked into their current processes and values requires a champion with sufficient power and prestige within the organization to overcome or reform institutional impediments in order to adopt a disruptive technology.\textsuperscript{157} Trying to change the processes and values of the current organization is difficult and rarely successful; Christensen describes a case where “heroic efforts” were needed to overcome institutional impediments within a current organization.

Christensen identifies that innovation will require changing organizational structures\textsuperscript{158} and stripping out counterproductive legacy processes that produce diminishing returns.\textsuperscript{159} Christensen implicitly recognizes that organizational processes are a result of effects derived from both the configuration of an organizational structure and the values of a particular organizational culture. The synergistic effects resulting from the intersection of a current organizational structure and an existing organizational culture tend to perpetuate a type of institutional value system that impacts both work processes and the internally perceived benefits of these processes. Existing processes, while seemingly neutral, can have certain value judgments embedded in them and therefore have a deleterious effect on accomplishing a new mission.\textsuperscript{160}

\textsuperscript{160} Recently, Peter Dombrowski and Eugene Gholz sought to make Christensen’s theory more testable by improving the classification of innovations along a single determining factor: whether the innovation
Christensen states larger organizations were more successful in the creation or development of disruptive technologies when they placed new developmental projects in a small spin-off organization or in a new component small enough to get excited about small opportunities and small wins. To achieve innovation, managers needed to pull relevant people out of an existing organization and create “heavy weight teams” to achieve their new objective, which entailed drawing a new boundary around the group. While utilizing some of the resources of the primary organization to foster the innovation, managers were careful not to leverage its existing processes or values. Furthermore, the managers recognized organizational boundaries are often drawn to facilitate the operation of present processes but impede the creation of new, innovative processes designed to cut across these boundaries.

Terry Pierce leverages Christensen’s model to examine internal factors driving military innovation. The central proposition of Pierce’s study focuses on how military leaders can manage disruptive innovation. Pierce and Christensen essentially identify the same main factors in their innovation models, namely the need for small groups to be created with leadership top cover; however, Pierce adds some additional elements that he improves performance that is measured in traditional ways or in new ways, positing that disruptive innovations offer new performance metrics, while sustaining innovations offer improvements along previously established performance trajectories. This approach was in response to their observation that Christensen conflated cause and effect by utilizing the definition for disruptive innovations as those in which incumbent firms lose out in the post-innovation competition. As CNO is an emerging MMI, and continues to be significantly classified, metrics are not publically available, and therefore not testable under this reworked schema (Peter Dombrowski and Eugene Gholz, “Identifying Disruptive Innovation: Innovation Theory and the Defense Industry,” Innovations 4, no. 2 (2009): 101-117).

His approach is based on a combination of Rosen’s intraservice rivalry model, Henderson and Clark’s architectural innovation theory, and Christensen’s disruptive technology management model (Terry Pierce, Warfighting and Disruptive Technologies: Disguising Innovation (London, UK: Routledge, 2004)).

That is, once military leaders identify that the innovation is disruptive in nature, which is not always a given.
believes must be addressed to ensure success. Pierce’s application of Christensen’s theory leads him to recognize that disruptive military innovation is the combination and integration of technological and doctrinal change, the elements of which can be modest, and ultimately more than the sum of its parts, due to new linkages between constituent technological and doctrinal components which are applied in a new, more powerful way. However, to achieve this type of integrated disruptive innovation, the activities must be disguised or promoted by its internal champion as a sustaining innovation to avoid bureaucratic intransigency or outright hostility designed to stop the changes from occurring. Pierce’s analysis also states the utility of a disruptive innovation is frequently controversial and in doubt until the moment it is proven in battle, which is consistent with Christensen’s analysis of disruptive technology.

**Summary of MMI Literature**

The review of the literature reveals why MMIs occur, in the context of the differences between sustaining and disruptive innovation (Table 1).

---

163 Pierce’s disruptive innovation framework is based upon five factors: (1) War fighting can be viewed as a set of integrated components linked by an architectural innovation (which consists of both technological and doctrinal elements). (2) Architectural innovation is difficult to recognize, and its underestimation can lead to negative effects. If an architectural innovation goes unrecognized, it can lead to “incumbent technology failure assertion,” where “incumbents who invent a new technology often do not champion a disruptive innovation because they have a difficult time recognizing the new technology is being linked in a novel way.” (3) The pace of sustaining technological processes often exceeds the war fighting performance demanded. (4) When senior military officials create and directly manage small innovation groups, the more likely new architectural linkages will emerge that will eventually define a new disruptive doctrine. (5) The greater the product champions can disguise or shape the disruptive transformation as a sustaining innovation, the greater the possibility the disruptive innovation will survive (Terry Pierce, *Warfighting and Disruptive Technologies: Disguising Innovation* (London, UK: Routledge, 2004)).

Table 1. How Major Military Innovations (MMIs) Occur

<table>
<thead>
<tr>
<th>How MMIs Occur</th>
<th>Type of Innovation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sustaining Innovation</td>
<td>Disruptive Innovation</td>
</tr>
<tr>
<td>Creation of Small Heavyweight Group with New Organizational Boundary</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Change in Existing Values and Processes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Change in Organization Structures</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Contribute to Mission Success Immediately</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Disguising of Innovation Type</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Combination of Tech and Doctrinal Change</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Controversial Until Proven in Battle</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Technocratic Innovation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Consensus Building within the Community</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Promotion within the Armed Services, Congress and the Executive Branch</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Open Windows—Leveraging External Threats</td>
<td>Yes</td>
<td>Maybe</td>
</tr>
<tr>
<td>High-Level Endorsement From within the Military Coupled with Funding</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The literature review also reveals enduring gaps between these different theories (see Table 2). There are five main areas of disagreement among MMI theories:

1. Role of Threat Environment. Civilian–Military Relations theorists believe changes in the threat environment are significant drivers in doctrinal change, while interagency rivalry theorists do not. Intraservice rivalry theorists implicitly recognize the role of the threat environment in the creation of MMIs, which undermines the efficacy of existing doctrine, although they place less importance on its role in fostering innovation.

2. Role of Doctrine. Disagreements as to whether doctrine precedes technological innovation or technological innovation precedes doctrine are evident in all three theories. Civilian–Military relations theorists believe that doctrine precedes technological innovation. Interservice rivalry theorists believe that technology precedes doctrine,
although both elements can co-evolve. Intraservice rivalry theorists believe that technological innovation precedes doctrinal innovation.

3. Role of Civilian Intervention. Civilian–Military relations theorists believe that civilian intervention is essential for innovation occur, especially in the absence of a heightened security environment. Interservice Rivalry theorists believe that conflict may accelerate doctrinal change due to civilian Intervention or there may be no civilian intervention present; interservice conflict can independently cause creation of innovative doctrine or can suppress it. Interservice conflict can cause change more quickly than intraservice rivalry. Interservice rivalry will be most prominent when there is a new mission area with no dominate player. Additionally, interservice conflicts are provoked by one service’s development of a new doctrine, often for use or integration of a new technology. Intraservice rivalry states that the internal entities are mostly immune to civilian intervention into doctrine and are silent on the role of interservice politics affecting doctrine, although the theory recognizes the potential impact and then treats it as an exogenous factor. Intraservice rivalry theorists believe that heightened security risk from changes in the security environment strike at the underpinnings of existing doctrine, causing intraservice conflict and change. Intraservice rivalry theorists believe doctrinal innovations emerge from within military organizations as a result of gradual and evolutionary changes in the internal distribution of organizational power, which determines the hierarchy among competing organizational factions or subgroups, and not from civilian intervention. In fact, if civilians intervene to try to foster innovation to address specific capabilities or intentions of potential adversaries, they will fail.
4. Maverick or Visionary Leader. Civilian–Military relations theorists believe it is necessary to have a maverick military officer assisting civilian executives to change doctrine; however, in their view, the civilians provide the doctrinal vision and direction. Interservice rivalry theories do not rely on a maverick leader or champion to explain innovation. Intraservice rivalry theorists believe there needs to be a visionary leader/internal champion together with a new promotional pathway for younger officers to carry the new vision and theory of victory forward. A predoctrinal New Theory of Victory in the next war is only recognized within Intraservice politics theory; however, ultimately it is driven by technological innovation which is then applied to formulate a new doctrine. The other two main theories are silent on the issue.

5. Resource Scarcity as a Driving Factor. Civilian–Military relations theorists do not directly address resource scarcity as an issue, although perhaps this may be an implicit factor since additional funding resources are typically made available to militaries during heightened threat environments. Interservice Rivalry theorists believe that resource scarcity is a primary issue. According to this view, some variability in the intensity of the rivalry exists due to different civilian management and budgetary allocation styles that effect whether budgets are fixed and presented as a zero sum game to the service components, or fixed but allocated on a relatively equal basis and will impact whether there is conflict or cooperation. Intraservice rivalry theorists do not believe resource scarcity is the main issue; however, competition over budgets and resources are a source of internal conflict as a champion seeks to develop a MMI capability.
Table 2. Why Major Military Innovations (MMIs) Occur

<table>
<thead>
<tr>
<th>Areas of Disagreement Among Theories</th>
<th>Civilian–Military Relations</th>
<th>Interservice Rivalry</th>
<th>Intraservice Rivalry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role of Threat Environment</td>
<td>Important</td>
<td>Minimal</td>
<td>Minimal</td>
</tr>
<tr>
<td>Relationship Between Doctrine and Technology</td>
<td>Doctrine Important; Doctrine Precedes Technology; Geography More Important than Technology</td>
<td>Doctrine Important; Technology Precedes Doctrine</td>
<td>Predoctoral New Theory of Victory; Technology Precedes Doctrine</td>
</tr>
<tr>
<td>Role of Civilian Intervention</td>
<td>Important; Key Integration and Innovation</td>
<td>Moderate</td>
<td>Minimal</td>
</tr>
<tr>
<td>Main Actor Driving Innovation/Source of Conflict</td>
<td>Interventionalist Civilian Leadership Aligned with Military Maverick; Conflict Over Status Quo Versus Externally Mandated Change</td>
<td>Military Service Branches; Heighted Interservice Rivalry for New Mission Space</td>
<td>Senior Military Officer within a Service Branch as Champion; Internal Conflict Over Status Quo Versus New Theory of Victory</td>
</tr>
<tr>
<td>Resource Scarcity</td>
<td>Neutral; Resource Availability Increases During Times of Heightened Threat</td>
<td>Important; Secondary Factor is Organizational Prestige</td>
<td>Neutral</td>
</tr>
<tr>
<td>Illustrated Cases</td>
<td>England, France, Germany and USA during Interwar Period</td>
<td>Polaris, Minuteman, Thor and Jupiter, Poseidon and Trident I during Cold War</td>
<td>Mini Case Studies: The British Army and the Tank, 1914-1918; United States Strategic Bombing Force, 1941-1945</td>
</tr>
</tbody>
</table>

Gaps in Main MMI Theories

This chapter’s comparison of the major MMI theories and the cases they address reveals two significant gaps. First, none of the main theories examined the specifics of how the innovation actually occurred from an organizational change or management implementation perspective. This current research will address this gap by the addition of a model of disruptive innovation management related to how MMIs occur as discussed above, which will be applied against a new case.
Second, none of the theorists have examined the role of intelligence organizations in the creation of MMIs. There may be several reasons for this. Intelligence agencies simply may not have played a significant role in past cases. An argument for this perspective would assert that an intelligence organization would not be involved with major military innovation developments such as the Apache helicopter, aircraft carriers or Polaris missiles, since these are tactical battlefield or strategic weapons. While there would be an intelligence role for targeting, there would not be a role for intelligence in weapons design or ideas for a new theory of victory. This overlooks the important role intelligence agencies play in obtaining information and determining through analysis the nature of enemy plans and intentions, including what weapons adversaries are developing, and providing assistance in creating possible countermeasures or offsetting capabilities, including weaponry that might be developed to regain or attain a tactical or strategic advantage. Similarly, intelligence agencies might also develop enabling technologies, as reportedly is the case for techniques such as data mining and retrieval systems, language translation machines and microwave technology that enhanced the speed of computers.\(^{165}\) Intelligence agencies may also provide an analysis related to the efficacy of various types of new technology implementation strategies that would successfully provide battlefield or wartime victories, or drive the integration of technologies to create a MMI itself, as appears to be the case with armed unmanned aerial systems. Regardless of the perspective, the role of intelligence and the expertise of the individuals in these organizations that might have at least assisted in developing the

technologies and the doctrinal basis for previous MMIs were not taken into account in these studies.

Another type of contribution to MMIs might include the role of intelligence agency threat assessments that impacted the motivation of the military to create a MMI. For example, since Barry Posen believes MMIs are driven at least in part by threat conditions, it would be reasonable to assume he should have incorporated the role of intelligence information as a factor in his theory; however, he did not. Posen treats intelligence as an exogenous variable and therefore outside of the scope of his theory. Steven Rosen did address, for example, the role of intelligence information as part of the feedback mechanism for using and developing radar technologies and strategic bombing effects during World War II; however, it must be stated that this is only one of the over twenty mini-case studies that were examined in his book. Rosen does recognize that the role intelligence agencies play in technological innovations is direct, for example in the development of electronic warfare countermeasures; however, he does not deeply examine the issue. In fact, Rosen asserts that peacetime innovation has proceeded remarkably independent of intelligence about foreign military powers. In fact Rosen specifically states that the role of intelligence in stimulating qualitative changes in military technology has not received attention. In Rosen’s defense, the fact that he did not substantively address this issue in his book may likely be due to the lack of available data and classification issues present as well.

A second alternative competing explanation for this gap in the literature would be if a set of facts existed that indicated that intelligence agencies never tried to create a
MMI or they tried and failed to innovate. There is some evidence that a US intelligence agency did in fact play a substantial role in creating a different emerging MMI, armed, unmanned aerial system, which occurred roughly during the same time frame as the CNO under examination in this dissertation, although the prominence of the role is not quite as acute.166 Furthermore, the role of the Intelligence Community in the development of aerial and space surveillance platforms such as the U-2 reconnaissance aircraft and the Corona photographic reconnaissance satellite has been well established.167 There is no available evidence that the US Intelligence Community tried but failed to create a MMI.

A final possibility for the gap in the existing literature looms large: This is in fact the first time a weapons capability that has resulted in an emerging MMI has been created by the Intelligence Community, a potentially new development in the traditional pathways that lead to creating the tools of warfare.

**Hypotheses**

A number of hypotheses can be derived from each of the major MMI theories. By testing each hypothesis against the case presented in Chapter 3, I will determine which theory has the greatest explanatory power for why and how CNO emerged as a MMI. The following hypotheses (also presented in Tables 3-8) must be answered affirmatively after appropriate evidentiary substantiation to determine the validity of the theory for each case. As part of the analysis of the case study, potentially disconfirming evidence will be proffered when available. Grey cells in the tables identify common hypothesis elements

that overlap across theories. While these elements are important to the theories, they may become of lesser importance in determining which theory has greater explanatory power when applied against the information developed in the case study.

*Civilian–Military Relations Theory as an Explanation for Why CNO Developed as a Major Military Innovation*

To test the validity of the Civilian–Military Relations Theory in explaining MMIs, the hypotheses in Table 3 will be determined to be either present or absent.

**Table 3. Civilian–Military Relations Theory MMI Hypotheses**

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Presence or Absence</th>
</tr>
</thead>
<tbody>
<tr>
<td>The push to innovate was a result of a previous military or intelligence failure.</td>
<td></td>
</tr>
<tr>
<td>A civilian intervention occurred as a result of a demonstration of an adversary’s technology, either through a test or combat use that was sufficiently stark and frightening to shake civilians’ faith in their own military or intelligence organizations’ ability to handle it.</td>
<td></td>
</tr>
<tr>
<td>Evidence indicates a heightened degree of attention was paid by senior civilian officials to a particular area of operational concern within the overall threat environment.</td>
<td></td>
</tr>
<tr>
<td>Pressure was brought to bear by an external civilian organization(s) on the IC or DoD.</td>
<td></td>
</tr>
<tr>
<td>Civilians exerted control over appointment of senior officials who would carry out policies deemed necessary for innovation in this area of operations to address the perceived external threat.</td>
<td></td>
</tr>
<tr>
<td>Civilians changed or modified budget requests submitted by IC or a DoD agency to reallocate resources in order to foster innovation to be applied against the threat they wanted addressed.</td>
<td></td>
</tr>
<tr>
<td>Internal pushback or resistance occurred after a civilian-led external intervention called for an expansion of intelligence areas of operations.</td>
<td></td>
</tr>
<tr>
<td>Evidence indicates that intelligence agencies adopted research and development or applied science policies favored by civilians as a result of their intervention.</td>
<td></td>
</tr>
<tr>
<td>Doctrine preceded technology development.</td>
<td></td>
</tr>
</tbody>
</table>
**Interservice Rivalry Theory as an Explanation for Why CNO Developed as a Major Military Innovation**

To test the validity of the Interservice Rivalry theory in explaining MMIs, the hypotheses in Table 4 will be determined to be either present or absent.

**Table 4. Interservice Rivalry Theory MMI Hypotheses**

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Presence or Absence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources for the services’ primary mission(s) are limited or perceived as being limited.</td>
<td></td>
</tr>
<tr>
<td>Rivalry-based behavior between IC or DoD organizations was driven by concern for current or future mission relevance.</td>
<td></td>
</tr>
<tr>
<td>IC or DoD organizations sought to maintain their current mission and attempted to capture a share of the new mission area.</td>
<td></td>
</tr>
<tr>
<td>IC or DoD organizations came to different conclusions or perceptions regarding the threats they were trying to address, which resulted in different mission need requirements and operational doctrine preferences that substantially influenced or defined how the organization interacted with other services.</td>
<td></td>
</tr>
<tr>
<td>The Intelligence Community leveraged its traditional operating experience and allowed it to expand into a new mission domain, making it less susceptible to external interference.</td>
<td></td>
</tr>
<tr>
<td>Co-option of one IC or DoD organization’s traditional mission space by another organization occurred.</td>
<td></td>
</tr>
<tr>
<td>An evaluation mechanism utilized by senior civilian leadership during an interservice competition led to the selection of a winner based on the perceived effectiveness of one IC organization’s approach to innovation over another’s.</td>
<td></td>
</tr>
<tr>
<td>Technology development preceded doctrine development.</td>
<td></td>
</tr>
<tr>
<td>Technological innovations were largely the product of long-term development projects conducted within or at the direction of the military with important civilian support but without significant civilian direction.</td>
<td></td>
</tr>
</tbody>
</table>

Note. Gray cells identify common hypothesis elements that overlap across theories.
Intraservice Rivalry Theory as an Explanation for Why CNO Developed as a Major Military Innovation

To test the validity of the intraservice rivalry theory in explaining MMIs, the hypotheses in Table 5 will be determined to be either present or absent.

Table 5. Intraservice Rivalry Theory MMI Hypotheses

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Presence or Absence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respected senior military officers formulated a strategy for innovation which possessed both intellectual and organizational components.</td>
<td></td>
</tr>
<tr>
<td>An ideological struggle manifested within a particular IC or service component revolving around “a new theory of victory,” which included an explanation of what the next war will look like and how leaders must fight it if it is to be won.</td>
<td></td>
</tr>
<tr>
<td>A bureaucratic imperative to preserve existing missions and ways of operating attempted to crush the impulse to make technological innovations.</td>
<td></td>
</tr>
<tr>
<td>A conscious effort was made by leadership to empower a small group of talented individuals to operate outside of normal bureaucratic channels to foster bureaucratic change.</td>
<td></td>
</tr>
<tr>
<td>The innovation program was promoted as an evolutionary rather than a revolutionary system.</td>
<td></td>
</tr>
<tr>
<td>Initiating the innovation and bringing it to the point where it provided a strategically useful option was accomplished when money was tight.</td>
<td></td>
</tr>
<tr>
<td>A more decentralized organization was created within the agency that was designed and empowered to create and effectively execute an innovation without the need for organizational changes elsewhere in the agency.</td>
<td></td>
</tr>
<tr>
<td>New career paths were created from within the organization by senior leadership to ensure incorporation of key skills necessary to support the new theory of victory.</td>
<td></td>
</tr>
<tr>
<td>A new distribution of power within the IC or service emerged as a result of an ideological struggle manifesting itself as a new senior leadership rank, billet or command.</td>
<td></td>
</tr>
<tr>
<td>Technology development preceded doctrine development.</td>
<td></td>
</tr>
<tr>
<td>Technological innovations were largely the product of long-term development projects conducted within or at the direction of the military with important civilian support but without significant civilian direction.</td>
<td></td>
</tr>
</tbody>
</table>

Note. Gray cells identify common hypothesis elements that overlap across theories.
The Christensen Model for Creating and Managing Disruptive Technological Innovation as an Explanation for How CNO Developed as a Major Military Innovation

To test the validity of the Christensen model for creating and managing disruptive technological innovation in explaining how MMIs develop, the hypotheses in Table 6 will be determined to be either present or absent.

Table 6. Christensen Model for Creating and Managing Disruptive Innovation MMI Hypotheses

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Presence or Absence</th>
</tr>
</thead>
<tbody>
<tr>
<td>The organization was locked into its current processes and values. Innovation was only accomplished as a result of the presence of a champion (visionary) leader with sufficient power and prestige within the organization to overcome great resistance to change, including elements of internal processes and values.</td>
<td></td>
</tr>
<tr>
<td>Innovation occurred when leadership separated out an independent organization.</td>
<td></td>
</tr>
<tr>
<td>The new organization was autonomous.</td>
<td></td>
</tr>
<tr>
<td>The autonomous organization developed new processes and values required to solve a new problem.</td>
<td></td>
</tr>
<tr>
<td>Innovation was a result of creating a “heavy weight team” to achieve an innovation objective.</td>
<td></td>
</tr>
<tr>
<td>A heavy weight team was created from disparate intra- or extra-organizational departments.</td>
<td></td>
</tr>
<tr>
<td>A new organizational boundary was drawn around the group.</td>
<td></td>
</tr>
<tr>
<td>Innovation is a result of a purposeful change to an organizational structure.</td>
<td></td>
</tr>
<tr>
<td>The purposeful change to organizational structure is directly correlated with creating innovation.</td>
<td></td>
</tr>
</tbody>
</table>

Research Design

Case Method Selection

This dissertation presents a single in-depth multi-organizational case study over a 35-year time period to test hypotheses derived from the theories described above. The case study approach allows a detailed examination of the development of CNO as a MMI and tests a series of theories and models for why and how this development occurred. The
case selection decision was based on an influential case model: An influential case is used to examine and test tenets of a theory to see if the theory has generalizable explanatory power for an atypical case. The decision to use the development of computer network operations as an influential case offers a strong test of the principal tenets of each theory to determine whether these theories still provide strong explanatory power.

The influential case selected, at first glance, appears to invalidate or cast doubt upon a theory due the traditional examination of only military entities. Evidence exists to suggest a significant role of the Intelligence Community in CNO development, and it is important to determine if the same operant factors outlined for each theory that are applied to traditional military organizations and dynamics also hold true for Intelligence Community components. Furthermore, the case under examination is the first instance of a non-military organization creating a weapons system as part of major military innovation. This new phenomenon may have influence on cross-case models of major military innovations, as the civilian-intelligence relations, inter- (intelligence) agency or intra- (IC) agency elements may behave or interact differently, or new drivers or innovation not previously identified or accounted for may emerge. Additionally, this case history will also be examined for the presence or absence of organizational and managerial models of innovation development, which are not currently accounted for under the traditional theories of MMI development, nor are they addressed in the seminal case studies in this field and thus might yield new, more comprehensive insights into why and how all MMIs occur. This case study is not expected to be part of a larger representative sample at this time, although it is possible some of the findings might be
applicable to a larger case population or useable for a cross-case comparison if more
MMIs emerge from the Intelligence Community in the future. The current MMI
population generated from the IC is likely no more than one or two cases in total.  

**Method of Analysis**

This dissertation research was conducted through a small $N$ qualitative analysis. I
utilized a descriptive process-tracing methodology for the case based on both primary and
secondary sources. More specifically, I used a within-case analytical methodology, where
I drew descriptive and causal inferences from diagnostic pieces of evidence based on
documentary and oral evidence that trace a temporal sequence of events. The process-
tracing methodology within this dissertation systematically examined historical evidence
in light of the research question and constituted elements that comprised the hypotheses I
posed in this chapter. As such, I acknowledged the epistemological requirements
embedded in providing a process trace-based explanation required converting a purely
historical account into an analytical explanation expressed in the theoretical variables
identified in my research design. The unit of analysis/dependent variable was the case
itself: The development of Computer Network Operations as a major military innovation
between circa 1982 and 2010. This method also allowed me to engage in an “intensive
study of a case that might fail to fit into existing theory, [and] may provide significant

---

theoretical insights. My research “attempts to uncover what stimuli the principal actors attend to; the decision processes they used to arrive at decisions; the actual behavior that occurred; the effect various institutional arrangements had as part of their decisions and actions; and the effect of other variables as identified on their attention, processing, and behavior.” This line of methodological analysis is supplemented by “attempts to trace the links between possible causes and observed outcomes.” To accomplish this I examined histories, archival documents, interview transcripts, in-person and telephone interviews, assessments of newspaper accounts, government research reports and other sources to determine whether the causal process described in the independent variable (theories) selected for testing were in fact evident in the sequence and values of my selected case. An analysis of the case history was made against a broad set of explanatory theories culled from the literature review above. These theories were used as the independent variables for this study to test the explanatory power of traditional MMI theories in the areas of Civilian–Military relations, Interservice rivalry and Intraservice rivalry to determine which has stronger explanatory power. I then used aspects of three theories to test their explanatory power as to how the MMI identified for case selection developed within the Intelligence Community. The analysis was conducted along theory-confirming and/or theory-informing parameters, which were meant to determine whether

or not the theories under examination provided sufficient explanatory power for the case under review. If the analysis determines the case study strengthens the propositions of the theory, the case will be considered theory informing and will add a new type of case history (Intelligence Community-based MMIs). If the analysis determines the explanations proffered by the theory do not apply or are insufficient to explain this Intelligence Community-based MMI, I sought to provide additional explanatory elements that would further inform the theory with the most explanatory power or provide a combinatorial theory that can best explain the case under examination.175

To determine what best explains why CNO emerged as a major military innovation, the research must identify the presence or absence of Civilian–Military relations, Interservice and Intraservice Rivalries theories in each phase of the case. I created a table of qualitative evidence identified from the sources used in the process trace using a research source-driven triangulation/data convergence method,176 and coded it along a continuum based on the presence or absence of evidence and the strength of that evidence, should it exist. To inform the data triangulation, and data convergence methods, which involved analyzing a research question from multiple perspectives and identifying common themes that emerged from the data collected, I leveraged the histories, archival documents, interview transcripts, in-person and telephone interviews, assessments of newspaper accounts, government research reports and other sources to determine points of convergence and divergence to apply against the theory elements.

176 That is, I analyzed the research question from multiple perspectives to arrive at consistency.
The theory that was determined to be ranked first in relative importance is operant in all phases of MMI development and has the greatest cumulative total of affirmative answers that can be identified from the process trace. Furthermore, to provide insight into how CNO emerged as a MMI, the research must identify the presence or absence of several major drivers of managerial action and organizational factors as described in Christensen’s book *The Innovator’s Dilemma*. The competing theories as analyzed above each make different predictions on the causal processes thought to have taken place in a particular case, although preliminary research indicated that a portion of each theory appears to be congruent with the case histories, as expected. I anticipated sufficient evidence being accessible for process-tracing and congruence testing—and should have the means to reject many of the possible alternative explanations regarding the case history.177

George and Bennett provide a variety of methodologically sound process tracing types in their seminal 2005 text. The category described as “More General Explanation” is the most appropriate technical approach since it allows for explanations couched at a higher level of generality and abstraction, which was preferred for the research objective in this study. Due to the time frames associated with the case as well as the classified nature of much of the potential source material, this method allowed for latitude to provide a “general explanation rather than a detailed tracing of the causal process,” while allowing both micro- and macro-phenomena analyses to be performed depending on the

material available, while not claiming to have obtained or processed all the relevant data that pertains to the cases under examination.\textsuperscript{178} The use of George and Bennett’s congruence approach, which allowed my research to “test, assess or refine a theories predictive and explanatory power,” together with their recommended process tracing methodology, as described above, was the principal methodological approach.

Dependent on the nature of the data uncovered, process-verification and process-induction methodologies have been applied.\textsuperscript{179} The variance space for the case study was based on available chronological and organizational information, as well as the willingness of the participating individuals and agencies to make the data available. In order to ensure candor and reach a level of specificity required to create actionable findings, I offered to grant all interviewees anonymity on an “as requested” basis. As this situation arose, I cited quotations by referring to such interviewees as Contracting Official, Researcher, High-Level Intelligence Community Official, etc., as requested. In addition, I have been assisted by current IC officials through the selective use of unclassified portions of classified documents, worked with archival historians at NSA, and submitted the research for a classification review to ensure the research can be published under George Mason University Dissertation Guidelines. Furthermore, there were limitations to the extent of the data collection that could be accomplished for this case study. Specifically, many facts of computer network operations continue to be classified and therefore it must explicitly be acknowledged that the lack of some specific,

relevant information might affect certain conclusions. The relevant agencies have gone above and beyond the call of duty to ensure that facts as presented here reasonably and accurately represent the historical record within the boundaries of important and enduring national security considerations.

**CNO Case Study**

This dissertation provides a detailed examination of the Intelligence Community’s role in the historical development of Computer Network Operations (CNO) capabilities by the United States from the late 1970s-2010. The project seeks to determine why CNO developed as an emerging major military innovation, and to what extent did civilian–military relations, intraservice rivalry and interservice rivalry impact the emergence of the MMI throughout the case.

The case history is divided into four phases. The case starts with the pre-history of computer network attack, grounded in computer vulnerability analyses conducted by think tanks and the Air Force for US intergovernmental agencies and addresses the strategic impetus and military necessity behind the desired disruption of Soviet Command and Control capabilities. The first phase of development of these capabilities is traceable to the end of the Cold War. The second phase of the case history, from 1992-1996, will focus on the sunsetting of the Air Force Intelligence Command, the subsequent creation of the Air Force Intelligence Agency and the role its leader provided in creating the foundational elements for computer network attack. This time period will also examine the simultaneous emergence of capabilities being developed at the National Security Agency and the stand-up of a new organization at the Central Intelligence
Agency. The third phase of the case history, from 1997-2004, will trace the origins of the Information Operations Technology Center, a truly interagency organization housed at the National Security Agency during the time period where evidence of adoption of the capabilities will be presented, together with additional organizational creations to carry out the new mission. The fourth phase of the case history, from 2005-2010, will document the further adoption, refinement and diffusion of the major military innovation capabilities to the military. The facts of the case history will also be examined to explain how the technology change occurred, what systems development was applied, how it was envisioned to be operational when employed and what organizational adaptations occurred to successfully field the innovation.

**Roadmap for the Rest of the Dissertation**

Chapter 3 provides a brief foundational prehistory of the U.S. government’s identification of computer systems’ vulnerabilities from 1965 to the late 1970s, and early historical development of CNO from 1982-1989. The second portion of the chapter analyzes the 1982-1989 time period in light of the three main theories of major military innovation development to determine why CNO developed as a MMI. Chapter 4 traces the development of CNO as a MMI during the 1992-1996 time period, and then analyzes the case history against the same three MMI theories. Chapters 5 and 6 provide additional historical development information for the time periods spanning 1997-2004 and 2005-2010 respectively, and again analyzes these time periods against the hypotheses developed from Posen, Sapolsky et al., and Rosen in the second half of both chapters. Chapter 7 examines Christensen’s Innovator’s Dilemma against the developed case
history from the 1997-2004 time period to determine whether or not this model provides strong explanatory power as to how MMIs occur. Chapter 8 offers conclusions as to which of the theories for “Why” and “How” offer the best explanatory power based on the analysis of the available history, discusses theoretical implications and future research, and offers a meaningful path forward for the future management of emerging MMIs from a policy perspective. The appendices provide some newly available historically important information that informs the research and findings in this manuscript.
CHAPTER 3. PREHISTORY AND 1982-1989

All warfare is based on deception . . . hold out baits to entice the enemy. Feign disorder, and crush him.
—SUN TZU, THE ART OF WAR, 1.18–20

Prehistory

This chapter provides an overview of the origins of computer network operations from the 1970s through 1989. The identification of an early Soviet digital command and control network during the Reagan Administration led to creation of the Joint Strategic Studies Group (JSSG), an NSA-housed interagency entity that developed early Information Warfare capabilities that are foundational to modern cyberwarfare. The historical record from this time period shows the origins of what are now termed offensive computer network operations (CNO)\(^ {180} \) (computer network exploitation (CNE) and Computer Network Attack (CNA\(_1\) and CNA\(_2\)) developed as a result of a change in thinking inside the combined intelligence/military intelligence communities, coupled with the technical feasibility to do more than signals intelligence interception

\(^{180}\) Today, Computer Network Operations (CNO) is an umbrella term that incorporates Computer Network Defense (CND), Computer Network Exploitation (CNE) and Computer Network attack (CNA). There are two subtypes of Computer Network Attack: Computer Network Attack “sub 1” (i.e., CNA\(_1\)) involves digital actions that have a negative digital effect, such as denial of service, destruction of data, and the like. Computer Network Attack “sub 2” (i.e., CNA\(_2\)) involves digital actions that have a negative physical effect, such as destruction of critical infrastructure. For a fuller description of these concepts see: Department of Defense Joint Chiefs of Staff, Joint Publication 3-13: Information Operations (Washington, DC: Department of Defense, 27 November 2012); Kraig Hanson, Organization of DoD Computer Network Defense, Exploitation, and Attack Forces (Carlisle, Pennsylvania: Army War College Carlisle Barracks, 2009), accessed August 30, 2016, http://www.dtic.mil/cgibin/GetTRDoc?AD=ADA500822; Richard Bejtlich, “Executive Briefing with Retired General Michael Hayden,” FireEye Website, February 29, 2012, accessed August 30, 2016, https://www.fir,eeye.com/blog/threat-research/2012/02/executive-briefing-retired-general-michael-hayden.html.
This approach was combined with knowledge gathered from ongoing vulnerability analyses in computer hardware and software systems that date back to at least the early 1970s. The change in conceptual thinking resulted in the development of “deep penetration” technical capabilities against U.S. adversaries in the 1970s, and eventually led to the concepts of Command and Control Warfare (C2W) and Command, Control, and Communications Countermeasures (C3CM) during the 1980s. In many ways, what are now described as computer network operations were squarely anchored in previously existing military and intelligence thinking and heavily influenced by the developmental history of modern communications and electronic warfare.

---

181 Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.
182 During the Cold War, Strategic Air Command planners built an electronic warfare (EW) plan right into the Single Integrated Operating Plan (SIOP) execution. Penetrating bombers were provided with increasingly sophisticated EW suites, with both active and passive capabilities, and missions were supported by dedicated EW platforms (National Security Agency, redacted author, “The Role of Information Warfare in Strategic War,” Cryptolog 23, no. 1 (March 1997).
183 These activities included “security, military deception, jamming, and physical destruction, supported by intelligence to deny information to the enemy, to influence, degrade, or destroy adversary C3 capabilities and to protect friendly C3 against such actions.” The concept of command and control warfare (C2W) was codified in Department of Defense, “Command, Control, and Communications Countermeasures (C3CM),” DoD Directive 4600.4, Washington, DC, August 27, 1979. Also see Chairman of the Joint Chiefs of Staff, “Memorandum of Policy (MOP) 185, Command, Control, and Communications Countermeasures” (December 20, 1983). MOP 185 phrased the goals of C3CM as being: “to deny enemy commanders effective command and control of their forces and to maintain effective command and control of United States and allied forces.” See Department of the Army, “FM 100-15: Corps Operations,” Field Manual (Washington, DC: HQ Department of the Army, 1989); see also Department of the Army, “FM 34-1: Intelligence and Electronic Warfare Operations,” Field Manual (Washington, DC: Headquarters Department of the Army, July 2, 1987), which outlines electronic warfare systems thinking, and writings by Kevin P. McGovern, Corps Level Command, Control, and Communications Countermeasures (C3CM) (Ft. Leavenworth, Kansas: Army Command and General Staff College, 1991), accessed August 30, 2016, http://www.dtic.mil/dtic/tr/fulltext/u2/a242346.pdf. The application of C3CM can be seen as part of the development of a body of literature that grew during this time frame through the senior service war colleges. These writings fell into the general category of Command and Control warfare, electronic warfare, electronic countermeasures to electronic warfare and counter countermeasures for electronic warfare.
184 Electronic warfare components, which can be passive or active, can be described as:
1. Denial of service, which includes jamming, mimicry and physical attack.
2. Deception, which may be targeted at automated systems or at people.
3. Exploitation, which includes not just eavesdropping but obtaining any operationally valuable information from the enemy’s use of his electronic systems” (Ross J. Anderson, Security Engineering: A Guide to
included the development and use of radar systems for tracking and targeting enemy assets including critical communications nodes.\textsuperscript{185}

In the second part of this Chapter, the case history for the 1982-1989 time frame is examined against the hypotheses of each of the main MMI theories. Stephen Rosen’s theory of intraservice rivalry is most congruent with the somewhat limited historical record available for CNO development during this time period.

\textit{Identification of System Vulnerabilities: 1965 Onward}

The ability to compromise, corrupt or steal data from computers was a concern in the US government during the 1960s. Indeed, as early as 1965, NSA possessed internal computer networks and realized that security may be an issue.\textsuperscript{186} Various hearings and studies regarding computer vulnerabilities were conducted by the US House of Representatives and the Defense Science Board (DSB).\textsuperscript{187} A DSB report, chaired by RAND researcher Willis H. Ware (a member of NSA’s Scientific Advisory Board),\textsuperscript{188} concluded that: “Contemporary technology can provide a secure system acceptably resistant to external attack, accidental disclosures, internal subversion, and denial of use.
to legitimate users for a closed environment (cleared users working with classified information at physically protected consoles connected to the system by protected communication circuits); and contemporary technology cannot provide a secure system in an open environment, which includes uncleared users working at physically unprotected consoles connected to the system by unprotected communications.”

As early as 1972, a seminal U.S. government study (known today as the Anderson Report) recognized that a “major threat to [open] systems is…external penetration, [which]…is countered by using combinations of physical, procedural and communications security techniques.” The study group recognized that open computer systems provide a malicious user a “unique opportunity for attempting to subvert” the systems through rewriting the computer’s programming. This capability, “coupled with the concentration of the application (data, control system, etc.) in one place makes computers a uniquely attractive target for malicious (hostile) action.” The authors of the report recognized the difficulties in providing technical computer security due to a combination of factors which included the design of the hardware and software, which was considered “totally inadequate to withstand malicious attack,” the assumption being that these systems would operate in a benign environment and inadvertent but serious design and implementation flaws exist that can be exploited by individuals with

---


Furthermore, the authors determined that “if control of a node can be exercised by a malicious user, the entire network may be compromised, limited only by the level of programming a malicious user could perform. Moreover, there would not be any technical impediments for an attacker to gain “unauthorized access to [classified] data by exploiting a pre-programmed weakness due to careless design or implementation,” or “planting a ‘trap door’ in the application or in the programming and operating systems supporting the application, or inducing a targeted system to accept and install a trap door modification to its operating system…and leaves the practicability of analyzing the computer system for trap doors in doubt…” The report concluded that in absence of efforts by the government, there would be “little hope that spontaneous efforts will provide the technology needed. The situation will become even more acute in the future as potential enemies recognize the attractiveness of (government) data systems as intelligence targets, and perceive how little effort is needed to subvert them.” According to a DoD historian, “the Anderson Report study group included personnel from NSA and CIA. After serving on the study group, they went back to their parent organizations and recognized potential security issues and potential exploitation possibilities. As a result, the IC essentially spent the 20 years (1972-1992) on the proof of concept for computer network exploitation.”

194 Department of Defense Historian, name withheld upon request, interview by the author, Maryland, May 22, 2015.
By 1979, NSA recognized that any computer system could be penetrated by a knowledgeable user and set out to examine seven types of operating system vulnerabilities and seven types of penetration techniques.\textsuperscript{195} In an internal NSA article published in \textit{Cryptolog}, the author recognized that the choice of penetration techniques would depend on the end goal—either obtaining “information or system degradation”—and highlighted the use of utility programs, spoofing the system, use of Trojan horse programs within an utility program, wiretapping (connecting a “passive” listening device “between a peripheral device and a computer’s central processing unit”), between lines entry (“similar to wiretapping, except the process is active,” where a penetrator “enters spurious commands onto communication lines” while the computer terminal is idle), clandestine code (possible insertion of Trojan programs in the computer operating systems), and masquerading, “which involves logging into a computer system as a legitimate user whose account and password have been acquired by begging, borrowing or stealing.”\textsuperscript{196}

\textit{A New Type of Special Means in Warfare: 1982-1989}

According to Admiral William O. Studeman,\textsuperscript{197} the development of computer network attack capability was a result of a joint NSA and US Navy endeavor during the


\textsuperscript{197} Admiral William O. Studeman has held positions as the Commanding Officer, Navy Operational Intelligence Center, 1982-84; Director, Long-Range Planning Group, and Executive Director of Advanced Technology Panel of the Chief of Naval Operations Executive Board, 1984-85. He served as the Director of Naval Intelligence, 1985-88, prior to becoming Director, National Security Agency, August 1988–April 1992; Admiral Studeman began his tenure as Deputy Director, Central Intelligence Agency (CIA) on 9 April 1992–3 July 1995 and was Acting Director of Central Intelligence, 21 January–5 February 1993 and 11 January–9 May 1995 respectively.
1970s and ‘80s. This development was an outgrowth of a joint NSA/CIA/US Navy SIGINT program and electronic warfare derived techniques. He described this time period as a renaissance in warfare development that resulted in a complete upshift in the application of “special means” in warfare.\textsuperscript{198} The background to CNO development is both a strategic story as well as a “system of systems” engineering problem.\textsuperscript{199} Vice Admiral Michael McConnell, former Director of NSA and Director of National Intelligence, provided additional insights into the thinking that surrounded the early history of computer network attack capability development. “This was mostly technology driven and for mission enablement. Once the technology is there, then the military will apply it to warfare. From a technology perspective, the services sit on the status quo until they are forced to see or inherently see the value of new technology or capability to their operations.”\textsuperscript{200}

The number one priority of the US Navy during the latter part of the Cold War was anti-submarine warfare with emphasis on the Soviet ballistic missile submarines (SSBNs). This was due to lessons drawn by the Soviets from the Cuban missile crisis, which led the Soviets to add ballistic missiles to their submarine fleet, thus resulting in reduced warning time for any potential attack on the US.\textsuperscript{201} For example, “in 1968 a Soviet SSBN was detected patrolling off Norfolk, Virginia, which positioned these assets inside our decision cycle for our deterrence strategy of ‘mutually assured destruction.’ If the Soviets had reason to attack the US, a launch from an area near Norfolk would allow

\textsuperscript{198} Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.  
\textsuperscript{199} Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.  
\textsuperscript{200} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.  
\textsuperscript{201} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
them to achieve major destruction and potentially take out decision making capabilities by the National Command Authority.”

Consequently, the Navy, as well as major portions of the US Intelligence Community, began to work this problem over the next 20-plus years. In the course of working naval strategy issues, various entities started developing concepts related to Information Warfare: “In the early 1980s the SECDEF decided to put IW coordination capabilities under the control of the Chairman of Joint Chief of Staff with day-to-day oversight by the Director of the Joint Staff.”

Vice Admiral Studeman ascribes particular personnel as contributors to what is now known as computer network operations to several key “main” actors within the U.S. Navy and NSA: Richard L. Haver, Technical Director of the Naval Ocean Surveillance Information Center and the Operational Intelligence Office; Admiral William Small, Vice Chief of Naval Operations; and Joseph Amato, a senior executive at NSA. The Naval work was accomplished via the Advanced Technology Panel (ATP), an Intelligence Community organelle, on behalf of the Naval Technical Board during the 1982-1984

---

202 Admiral McConnell discussed the activities during this time period. “The Air Force spent the more time and money on the Information Warfare concepts and capabilities; the Navy did some programs, and the Army had the smallest effort. The Army approach was more drawn from Air land Battle (Army/Air Force) ‘anti-Fulda Gap’ strategy for Europe and could be applied to tactical or division or corps maneuvers. The Air Force had the most aggressive posture, and sought to impact, degrade or contaminate strategic communications. The Navy was developing similar capabilities, but each Service operated as a separate entity and there was little to no information sharing across the Services. The only coordinating functions occurred through the Secretary of Defense (SECDEF) and his hand was not strengthened until passage of the Goldwater-Nichols Act of 1986” (Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015).


time frame and thereafter. According to a Center for Naval Analysis study, the Vice Chief of Naval Operations and the ATP focused their efforts on the “creation of an ‘anti-SSBN’ strategy both in terms of deterrence and war avoidance, and for war fighting.”

This work was based on continuing intelligence analysis and was supported by a number of other efforts. A study was commissioned and was directed by Rear Admiral W. J. Holland, leader of the Strategic and Theater Nuclear Warfare Division (OP-65), and his deputy, Captain Linton Brooks, assisted by Richard Haver and Captain Manthorpe.

According to Ambassador Brooks, the US Navy had gained access to a special source, which gave the U.S. unique insights into high-level Soviet Navy thinking. Rich Haver, who was part of the Office of Naval Intelligence at the time, interpreted the meaning of the information obtained from the special source. His inferential conclusions relative to Soviet thinking were seen as authoritative, and began to impact what came to known as the US Navy’s Maritime Strategy. Haver, a lifelong civilian intelligence analyst who worked with Studeman on and off his entire career, stated that “a body of information was collected and aggregated over a couple of years, leading the Office of

---

205 Admiral William N. Small was the Vice Chief of Naval Operations (1981-1983) (Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015).


Naval Intelligence [ONI] to make certain conclusions about the way the Soviet Union controlled their strategic forces in the early 1980s.... Some initial briefings from the analysis were given to President Reagan (prior to the Hinckley assassination attempt).”

However, Brooks noted, to make use of the inferences drawn from this information “we needed a flag champion.” The champion was the Vice Chief of Naval Operations Admiral Bill Small (and his Executive Assistant, Bill Studeman).211

Admiral Small and his colleagues, as part of the ATP, were spending Saturday mornings212 working through the meaning of what the special source information meant for the U.S. Navy. The Navy was “preparing to refight the World War Two Battle of the North Atlantic, with a comparable effort in the Pacific Ocean. However, some of the four-star Admirals could not believe anything else about Soviet SSBN (doctrinal) thinking [i.e., a defensive-style bastion posture] because a Navy designed for defensive missions was not what they would have created”213 even though “specific translations of open-source Soviet publications from the Center for Naval Analyses by Brad Dismukes and Jamie McConnell were directly and indirectly confirming US inferences derived from information obtained from the special source.”214 When Admiral James David Watkins assumed command as Chief of Naval Operations in late 1982, he took a strong interest in Soviet nuclear weapons issues, spending an unprecedented (for a CNO) seven

\[\text{footnotes}\]

212 Brooks noted that the ATP in and of itself was an important organization wrestling with an objectively important issue: He cited the typical difficulties of engaging in serious discussions on a sustained basis around one central issue with a concerted group of senior leaders. Even so, Bill Small was a flag officer with “enough heft” to accomplish this. “These were enormously busy people with broad responsibilities, making the amount of time they devoted to this remarkable” (Ambassador Linton Brooks, interview by the author, Washington, DC, November 23, 2015).
hours in briefings to get up to speed on an issue with which he did not have a deep familiarity.\footnote{Ambassador Linton Brooks, interview by the author, Washington, DC, November 23, 2015.} According to Brooks, “Haver and the ATP were examining the overall Navy strategy in light of the information from the intelligence insights we gained, which led to an understanding that the Soviets would use much of their Navy to establish defensive bastions near their coasts in order to protect (the Soviet term was ‘provide combat stability to’) their SSBNs. This in turn led to war plan changes that involved sending submarines into the bastions early in the conflict—my assessment is that only a handful of us were looking at nuclear deterrence.”\footnote{Ambassador Linton Brooks, interview by the author, Washington, DC, November 23, 2015.} Brooks described the time period as a fairly harmonious decision-making process devoid of mavericks and with definitive champions for top cover.\footnote{Ambassador Linton Brooks, interview by the author, Washington, DC, November 23, 2015.}

As the ATP deliberated, a small group of mostly O-6 level officers ("with a couple of O-5s and civilians sprinkled in") who supported the three-star flag officers also began to discuss the operational implications of the information. This group of highly talented individuals, which included Rich Haver, became to be known as the “Breakfast Club.” CNO Watkins tasked the Breakfast Club to develop disruptive options for the Joint Chiefs of Staff to change Soviet perceptions of what would occur at the brink of war and change their decision calculus.\footnote{Ambassador Linton Brooks, interview by the author, Washington, DC, November 23, 2015.} At the time there was an intellectual current in the Navy that revolved around attacking ballistic missile submarines prior to launching their
nuclear missiles—Brooks thought the ideas being considered for attacking these submarines as destabilizing—for example, one of these ideas was to create high-speed underwater rockets to destroy nuclear capable submarines before they launched their payloads, and sought to stop the Breakfast Club from putting forward the option. One of these options was related to Soviet Command and Control.\(^{219}\) Soviet (Naval) command and control was influenced by what Soviets called radio electronic combat, which emphasized the importance of both denying the enemy the use of his electronic systems and of protecting Soviet systems from disruption. “The REC has broader application than the Western notion of electronic warfare (EW). They regard REC as a fundamental principle of modern electronically dependent warfare and vital to the success of naval operations.”\(^{220}\) While the open source historical record is sparse, one possibility is that

\(^{219}\) Captain Brooks was not invited to become a member of the Breakfast Club initially; “he actually ‘muscled his way in’ after he got wind of the ideas being formulated. Upon becoming part of the group, his mind was changed as a result of some new insights provided by the participants…and he became involved in a ‘whole bunch of other things; Brooks indicated that some of Breakfast Club’s efforts didn’t come to fruition as Admiral Watkins’ tenure as CNO ended, however the work of the group did effect the reorienting of the US Navy to what is now known as the Maritime Strategy” (Ambassador Linton Brooks, interview by the author, Washington, DC, November 23, 2015). See also John T. Hanley, Jr., “Creating the 1980s Maritime Strategy and Implications for Today,” *Naval War College Review* 67, no. 2 (2014): 11, accessed August 30, 2016, https://www.usnwc.edu/getattachment/2b962da8-c60f-4916-9a98-86d1dd831b5b/Creating-the-1980s-Maritime-Strategy-and-Implicati.aspx. Bill Owens, a member of the Chief of Naval Operations Special Studies Group (SSG), recalled his time in the small group of 6 officers “as an epiphany”: The overall creation of the new US Maritime Strategy by the varied small groups of “extreme teams” reportedly led Owens (and colleague Art Cebrowski) to conclude that networking all service and allied intelligence, surveillance, and reconnaissance (ISR) capabilities into a system of systems could lead to a decisive information advantage over adversaries (John B. Hattendorf, *The Evolution of the US Navy’s Maritime Strategy, 1977-1986, Volume 19* (Newport, Rhode Island: Naval War College, 2004); Hattendorf, John B., and Peter M. Swartz, eds., U.S. *Naval Strategy in the Late 1980s: Selected Documents*, Naval War College Newport Papers 33 (Newport, Rhode Island: Naval War College, December 2008), accessed August 30, 2016, http://fas.org/irp/doddir/navy/strategy1980s.pdf). Admiral Studeman came to a similar conclusion while he was the head of ONI in 1985: “I had an ‘epiphany that information is power’” (Admiral William O. Studeman and James (Jim) R. Gosler, interview by the author, Ft. Meade, MD, December 2, 2015).

\(^{220}\) Based on the information contained in a now declassified CIA NIE: Central Intelligence Agency, *National Intelligence Estimate NIE 11-15-82/D Soviet Naval Strategy and Programs through the 1990s*,
the US Naval analysis of the Soviet technical approach led to the adoption of specific integrated electronic warfare-based disruption techniques based on applied US SIGINT capabilities levied against the Soviet ocean surveillance system (SOSS) which was designed to provide information on the location, identity, and movements of foreign naval forces, especially those posing a threat to the Soviet homeland or forces. The most important elements in the system are land-based SIGINT stations, space-based electronic intelligence (ELINT) and radar satellites, auxiliary general intelligence vessels (AGIs), and reconnaissance aircraft.221 Indeed, in declassified documents detailing US Naval Strategy, targeting of Soviet SOSS systems was deemed critical to US success.

“The neutralization of the SOSS is extremely important for the success of U.S. and allied air, surface and subsurface naval operations. C3I countermeasures programs and operations are designed to confuse, deceive and disrupt the SOSS, thereby precluding its effectiveness and making the targeting of naval forces much more difficult. Some of the options available to the on-scene commander include force dispersal, emission control, deception, decoys, and the destruction of AGIs and tattletales as well as the neutralization of Soviet C3I nodes.”222

---

The Joint Strategic Studies Group (JSSG) and Special Technical Operations (STOs): 1982-1989

In addition to the activities engaged in by the ATP and the Breakfast Club, as part of an analytic arm focused on discerning Soviet Naval intentions and nuclear submarine movements,223 another key, small group organization named the Joint Special Studies Group (JSSG) was created by the Joint Chiefs of Staff in 1982-83, and drew on NSA and US Naval expertise.

During this time period, the Navy and the IC conducted follow-on operations to confirm the ONI analysis regarding the way the Soviet Union controlled their strategic forces in the early 1980s. The outcomes from the activities and subsequent analyses were briefed to President Reagan, who was fascinated by the results.224 Deputy Director of Central Intelligence Bobby Inman, Secretary of Defense Cap (Casper) Weinberger, Secretary of State George Schultz, Secretary of the Navy John Lehman, Deputy Secretary of Defense Frank Carlucci and Vice President George H.W. Bush were also involved in the briefings.225 Haver noted despite the presence of high-level civilian leadership, there was not any top-down direction from them: These were informational briefings from joint NSA/Navy self-directed efforts.226

A simple question arose in the room after a briefing: “if we have this information, what can we do with it?” Haver recounted that “it was unclear what the United States could do with the information and what was feasible to try to do—this was not something that was previously discussed before and after the acquired information was collected and analyzed.” The decision was made to exploit the information acquired; essentially the conclusion was: “Let’s get on with it and figure it out.” The motivating force behind the decision to try to do something with the information was: “In the future, if something bad happened, i.e. war broke out, how could we ever explain to the American people that we had this information and did not do something with it?”

The activities undertaken were roughly called Information Warfare (IW) at this time, and were focused on Soviet Command and Control. Haver made it clear that “all of this was for deterrence purposes, not saber rattling.” Weinberger gave the mission to Carlucci who in turn gave it to Lincoln Faurer and Faurer turned to Amato—then Admiral Watkins became the operational arm for the mission. Watkins had the strategic ‘so what’ vision.” When the question of expenditures necessary to create an IW program was raised by Cap Weinberger during a meeting, Bobby Inman offered a rough

---

232 Author’s note: This places the discussion in the mid- to late-1982 time period, prior to Watkins becoming CNO, and happening somewhat simultaneously with the ATP efforts (Richard L. Haver, interview by the author, Tysons Corner, VA, December 11, 2015).
estimate of two billion dollars. Weinberger’s unflinching response: “Done! I will find the money.”

Although nominally a DoD-initiated activity, “JSSG was an interagency activity that was based primarily at NSA with representatives from service intelligence components, together with DIA and CIA all source analysts. The Director, NSA (DIRNSA) was the executive agent, responsible for the performance of the work charter.” According to Bruce Berkowitz, the purpose of JSSG was to “determine whether vulnerabilities identified from critical node analysis, such as message intercepts, jamming and signals injection into adversary networks could be turned into a military or intelligence capability.” Haver stated:

At this point in time we realized we were looking at an automated system that was meant to keep the Soviet leadership in control of their forces—basically it was an early digital system, a Soviet-style concept of a network. We understood we had an opportunity to affect the network and affect confidence in the network for deterrence purposes only, not for conducting war, although the idea for using the capability in warfare was always present. It was a major part of any plan, but the desire from the top was that it, along with other things, would deter the Soviets from going that far, by playing on their fears in such a way as to convince them the outcome of any war would be far worse than they could imagine and the West would come through in much better shape because we had penetrated their systems. We believed that if we could disrupt faith in their machines, we could maximize US options and minimize Soviet options.

---

Key JSSG officials in the early years included Lt. Gen Lincoln D. Faurer, USAF (DIR NSA and DIR JSSG), Commodore (and later) Admiral Clark, Vice Dir. JSSG, LTG William O. Odom, USA (Dir NSA and Dir JSSG), Ed Hart, Vice Dir JSSG as well as VADM William O. Studeman (Dir NSA and Dir JSSG). According to Rich Haver, “General Faurer was the moving force behind the project and picked Joe Amato to start up the new organization and gave him top cover. Faurer was intrigued by and engaged in the project. Everyone agreed to populate a new organization, although no one really knew what the organization was…and the organization itself, once formed, had very little structure.” The lead for JSSG at the Pentagon was a naval captain named Jim Julian and included a promising NSA staff member named Mr. William (Bill) Marshall. Haver indicated that the threat environment was the backdrop, but not the impetus for the creation of the capabilities: This was technological opportunism.

Admiral Studeman described the JSSG as “really invented to deal with ‘the material’ and was targeted at deep penetration of Soviet Command and Control capabilities through the application of complete SIGINT, where computer systems were not necessarily the target of interest.” Bill Marshall elaborated a bit more about the

---

240 Bill Marshall was one of the original members of the JSSG and started as an analyst and later managed two different divisions within the organization over the course of his five-year tenure (William P. Marshall, interview by the author, Washington, DC, December 2014; William P. Marshall, email correspondence with the author, Washington, DC, October 2015).
242 With the exception of when computers were a component of a command and control system (William P. Marshall, email correspondence with the author, Washington, DC, October 2015).
JSSG: “The JSSG’s work was focused on strategic command and control measures that fed into operations. NSA K group was the administrative arm.”

Haver stated that “the potential existed to use vulnerabilities for compellence. However, the US recognized that certain vulnerabilities should not be exploited.” Despite this self-restraint, early on “we became worried about the destabilizing effects of this type of approach, however once we thought through the problem and associated frameworks, the problem was deconstructed and operationalized.”

By 1984 President Reagan recognized the risks of IW [Information Warfare] and accepted that a good model existed to move forward, but was concerned about any Soviet reactions and pushed for more elegant intelligence collection to check and double check our analysis. We were trying to change Soviet behavior and thinking on nuclear weapons—this was an allied partner activity as well. The Intel people were worried about giving away sources, but policy leaders wanted this to be allied, both geographically and functionally. The threat environment was the backdrop to this, but not the impetus for the creation of the capabilities—this was technological opportunism. Our leaders understood that this was all due to technological opportunity, but the biggest driver was that they believed they would never be forgiven if they did not take action on the information available to them: “We cannot afford not to do this if war broke out one day.”

According to Berkowitz, the JSSG had its antecedents in “critical node analysis,” part of the US targeting process for strategic nuclear war, which leveraged signals intercepts from the Soviet Union such as intercepted shortwave and satellite communications, microwave links from space and telephonic intercepts.” The Pentagon wanted to turn these one-off operational intelligence-gathering capabilities into a single integrated system that would look to leverage vulnerabilities identified in Soviet

---

244 Richard L. Haver, interview by the author, Tysons Corner, VA, December 11, 2015.
communications systems in the late 1970s. This capability became known as Special Technical Operations (STOs), which is described as a prototype of hacking.

According to published reports, the JSSG was able to model the technical characteristics of Soviet nuclear communication networks (critical nodes and devices), but did not have a silver bullet to ensure the remote disruption of communications, and eventually the program was wound down due to the end of the Cold War. JSSG activities provided key elements for a proof of concept operational capability (and what would later become CNE and CNA)—namely breaking into an information network and disrupting or denying communications on that network.

Haver provided more insight as to the origins of the IW program. The technical approach taken by NSA was based on lessons learned from the WWII-era Battle of the Beams. NSA’s explanation of the new approach led DoD to view the activity through their previous experience, and improperly concluded that the capability was EW jamming activity. NSA explained to DoD that the new IW capabilities were the combination of collection (stealing signals) and execution of action against the beams in real time. Haver stated that “the point of the [IW] activities during this time period was to get the

---

251 Early on in WWI, the German military developed a radio-aided navigational device, known as Knickebein, which was designed to improve night bombing accuracy. British countermeasures to defeat the system were subsequently developed. For more information on the Battle of the Beams, see R. V. Jones, *Most Secret War* (London: Hamish Hamilton, 1978) (Richard Haver, interview by the author, Tysons Corner, VA, December 11, 2015.).
Soviets to doubt themselves—if the US can do this to us, what else can they do? This is a lesson of World War II, which was provided to us by Douglas Fairbanks Jr., whom we consulted with—‘remember one thing, it is easier to convince an enemy he is right than to try to convince him that he is wrong, deceptions that try to change their minds usually fail.’ A number of the WW II Game of the Foxes experts were present telling us what to do and not to do.”

Over time, to coordinate various activities the Air Force Strategic Air Command (SAC) and LANT (Atlantic Command, U.S. Navy) organizations set up a command and control network for the JSSG to link the Joint Chiefs of Staff, unified commands and intelligence agencies with the various STOs known as the Planning and Decision Aid System (PDAS) that is still in use today. Prior to the PDAS being created there was

---

253 Richard Haver, interview by the author, Tysons Corner, VA, December 11, 2015.
254 PDAS technically was not a command and control network; however, it essentially served the purpose as a de facto strategic C2 system in support of Integrated Joint Special Technical Operations (IJSTO) (William P. Marshall, email correspondence with the author, Washington, DC, October 2015).
255 “Col. Ron Knecht, USAF was the brains behind PDAS and served as Project Manager during the first few years in the JSSG” (William P. Marshall, email correspondence with the author, Washington, DC, October 2015).
256 Admiral Studeman indicated that the STO Center had to be invented to support JSSG activities for what is more recently defined as J3 (Operations) and J39 (Information Operations) related program activities (Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015); J3 and J39 descriptors as published by Leigh Armistead, Information Operations: Warfare and the Hard Reality of Soft Power (Dulles, Virginia: Brassey’s, 2004). According to Dana Priest and William Arkin, as of 2011, STOs involve non-kinetic modes of warfare from “classic electronic warfare to the latest cyberwarfare and directed energy techniques. J39 organizations are responsible for all offensive information warfare programs and activities coordinated by the joint staff, but because of its unique handling of Special Access Programs…it is also called on to deal with most compartmented cyber and intelligence operations, with the exception of Special Operations” (Dana Priest and William M. Arkin, Top Secret America: The Rise of the New American Security State (New York: Little, Brown, 2011). Additional information from William P. Marshall, interview by the author, Washington, DC, December 2014. Studeman expanded on the strategic intent behind JSSG activities: “All these concepts were part of an overall strategy: gigantic psychological operation (PSYOP), which included operational deception (OPDEC) and perception management (PM) at all levels against an adversary which was meant to have the adversary mistrust the information upon which they might make military judgments; the applications can be seen in both the Soviet context but also in the Desert Storm context as well. Today this is no longer known as PSYOPs, but has been renamed MISO [Military Information Support Operations]. By 1991 we were able to apply the entirety of these capabilities
“an absolute refusal to share information from one IW (cryptologic) service (element) to
the other.”

257 Haver recollects that Joe Amato set up the PDAS system for IW use. The
system was designed to remove bureaucratic seams, and facilitate fast-moving decision
making and capability execution. By limiting the number of people in the
communications structure, PDAS provided a clear line of decision authority with direct
communications and fostered a seamless integration of intelligence and operations.

258 Questions of statutory authorities to execute IW missions arose as a result of the
new capability. According to Haver, “the Joint Staff struggled with the Title 10 versus
Title 50 authority issues...however, with netwarfare this becomes a distinction without
a difference. The very act of penetrating a network is an attack—the niceties of this were
worked out during the 1982-84 time period. This became a fundamental question, even
then, and for what we now face today for cyber—this type of knowledge and capability,
even though it grew up in the Intelligence Community, becomes a military issue. We had
dozens of meetings on this with CINC’s, the CNO, etc. The issues that come into conflict
are not vitriolic or blatant parochialism, but Title 50 versus Title 10 authorities. Title 10

and concepts into our integrated thinking, but after the Gulf War it slowly started to silo again” (Admiral
William O. Studeman, interview by the author, Severna Park, MD, August 2015). For the update to the
doctrinal change, see Chairman of the Joint Chiefs of Staff, Military Information Support Operations:
Change 1 To Joint Publication 3-13.2 Dated 7 January 2010, accessed August 30, 2016,
Studeman alluded to OPDEC as the equivalent to the Soviet doctrine of “Maskirovka,” and said that “early
on in those days it was not about stealing or manipulating data, this was about using the full spectrum of
IW/IO” (Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015. This
was later put to use in Desert Shield and Desert Storm to make the numbers of people in the decision
process smaller (this group was Secretary of Defense Dick Cheney, Colin Powell, Tom Powers and
Admiral McConnell), who would then communicate with CENTCOM.

259 References Department of Defense’s Title 10 Warmaking authorities and Intelligence Community
activities authorized under Title 50 of the US code and E.O. 12333.
organizations did not have the expertise—the Title 50 organizations did; there was no clear answer; we couldn’t take NSA and make it Title 10 and we couldn’t take a Title 10 mission and make it Title 50—which is two sides of the coin of the same problem—so we made a blended amalgamation.”

Marshall had an insider’s view to the special activities undertaken by the JSSG. From his perspective, the JSSG was controversial because it was a newly forming mission area, which made it susceptible to intra-organizational politics—where money (budgetary authority) and mission statements drive the bureaucracy’s direction. Within DoD, the JSSG special activities were taking a portion of the responsibilities and resources from other mission authorities. At the time, Marshall was acutely aware of the fact that innovative, controversial organizations must demonstrate the value of newly initiated activity within six months or else the program stood a highly likelihood of being (cancelled) killed. Haver recalled that “some people did not like to see NSA as enabling this type of capability. Joe Amato worked this issue in the bureaucracy and isolated people who were a problem to executing the mission responsibilities.”

---

262 “Organizations usually look at these situations as a zero sum game with respect to resources, authorities, and influence. As a result, new organizations such as the JSSG usually need top cover from senior government officials, especially in the formative stages, and have to demonstrate their added value in relatively short order in order to survive and/or thrive. The statement regarding six months was actually an astute observation that Joan Dempsey made to me when I became Director of the IOTC in 1998” (William P. Marshall, email correspondence with the author, Washington, DC, October 2015).
Fortunately for the JSSG and its members, the Joint Chiefs valued what came out of organization, which included technical studies, strategies, and some capabilities.\textsuperscript{264}

During this time frame, Admiral McConnell was a Navy O-6, and Admiral Bill Studeman’s Executive Assistant (EA) during his tenure as Director of the Office of Naval Intelligence.\textsuperscript{265} After serving as Studeman’s EA from 1986-1987, where he regularly stood in for the extremely busy Admiral,\textsuperscript{266} McConnell was assigned to NSA as the Chief of A24 (Soviet Naval Forces Division) from 1987-88. McConnell’s office was located next door to NSA K Group, headed by an Air Force Brigadier General. As far as McConnell could determine, the Air Force Brigadier General had an NSA hat as Chief of K Group and a joint Staff hat reporting to the Director of the Joint Staff to coordinate IW activities and program security management. The focus, when directed, was to develop IW capabilities and to coordinate/conduct IW against the Soviets to degrade or destroy Soviet ability to conduct an attack in case of a crisis.\textsuperscript{267} McConnell, as Chief of A24, was asked to share certain information that came into his possession with the head of K Group to enhance their IW capabilities. McConnell approached his supervisor, the Chief of A2, for permission to share relevant sensitive information. The response was, “Don’t give those bastards anything!”\textsuperscript{268} The response McConnell received from his supervisor did not seem appropriate to him, so he appealed the decision to the head of A Group. Much

\textsuperscript{265} Studeman was Admiral Bobby Inman’s EA when he was Director of Office of Naval Intelligence.
\textsuperscript{266} McConnell provided some additional background to the issue of IW development during this time frame. The Navy “Crypties” were supportive of IW, but were fighting for ascendancy with the general intelligence officers as to who would have the ultimate authority of IW decisions. Ultimately this led to the Crypties being subordinated under the general Naval Intelligence personnel in 1986-87 (John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015).
\textsuperscript{267} John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
to McConnell’s surprise, he received the same response with regard to sharing mission information with K Group. These transactions in 1987-88 had a marked influence on McConnell. He became convinced that any significant IW capabilities needed by the Nation were inherently embedded in NSA and the NSA culture was to never share sensitive mission-related Signals Intelligence (SIGINT) information.269

In 1989, the JSSG was disestablished.270 Admiral Studeman provided a succinct observation when asked about the JSSG and why it might have been wound down: He stated that “NSA does not like special organizations within it.”271 Haver assessed the organization and its legacy: “The JSSG activities were chaotic, ugly and messy—it sounds better than it was able to achieve, although the capabilities got much better by the late 1980s. A lot of pieces from this period still remain and the lessons learned are still alive today, however, a lot of people have never learned these lessons as the people involved have retired—unfortunately a lot of maturity has left the system. What we developed here was never seen as a standalone capability to make deterrence work—it included many other capabilities—we had a matrix of options.”272

The JSSG experience provided Marshall a valuable lesson in organizational stand-up related to new mission areas. He learned that in order to accomplish a transformational

---

269 John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015. After completing his rotation at NSA, McConnell was reassigned as the Director of Intelligence (N2) Commander in Chief Pacific Fleet, 1989-1990 and worked in Hawaii for Admiral Jeremiah. During this time, the Pacific Fleet was achieving “success” in their anti-SSBN mission, and Adm. Jeremiah, who chaired the Navy’s Flag Selection Board in November 1989, was responsible for McConnell’s promotion to Admiral over more senior officers. After completing this assignment, McConnell was reassigned as the intelligence officer for Colin Powell and Secretary Cheney. Admiral McConnell was promoted in rapid succession to a three-star level to take over the DIRNSA position from Admiral Studeman in 1992.


271 Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.

change, leadership must address both technological and organizational reorganization—through the insertion of managerial change agents and value add personnel—and pull them into new organizational circle. “Small (heavy weight) teams of bright talented people focused on a new mission…‘If you build it, they will come.’”273 Admiral Studeman’s experience is similar: “it is usually a small core of interconnected people ‘pushing other people, programs and ideas around’ to achieve a transformational goal. Typically, personalities will emerge around a situation or a topic—these are extreme teams of the best, most talented people with a specifically defined mission. There is usually a collective spiraling up of an idea, opportunities to develop the idea present themselves operationally and soon you’d have a doctrine—the technology comes first, and then the doctrine—Krepinevich is right.”274

As Marshall describes it,

A wide range of DoD and IC organizations were engaged in developing new capabilities; however, the value of these capabilities were not fully realized as they were not well coordinated across the DoD and IC and depended on access to targets which were frequently difficult to acquire and maintain. The sensitivity of the technologies involved also led to highly restrictive compartmentation of capabilities within SAPs and other highly restricted security programs. The result is that those elements which needed to actually use these capabilities for operational purposes had limited visibility into these programs. This meant that operational organizations had a limited ability to incorporate these capabilities into their mission training, planning, and operational activities. The bottom line was that most of these capabilities were rarely used operationally.275

While the work of the JSSG ultimately did not provide the level of certainty in action that was hoped for, Bill Marshall notes that “Folks in forward-leaning programs

---

274 Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.
that are shut down learn a tremendous amount during their activities; while the bureaucracy might kill an organization, they do not kill the people—invariably the members of these forward-leaning projects from the past come back with new technological developments.” In fact, “the JSSG’s work influenced P04, G08, G44, K 15 and K 7 activities as well. It took a village.” See Appendix A for the early organizational history of K 7 and Tailored Access Operations.

CNO MMI Analysis of 1982-1989

Civilian–Military Relations Theory 1982-1989

A review of the case history during this time does not include any evidence indicating pressure was brought to bear by external civilian organizations per se in regard to IW development, although indirect threat environment pressure clearly did exist due to the overall Cold War environment. The indirect pressure included the Reagan Administration’s rhetoric toward the USSR, and the ongoing nuclear arms buildup that continued throughout this time period. Longstanding tensions between the US and USSR clearly led to a variety of US Navy (and other armed service) and IC efforts to analyze and address the Soviet nuclear arms threat. For example, the US Navy’s number one priority during the latter half of the Cold War was anti-submarine warfare with an emphasis on the Soviet ballistic missile submarines (SSBNs), which, due to changes in deployment numbers and tactics, were able to reduce US warning times for any potential attack. As recounted in the case history, one of the off-setting solutions to this threat

was the development of what roughly came to be known as IW, which initially focused on Soviet Command and Control systems.

The push to innovate during this time period does not include a previous military or intelligence failure; in fact, the discovery and detection of the changes in Soviet tactics and the creation of a new command and control system would rightly be seen as an intelligence success. Ultimately the actual IC response to the change in Soviet tactics was the creation of a defensive style countermeasure for warfighting avoidance and deterrence. Posen’s theory predicts that whatever innovation was created would likely be offensive in nature, which is belied by a variety of the facts assembled for the case study during this time period.

Similarly, there is no evidence that external intervention from civilians resulted in internal pushback or resistance after an expansion of intelligence operations was initiated. Instead, it appears the Intelligence Community was galvanized against the Soviet Union and set out to create an IW solution in the interests of national security. Internal resistance at NSA was due to the domiciling of the JSSG and STO special access programs inside the agency, which for internal bureaucratic and cultural reasons was not liked.²⁷⁹ Contrary to Posen’s theory, it was only after these entities created proto hacking capabilities,²⁸⁰ which were shown to be sufficiently stark in their effects, did the civilians take notice and question whether the US was vulnerable to the same methods. The answer to this inquiry was yes, the US was vulnerable as well, and led to efforts to

²⁷⁹ Richard L. Haver, interview by the author, Tysons Corner, VA, December 11, 2015; Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.
address US vulnerabilities over time. Similarly, the acquisition of actionable special intelligence, analysis of that information and the subsequent creation of US proto hacking capabilities targeted against this system were not the result of civilian intervention, as Posen would predict. Civilians intervened well after the fact of the initial capability creation, and only in response to domestic computer network defense concerns.

Although US civilian leadership did control the appointment of senior IC and military officials, these personnel choices had nothing to do with the creation of the MMI at this point in time. These leaders appear to be normally appointed to their organizations and without a civilian intervention agenda designed to generate MMI changes within their organizations. In the course of their organizational duties, self-initiated intelligence collection and analysis performed by NSA and Naval Intelligence was provided to the civilian leadership outlining an intelligence discovery. In response to the implications of these collection and analysis efforts, the civilian leadership asked the IC to craft a solution based on the threat information the officers had presented. This is not evidence of civilian intervention as Posen describes it: Essentially the efforts to create an IW capability were initiated as a result of informational intelligence briefings. The civilians did not intercede in budget requests in a manner that would indicate control of their own objectives, but simply provided support for the capability creation. In fact, the civilian leadership let the IC name a dollar figure they believed would be sufficient to explore and develop a capability to address the national security challenges the Soviet Command and Control system presented. Notionally, this portion of the case history provides evidence that civilians changed or modified budget requests submitted by the agency, but this
modification was in furtherance of a mission plan that was essentially already started and self-generated, and not the result of significant civilian intervention aimed at a recalcitrant bureaucracy.

There is no evidence that intelligence agencies adopted research and development or applied science policies not favored by civilians during this time period, leading to civilian intervention—in fact the exact opposite is true: IW capabilities, which were developed as a result of actionable intelligence information, were favored by the civilians. This provides disconfirming evidence of Posen’s theory as well. Posen believes the role of the threat environment plays a strong role in civilian intervention and the creation of MMIs. This cannot be seen as causative for the case, as a high level of operational concern existed for the entirety of Soviet activities throughout the duration of the Cold War, and as such represents nothing particularly special per se. Undoubtedly, the newly revealed Soviet activities were particularly troubling and plainly required high-level civilian attention. However, these troubling activities were not detected or uncovered by the civilian leadership. The design and purpose of the Soviet Command and Control system was brought to civilian leadership’s attention by the IC and was not generated as a result of top-down mandates or active intervention that compelled the IC or military to engage in a different course of action leading to this discovery.

Posen discusses the phenomenon of (military) bureaucratic conservatism and its inclination toward slow incremental change or, in the worst cases, “routine” intransigent failure to adapt, resulting in the routine suboptimization of strategic initiatives. The specific JSSG efforts to create early IW technical capabilities are definitively not
evidence of bureaucratic conservatism in the Intelligence Community. In fact, 2 billion dollars were requested by the IC/DoD team to develop a special joint program to successfully address the threat uncovered as a result of NSA and ONI’s collection and analysis. Elements of bureaucratic conservatism (reticence) do appear amongst some individuals internally at NSA, who did not see their role as being a part of capability development that might be used for direct warfare, but those personnel were isolated by Joe Amato to ensure the capability development progressed successfully. In this phase of CNO MMI development there does not seem to be routine intransigent failure to adapt quickly to the new technological capabilities resulting in routine suboptimization.

Posen also predicts that doctrine precedes technological innovation. This maxim is not borne out by the case history, and is in direct conflict with Admiral Studeman’s observations that technological development preceded doctrinal development during this time period, as well as generally for CNO.\textsuperscript{281} What did exist during this phase of CNO development was the predoctrinal idea of Information Warfare developed by Rona in 1976.\textsuperscript{282} However, Rona ideas do not directly pertain to the Command and Control Warfare doctrine per se. The role of successful intelligence collection operations seems to inform doctrine creation. For example, it was only after the intelligence pertaining to the Soviet Command and Control system started to be collected, assembled and analyzed in the late 1970s that DoD issued the Command and Control warfare document, in 1979.\textsuperscript{283}

\textsuperscript{281} Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.
Similarly, the Command, Control Communications Countermeasures (C3CM) document was issued in 1983.\textsuperscript{284} This was well after the special intelligence on the Soviet Command and Control system was acquired, the critical nodes of the system were being mapped, findings from the collection and analysis efforts were briefed and leadership decisions were made to develop capabilities against the Soviet systems. The issuance of the C3CM document was simply a codification of what was already in development, a pattern that will repeat itself throughout the case study. See Table 7 for a summary.

\textsuperscript{284} Chairman of the Joint Chiefs of Staff, “Memorandum of Policy (MOP) 185, Command, Control, and Communications Countermeasures” (December 20, 1983).
### Table 7. Civilian–Military Relations Theory 1982-1989 MMI Hypotheses Analysis

<table>
<thead>
<tr>
<th>Civilian–Military Relations Theory 1982-1989</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>The push to innovate was a result of a previous military or intelligence failure.</td>
<td>No</td>
<td>In fact the opposite is true. There was no previous military or intelligence failure driving this innovation.</td>
</tr>
<tr>
<td>A civilian intervention occurred as a result of a demonstration of an adversary’s technology, either through a test or combat use that was sufficiently stark and frightening to shake civilians’ faith in their own military or intelligence organizations’ ability to handle it.</td>
<td>Yes</td>
<td>This dynamic is somewhat apparent in the case history, but it was not a result of an adversary’s test, it was a US test of IW capabilities being developed that highlighted possible US vulnerabilities as well.</td>
</tr>
<tr>
<td>Evidence indicating a heightened degree of attention was paid by senior civilian officials to a particular area of operational concern within the overall threat environment.</td>
<td>Yes</td>
<td>Once the area of operational concern was brought to civilian attention by the IC. However, the briefings were bottom-up informational, not top-down mandates.</td>
</tr>
<tr>
<td>Pressure was brought to bear by an external civilian organization(s) on the IC or DoD.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>Civilians exerted control over appointment of senior officials that would carry out policies deemed necessary for innovation in this area of operations to address the perceived external threat.</td>
<td>No</td>
<td>Although civilians could have exerted control, the senior officials were already in place and not inserted.</td>
</tr>
<tr>
<td>Civilians changed or modified budget requests submitted by IC or DoD agency to reallocate resources in order to foster innovation to be applied against the threat they wanted addressed.</td>
<td>Yes</td>
<td>Although the budget changes were in support of the IC’s internally generated activity. Senior civilian officials asked the IC how much money was needed to develop an offsetting system and the appropriation was granted.</td>
</tr>
<tr>
<td>Internal pushback or resistance occurred after a civilian-led external intervention called for an expansion of intelligence areas of operations.</td>
<td>Yes</td>
<td>An internal pushback dynamic was present although it was not a result of external intervention.</td>
</tr>
<tr>
<td>Evidence indicating that intelligence agencies adopted research and development or applied science policies favored by civilians as a result of their intervention.</td>
<td>No</td>
<td>The exact opposite dynamic occurred: The internally generated R&amp;D and applied science policies were approved of by civilians.</td>
</tr>
<tr>
<td>Doctrine preceded technology.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
</tbody>
</table>
**Interservice Rivalry Theory 1982-1989**

The main tenet of interservice rivalry theory states that conflict between constituent elements is due to resource scarcity—i.e. the resource(s) needed to execute a primary mission(s) are limited or perceived to be limited. A review of the case study during this time period does not show evidence of resource scarcity issues limiting or being perceived to limit the effectiveness of one IC element over the other. Nonetheless, issues of resource allocation and perceived scarcity were an internal concern at NSA. The perception of scarcity arose between two elements: the traditional SIGINT collection directorate and the special project embedded at NSA. The SIGINT (Operations) Directorate feared the new special project, which was specifically established to create a rudimentary IW capability, would draw financial resources away from their mission space. This fear apparently existed despite the infusion of new capital to fund the IW effort.\(^{285}\)

There is also no evidence in the record that would indicate any meaningful rivalry between IC or DoD organizations that was driven by a concern for current or future mission relevance. In fact, according to the interview accounts, NSA/CIA and the US Navy collaborated on intelligence-gathering projects during the late 1970s which led to a successful collation, aggregation and analysis by the Office of Naval Intelligence. This analysis uncovered the proto Soviet digital network and facilitated critical node mapping, which was directly supported by NSA collection and analytic capabilities. Once a decision was made to create an IW capability to address the findings from the initial

round of analyses, another follow-on collaborative interagency effort, known as JSSG, was created and based at NSA. This new organization was led by DIRNSA Faurer and the Chief of Naval Intelligence, Admiral Bill Small, and was organized and staffed by representatives from NSA with members for the service intelligence components, as well as Defense Intelligence Agency (DIA) and CIA all source analysts.\textsuperscript{286} There is no evidence that the IC or DoD organizations involved during this time period actively sought to maintain their current mission space and expand into a new mission area in an adversarial manner as would be predicted by interagency rivalry theory. However, NSA did leverage their existing mission space to expand into the new IW area during this time period (and ultimately, thereafter) due to the fact that NSA already possessed a variety of requisite core technical capabilities and capacities necessary to achieve mission success.

Additionally, there is no evidence that IC or DoD organizations came to different conclusions or possessed differing perceptions regarding the Soviet threat they were trying to address during this time period; their mission was clear: Address the threat through a variety of means, including IW, to influence the efficacy or the Soviet Union’s perceived efficacy of their nuclear weapons capability.\textsuperscript{287} As a result of this unanimity, the IC and DoD did not put forward different mission need requirements and operational doctrine preferences that substantially influenced or defined how the organization interacted with other services. By design, the JSSG, as well as the STO cells, were meant to be joint and interoperative organizations or organelles, and by all accounts functioned as intended.

\textsuperscript{287} Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.
Interservice rivalry theory indicates that technology typically precedes doctrine, and this appears to hold true for this portion of the case history. The intelligence collection concerning the Soviet Command and Control system started to be assembled and analyzed in the late 1970s, and on its face, seems to have at least influenced the DoD-issued Command and Control Warfare document in 1979. Similarly, the Command, Control Communications Countermeasures (C3CM) document was issued in 1983. This issuance appears to have been generated well after the special intelligence was acquired, critical command and control nodes mapped, findings briefed and decisions made to develop IW capabilities to address the functionalities of the Soviet system. In light of the case history, the issuance of the C3CM document appears to be a codification of what was already underway. The ONI and JSSG’s efforts clearly were part of a long-term development project conducted within the Intelligence Community with important civilian support but without significant civilian direction. See Table 8 for a summary.
<table>
<thead>
<tr>
<th>Interservice Rivalry Theory 1982-1989</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources for the service’s primary mission(s) are limited or perceived as being limited.</td>
<td>No</td>
<td>The fear of future resource scarcity was an internal NSA issue.</td>
</tr>
<tr>
<td>Rivalry-based behavior between IC or DoD organizations was driven by concern for current or future mission relevance.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>IC or DoD organizations sought to maintain their current mission and attempted to capture a share of the new mission area.</td>
<td>Yes</td>
<td>Yes, this dynamic occurred at NSA, but this was not an adversarial interagency process.</td>
</tr>
<tr>
<td>IC or DoD organizations came to different conclusions or perceptions regarding the threats they were trying to address, which resulted in different mission need requirements and operational doctrine preferences that substantially influenced or defined how the organization interacted with other services.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>The Intelligence Community leveraged its traditional operating experience and allowed it to expand into a new mission domain, making it less susceptible to external interference.</td>
<td>Yes</td>
<td>IW technical approaches were derived from traditional SIGINT and EW activities and applied against new targets.</td>
</tr>
<tr>
<td>Co-option of one IC or DoD organization’s traditional mission space by another organization occurred.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>An evaluation mechanism utilized by senior civilian leadership during an interservice competition led to the selection of a winner based on the perceived effectiveness of one IC organization’s approach to innovation over another’s.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>Technology development preceded doctrine development.</td>
<td>Yes</td>
<td>Vulnerability analysis performed on ICT and other critical communications nodes led to capability development, and eventually doctrinal development.</td>
</tr>
<tr>
<td>Technological innovations were largely the product of long-term development projects conducted within or at the direction of the Intelligence Community with important civilian support but without significant civilian direction.</td>
<td>Yes</td>
<td>As depicted in JSSG narrative in this section of the case history.</td>
</tr>
</tbody>
</table>

Note. Gray cells identify common hypothesis elements that overlap across theories.
Intraservice Rivalry Theory 1982-1989

A review of the case study during this time period shows direct evidence of respected senior intelligence officers formulating a strategy for innovation that possessed both intellectual and organizational components, consistent with Rosen’s theory. These types of efforts existed within the Office of Naval Intelligence and the ATP during the 1982-1984 time frame, championed by Admiral Small.288 Similarly, during the 1983-1989 time period, the JSSG’s efforts to turn one-off operational intelligence-gathering capabilities into a single integrated system to leverage and exploit vulnerabilities identified in Soviet communications systems289 was driven by DIRNSA Lincoln Faurer and executed by NSA’s Joe Amato.290

Neither the proto IW option created to address the threat from Soviet Command and Control systems nor the JSSG’s mandate to create disruptive capabilities manifested themselves as an ideological struggle over a new theory of victory or how it might need to be fought, although resistance to the new mission did exist at the working and management levels. The NSA-based JSSG efforts faced internal pushback from a small group of SIGINTers who did not want to see the Agency enabling an IW-based exploitation or attack capability. Clearly this faction preferred the comfort of their traditional passive signals intercept mission, which allowed them to avoid the inherent warfighting implications from the IW technical approach.291 However, these dissenters were managerially isolated by Joe Amato to ensure the innovative mission area efforts

288 Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.
went forward unimpeded. Similarly, internal resistance within the SIGINT directorate manifested as an unwillingness to share internal information that was relevant to the emerging NSA-driven IW mission. Further, the JSSG was considered controversial because it was a newly forming mission area, making it susceptible to intraorganizational politics—where money (budgetary authority) and mission statements drive the bureaucracy’s direction. The JSSG was a small group of talented interagency individuals directly empowered to operate as a special organization within NSA to foster technological change. This had both direct and indirect impacts on the bureaucracy, and presented ongoing challenges to NSA culture at the time which was opposed to sharing sensitive mission-related Signals Intelligence. The JSSG was a matrixed special interagency organization that was self-contained, designed and empowered to create an innovative IW capability, although no evidence exists that new career paths were created to support this novel technical approach to warfare, nor did a new IC distribution of power or senior billet emerge as a result of its activities per se.

Similar to the analysis for interservice rivalry, intraservice rivalry theory indicates that technology precedes doctrine, and this appears to be true for the 1982-1989 time period. The intelligence collection regarding the Soviet Command and Control system started to be assembled and analyzed in the late 1970s, and seems to have at least influenced the DoD-issued Command and Control Warfare document in 1979. Similarly, the Command, Control Communications Countermeasures (C3CM) document was issued

in 1983, well after decisions and efforts were already being made to develop capabilities against the Soviet systems. Admiral Studeman’s experience during this time frame patently states that technology precedes doctrine: “it is usually a small core of interconnected people…pushing other people, programs and ideas around…usually a collective spiraling up of an idea with opportunities to develop the idea operationally [that eventually leads] to a doctrine.”297 The ONI and JSSG’s efforts clearly were part of a long-term development project conducted within the Intelligence Community with important executive branch civilian support but without significant civilian direction. While the JSSG’s efforts were clearly innovative, they do not appear to have been promoted as revolutionary for NSA or the IC—rather this was viewed as logical extension of ongoing intelligence collection, the identification and analysis of a problem set and a logical follow-on activity to develop countermeasures for deterrence purposes.298 The fact that it was the beginning of a revolutionary warfighting capability was either not recognized or not promoted in this manner during this time period. Finally, since the JSSG only developed technical studies, strategies and some capabilities,299 together with its limited operational use due to compartmentation and other security-based information-sharing rules that impeded its wider development and use,300 it would be difficult to conclude that the IW development during this time period provided a strategically useful option that was accomplished when money was tight. See Table 9 for a summary.

297 Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.
### Table 9. Intraservice Rivalry Theory 1982-1989 MMI Hypotheses Analysis

<table>
<thead>
<tr>
<th>Intraservice Rivalry Theory 1982-1989</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respected senior intelligence officers formulated a strategy for innovation which possessed both intellectual and organizational components.</td>
<td>Yes</td>
<td>The strategy was formulated by senior leaders resulting in the creation of the JSSG and STO cells.</td>
</tr>
<tr>
<td>An ideological struggle manifested within a particular IC or service component revolving around “a new theory of victory,” which included an explanation of what the next war will look like and how leaders must fight it if it is to be won.</td>
<td>No</td>
<td>Not really, although NSA had small internal ideological struggle in A Group.</td>
</tr>
<tr>
<td>A bureaucratic imperative to preserve existing missions and ways of operating attempted to crush the impulse to make technological innovations.</td>
<td>Yes</td>
<td>The traditional passive SIGINT cadre at NSA was opposed to IW development.</td>
</tr>
<tr>
<td>A conscious effort was made by leadership to empower a small group of talented individuals to operate outside of normal bureaucratic channels to foster bureaucratic change.</td>
<td>Yes</td>
<td>The JSSG was staffed, empowered and created for this purpose.</td>
</tr>
<tr>
<td>The innovation program was promoted as an evolutionary rather than a revolutionary system.</td>
<td>Yes</td>
<td>This dynamic is indirectly evident via the modification of traditional SIGINT and EW approaches applied to create IW.</td>
</tr>
<tr>
<td>Initiating the innovation and bringing it to the point where it provided a strategically useful option was accomplished when money was tight.</td>
<td>No</td>
<td>There is no evidence in the case history that money was tight at this time.</td>
</tr>
<tr>
<td>A more decentralized organization was created within the agency that was designed and empowered to create and effectively execute an innovation without the need for organizational changes elsewhere in the agency.</td>
<td>Yes</td>
<td>The JSSG and STO cells provide evidence of this dynamic.</td>
</tr>
<tr>
<td>New career paths were created from within the organization by senior leadership to ensure incorporation of key skills necessary to support the new theory of victory.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>A new distribution of power within the IC or service emerged as a result of an ideological struggle manifesting itself as a new senior leadership rank, billet or command.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>Technology development preceded doctrine development.</td>
<td>Yes</td>
<td>Vulnerability analysis performed on ICT and other critical communications nodes led to capability development, and eventually doctrinal development.</td>
</tr>
</tbody>
</table>
Technological innovations were largely the product of long-term development projects conducted within or at the direction of the military with important civilian support but without significant civilian direction. | Yes | As depicted in JSSG narrative in this section of the case history.

Note. Gray cells identify common hypothesis elements that overlap across theories.

Introduction

Chapter 4 traces emerging CNO efforts at Air Force Intelligence Agency (AIA), NSA and CIA. The historical record shows AIA, NSA and CIA leveraged lessons learned from JSSG, STO cells, the Gulf War and national laboratory adversarial analysis research activities during the 1980s and early 1990s to develop niche remote access and HUMINT-enabled concepts of operations and computer network exploitation capabilities. The convergence of two factors—the end of the Cold War and the emergence of a networked world during this time period—led to the emergence of a new core competency, what Bill Black later called “cyberology,” which had a close technological relationship to cryptology and whose central activities were “exploitation,” “protection,” and “attack.”

The first part of this chapter provides a detailed history of the developments in computer network operations from the 1992 through 1996. At AIA, Ken Minihan developed and championed a new theory of victory for future conflicts that leveraged a 21st century approach designed to operationalize “Information Warfare” into a multi-intelligence discipline (MULTI-INT) that facilitated both intelligence collection and

301 William B. Black, Jr., “Thinking Out Loud About Cyberspace,” Cryptolog 23, no. 1 (March 1997); Black also noted that NSA was cognizant that “the post-Cold War enemy changed their tactics, techniques and procedures (TTP’s) and the Intelligence Community had to adapt as well.” This lesson was not lost on NSA leadership.
computer network attack. These changes occurred in the early post-Cold War period and shortly after the end of the First Gulf War. Admiral Mike McConnell was named DIRNSA and immediately faced Congress’s cancellation of important NSA-developed JSSG Information Warfare capabilities developed during the previous time. Despite this setback, and drastic cuts in overall funding levels, novel computer exploitation methodologies explored during the 1980s matured into the 1990s concept of Global Network Intelligence under McConnell. These developments facilitated a transformation from passive to Active SIGINT capabilities at NSA during the second half of this time period, fueling Ken Minihan’s new theory of victory. At the same time, commercial Internet expansion provided a simple, high-speed and easy-to-use delivery system to utilize these newly developing capabilities, positioning IW (later to be called information operations) to transform into something new and on a different time scale. At CIA, traditional clandestine activities were revolutionized by the expansion of the cyber domain, shaped by a young analyst’s experience in the 1980s IW STO cell and the influence of a Sandia National Laboratory technologist through applying a hybrid approach to collection known as HUMINT-Technical Operations. CIA’s technical approach to capturing digitally stored information placed the Agency in conflict with NSA’s dynamic collection capability development.

The second part of this chapter examines the case history from 1992-1996 against the hypotheses of each of the main MMI theories. Both the interservice rivalry and intraservice rivalry theories provide strong explanatory power as to why CNO developed
as a MMI during this time period, and can essentially be considered of equal significance based on the coding and weight of the evidence presented.


At the onset of the Gulf War in January 1991, the “US had a near monopoly of sophisticated national intelligence systems, electronic warfare, targeting, command and control, and space systems” which represented, at the time, “the most successful effort to date to integrate command and control, communications, battle management, reconnaissance, intelligence, targeting, and battle damage assessment (C4/BM/RTT/BDA) into a unified and near real-time effort.” Utilizing this intelligence advantage, coalition forces attacked air defense systems, leadership (including command, control, communications, and intelligence [C3I]), and electrical grids to impact Iraqi information flows and nodes. The purpose was to create an “information differential” through the use of satellite and airborne collection systems before and during the war to acquire “electronic intelligence, including the finding and fixing of C3I nodes of all types.” Admiral Studeman, who was DIRNSA during Desert Storm, oversaw NSA’s warfighting support in theater. He recounted, “I directed NSA to destroy whatever part of the target

---


set they could, and herded the rest into a place so that other aspects of US forces could destroy them the targets."\(^{304}\)

Ken Minihan understood the significant impact the C3CM/C2W/C3I technical approach coupled with NSA’s limited but reasonably effective IW capabilities displayed on the battlefield in Desert Storm. However, to his dismay, almost immediately after the cessation of hostilities in Iraq, Chief of Staff for the Air Force Merrill Anthony “Tony” McPea\(^{305}\) (described as anti-anyone who did not fly aircraft in the Air Force) wanted to disestablish the AF Intelligence Command (AFIC), whose constituent elements had provided significant SIGINT and EW support to the Gulf War victory.\(^{306}\) McPeak stated that he did not see need for AFIC to exist (although according to Minihan he provided no other justification for this belief).\(^{307}\) The movement to disestablish AFIC was presented strictly as a budgetary “savings” issue, although as it turns out, McPeak was not “paying the bill,” i.e. responsible for the operational funding from his budgetary lines. This was


perceived as McPeak’s attempt to recraft the Air Force in his own mold; as a consequence, the Intelligence, Communications and Medical Groups were all swept up in McPeak’s directed disestablishment and consolidation activity.308

Believing McPeak’s intent to disestablish AFIC to be a mistake, especially in light of the recent demonstration of US Command and Control Warfare capabilities in Iraq, Brigadier General Minihan pushed back. Minihan made the argument that the consolidation and reorganization being required by McPeak in the post-Gulf War period was an opportunity to mold the AF Intel organization from the version that supported Operation Desert Storm into one that leveraged a 21st century approach which would operationalize “Information Warfare”—changing it to take a multi-intelligence discipline (MULTI-INT) approach. General Minihan indicated that NSA had good technology to exploit the telecom environment in Saddam’s Iraq during Operation Desert Storm; for example, “NSA had active SIGINT and excellent access” (but did not get an opportunity to use it as it was all blown up by jet aircraft), as well as the ability to intercede in the radar tracking systems.” To Minihan, “the lesson learned from Desert Storm was the need to establish access access access!”309 Minihan was persuasive in articulating his vision and, to Minihan’s surprise, McPeak agreed. This decision actually resulted in the newly consolidated and aligned Air Intelligence Agency (AIA) organization being bigger than


the Strategic Air Command (SAC) Intelligence apparatus. Minihan was promoted to Major General by McPeak and sent to Kelly Air Force Base in mid-1993 as the new commander for the Air Force Intelligence Command and director, Joint Electronic Warfare Center, Kelly Air Force Base, Texas. On October 1, 1993, the Air Force redesignated AFIC as the Air Intelligence Agency (AIA). MG Minihan continued on in his roles under the renamed Air Intelligence Agency and Joint Command and Control Warfare Center, Kelly Air Force Base, Texas. As a Field Operating Agency (FOA), the organization reported directly to the USAF Assistant Chief of Staff, Intelligence. For the rest of the 1990s, AIA focused on Information Operations.

The litmus test for the newly forming capability for Information Warfare was the establishment of the Air Force Intelligence Information Warfare Center (AFIWC), one of

---

310 The Deputy Assistant Chief of Staff (DA COS) for the Air Force at the time was very dictatorial, and showed no interest in the details or the new mission-related activities and capabilities of the newly created organization. The only requirement he insisted upon was that Minihan create a badge for AIA. Minihan, who was intent on creating the capabilities to win the next modern war, thought this to be a very minor task; however, he followed the orders, creating a new organizational shield overnight. This became the extent of the DA COS’s directions to General Minihan as he built out the new organization. Minihan related that he had never created a shield before, and the design he developed had four components, while the traditional shields contained three. He was told to redesign the shield (General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015).

311 General Minihan points out that he was elevated into this position by a promotion board filled with flag-level fight pilots, and was selected over other equally ranking fighter pilots for the promotion, which he called remarkable, and a recognition that intelligence officers were now starting to be considered explicitly as part of the warfighting team (General Kenneth Minihan, interview by the author, Washington, DC, November 24, 2015).


two subcomponents within AIA. Minihan describes AIA and AFIWC as the infrastructure of the emerging powerbase for Information Warfare which later was called “cyber,” plus the inclusion of a warfighting center. AFIWC was engaged in research and development (R&D) on new types of weapons for Information Warfare. Minihan was not provided any direction, nor given any requirements from his leadership chain, and he did not impose any direction or requirements on his personnel. After setting these operating conditions, meant to foster creativity, “the troops started coming up with ideas.” Minihan purposefully established a “freeform think tank staffed by 22-year-old repurposed electronic warfare guys; what I wound up creating were ‘demon dialers’ who developed ideas and began to create capabilities for IW. Once these capabilities were demonstrated, requirements would flow from our ops center, warfare center and cryptologic center to create 21st century Information Warfare exploitation tools.”

As the AIA/AFIWC personnel started to develop capabilities and perform demonstrations, their work generated attention from the rest of the Air Force and led to an argument breaking out within the Air Force leadership. This was due, at least in part, to the belief that the term “Information Warfare” was a politically unacceptable description of the efforts AFIWC was developing. From Minihan’s perspective, this was

---

314 AIA was composed of AFIWC and the National Air Intelligence Center (NAIC) at this time. According to an official Air Force history, AFIWC was activated September 10, 1993, combining technical skills from the former Air Force Electronic Warfare Center (AFEWC), the Air Force Cryptologic Support Center’s Securities Directorate and intelligence skills from the former Air Force Intelligence Command due to the realization that the strategies and tactics of command and control warfare which included the exploitation of enemy information systems during Desert Storm could be expanded to the entire information spectrum and be implemented as Information Warfare (Air Force Intelligence Agency Almanac, “Air Force Information Warfare Center,” August 1997, accessed August 28, 2016, http://fas.org/irp/agency/aia/cyberspokesman/97aug/afiwc.htm).


not a battlefield the highest levels of Air Force leadership were accustomed to: AFIWC was leveraging private (telecommunications and critical) infrastructure information and this was perceived as politically dangerous. Questions as to whether to classify the work being performed, and to what level, were beginning to be discussed; concerns about the legality of what was being developed, as well as authorizations and authorities for utilizing this type of capability, were all factors of internal concern within the bureaucracy. These discussions led directly to a decision to change the nomenclature being used from Information Warfare to Information Operations, a term which did not make people angry. This change in terminology also served another purpose: as partial obfuscation for the activities being undertaken.

By 1994, the developmental activities and organizational structure at Kelly Air Force base were now set up in the manner Minihan needed to execute his vision for computer network exploitation development. According to Minihan, as AIA began to successfully develop and demonstrate some capabilities, interagency turf wars began to emerge regarding ownership of the mission space between the Intelligence, Research and Development (R&D) and Communications entities, among others. Principally, this bureaucratic battle was also “fought over who owned the access points”—as Minihan put it—"they were focused on divvying up the pie between the Title 10 and Title 50

---

318 According to Minihan the terminology Information Operations and “CNO” (computer network operations) took 4-5 years to homogenize; see the 1996-97 time frame in this case study for additional information (General Kenneth Minihan, interview by the author, Washington, DC, January 14, 2015).
320 Minihan describes CNO as 90% CNE, 5% CNA and 5% CND, as the difference between exploitation capability and attack capability is nominal (General Kenneth Minihan, interview by the author, Washington, DC, January 14, 2015).
organizational elements.” According to Minihan, this is natural evolution on how intelligence organizations and military organizations behave when there are significant shifts in technological capabilities being created. He described the dynamic inside the Intelligence Community in the following manner: “When budgets get reduced, the intelligence guys get innovative.” He further explained his philosophy regarding the development of innovative technological capabilities: “If it doesn’t satisfy a requirement, it’s a good idea.” AIA under Minihan spent a lot of “time, money, and applied technology” to support this philosophy, which “opened up a lot of new frontiers” in information operations (computer network attack/Information Warfare); however, “I was very careful not to use the ‘I’ word. Over time, our efforts led to the natural inheriting of good ideas up to the mothership,”321 and led to a “further divvying up of the pie” [the pie being tools and/or capabilities] created at AIA.”322 In October 1994 MG Minihan was moved into a new position as assistant Chief of Staff, Intelligence, Headquarters U.S. Air Force in Washington, DC. Eleven months later he was promoted to Lieutenant General and named the new director of the Defense Intelligence Agency (DIA). However, his tenure at DIA ended after five short months due to a phone call.323 The Air Force cryptologic element under General Minihan (AIA) was way ahead of the Navy and Army

321 Washington, DC DoD Headquarters.
322 During this time frame the Navy Information Warfare Activity (1994), and the Army Land Information Warfare Activity (1994) were created and stood up (Michael Warner, “Cybersecurity: A Pre-History,” Intelligence and National Security 27, no. 5 (2012): 781-799).
in developing IW capabilities during this time period. McConnell observed that “Minihan came spring loaded for IW” when he took over as DIRNSA in 1996.  

The former high-ranking DoD official provided some additional perspective for this time period. “In the early 1990s it became clear that we could not control midpoint attack, we had to get to the endpoint. From a communications perspective you have two options: kinetic disruption or non-kinetic (cyber) disruption.”

“In the early days, CNO was largely based on technological opportunity through the use of vulnerabilities that were not widely known. Some of the vulnerabilities were obvious opportunities to disrupt systems that could be easily overwhelmed via DOS or DDOS methods, while other opportunities were related to systems maintenance, ports and backdoors or examination of Open Source Intelligence [OSINT] write-ups on Disc Operating Systems issues.”

Further, “Another part of the approach we took was the recognition there was no such thing as a civilian Internet and military Internet: Most of it is owned by other folks; it is a physical layer that ultimately comes down to a box with electrical signals and a person operating it that is physically located somewhere.” Back in the 1990s, “simple shit” (meaning simple tools or capabilities that are simplistic by today’s standards) was placed in closely held special access programs (SAPs). “Cyber was an ‘odd duck’—we did not know how to treat the capability so we treated it as a weapon system—however, at the time, the technological capability was fragile so we SAP’d it to keep it close hold.” He expanded on the differing approaches between Title 10 and Title 50 organizations in this

---

325 Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
area of program protection: “The reasons why organizations placed capabilities into SAPs are 180 degrees different between DoD and the IC. In DoD, the reason for SAPing is related to the issue of military surprise and done at the starting point of a project. The IC SAPs at the time of the operation, which is much further downstream. Gradually cyber activities became more routine, especially when we took the concept of technology templating and applied to the area. However, we were not organized properly to do this work [cyber], which led to various organizational changes.”

NSA, IW and the Concept of Global Network Intelligence (NSA 1992-1995)

As Admiral McConnell took over as DIRNSA in May 1992 he faced a variety of budgetary cutbacks, driven mostly by the end of the Cold War, recasting relations with a post-Soviet Russia, and a strong domestic agenda set by incoming President Bill Clinton. Specifically, a congressional staff member for Congressman John Murtha was seeking to acquire more money for defense spending in Pennsylvania, and directed McConnell, early in his tenure, to kill the IW Program known as “M.” As Director of NSA, McConnell learned that he was the Security Manager for the Nation’s IW program known as “M.” McConnell, who was well aware of the importance of NSA expertise for effective IW as a result of his tour at NSA, believed this to be a significant mistake, and

326 Technology templating in this context refers to the categorization and analysis of various hardware and software system versions, i.e. IBM PCs running Microsoft 3.0. 3.1 operating systems for exploitation et al.
327 Department of Defense Former DoD Official, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
328 John Murtha, the chairman of the powerful subcommittee that controls Pentagon spending, was dubbed the “King of Pork” for the volume of taxpayer money he could direct to the area around his hometown of Johnstown. Most of the largess came in defense and military research contracts he steered to companies based in his district or with small offices there (Carol D. Leonnig and Martin Weil, “John Murtha Dies; Longtime Congressman was Master of Pork-Barrel Politics,” Washington Post, February 09, 2010, accessed August 28, 2016, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/08/AR2010020802352.html).
went to discuss the demand with his mentor, Colin Powell, who was also aware of the IW programs. Powell, based on his knowledge of the program’s importance, decided to direct a review of the various Service programs to see if a case could be made to preserve each. The review was conducted by Admiral Richard Macke, who was at the time the J-6 Joint Staff and soon to be the Director Joint Staff for Colin Powell. The review recommended disestablishing the Army-oriented portion of the program but keeping the Air Force and Navy program elements intact. Unfortunately, Congressman Murtha was not pleased, and threatened to cut other NSA budget lines if McConnell insisted on keeping the overall security management program. As a result, NSA was forced to defund the M program. McConnell said “the Program didn’t have a strong sponsor,” and NSA institutionally did not like the program since it did not fit in with the bureaucracy’s conception of its traditional mission space. “There was always IW resistance at NSA, who wanted to engage in SIGINT while protecting all sources and methods, which was culturally hard to overcome.” McConnell candidly admits that “I blinked under pressure,” and the program was disestablished.\textsuperscript{329}

Bill Black’s involvement with Information Warfare and the development of computer network attack capabilities had an interesting yet inauspicious beginning.\textsuperscript{330}

One day in 1992 Black attended a breakfast for Duane Andrews,\textsuperscript{331} the Assistant

\textsuperscript{329} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
\textsuperscript{330} Information from this section is drawn extensively from information provided by William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
\textsuperscript{331} Before entering the private sector in 1993, Duane P. Andrews was the Assistant Secretary of Defense, Command Control Communications and Intelligence, and chief information officer from 1989 to 1993 where he supervised the intelligence, security, command and control, telecommunications and information technology programs of the Department of Defense and their approximately $60 billion budget. He directed
Secretary of Defense for Command Control Communications and Intelligence (C3I). Andrews recently authored a paper on Information Operations/Information Warfare, and as he described it to Black, stated “Bill, I have been working on something that your agency doesn’t accept, but it’s very important to you.”\(^\text{332}\) Unfortunately, Black did not know what Information Warfare was—he was too busy closing out European operations for NSA in the aftermath of the fall of the Soviet Union.\(^\text{333}\) Bill dutifully told Andrews that he would look into IW but was going to be very busy as his next task was to reorganize NSA’s Russia- and European-focused collection efforts. After reading the Andrews paper, and with the benefit of hindsight, Black indicated that “the Andrews white paper was an analysis of the oncoming digital world in military terms when no one was recognizing or accepting this in military terms at the time.”\(^\text{334}\)

Soon after Duane Andrews’ discussion with Bill Black, and in the aftermath of the cancellation of NSA M programs, on December 21, 1992, DoD TS 3600.1, a top secret but now mostly declassified document, was issued by Donald Atwood, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)), on the subject of Information Warfare. Information Warfare was defined in

\(^{332}\) William Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.

\(^{333}\) William Black, Jr., interview by the author, Pasadena, MD, May 1, 2015. In the immediate aftermath of the fall of the Soviet Union, NSA needed a reorganization to meet the new the realities of the new international security environment. The organization’s orientation needed to change from what was essentially a single explicitly Soviet-focused effort under the “A Group” to an emerging shift to a multilateral power structure at the international level of analysis. Furthermore, NSA (and other members of the IC) was not organizationally optimized for the rapid changes. For example, NSA had thousands of Russian linguists, and was faced with an explicit difficulty in retraining them for a changing mission space and disparate nation-state focus (William P. Marshall, interview by the author, Washington, DC, December 2014).

\(^{334}\) William Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
TS3600.1 as including “the exploitation, corruption or destruction of adversaries’ information systems through such means as signals intelligence and command and control countermeasures,” and “requires the interaction and the integration of command control, communications (C3), intelligence, information systems countermeasures, and information systems security.” Furthermore, “Intelligence collection against the information systems of potential adversaries shall be afforded sufficient priority to support the Information Warfare requirements of the Department of Defense. The document also called for the procurement of “dual use systems that can be used for both exploit [sic] adversary information systems as well as corrupt those systems [which] shall be acquired whenever practical and cost effective.”

The recently appointed Director of Operations (J-3) for the Joint Staff, a Marine Lt. General, interpreted the issuance of the TS 3600 Information Warfare order as being under his cognizance, essentially asserting, that “the order has war in the title, which means I’m in charge.” As part of the formal attention being given to IW, the services started to seek new mission-related opportunities, and the “Air Force and the Navy rushed off to develop new capabilities,” manifesting a measure of interservice rivalry described by McConnell as “Mine is better than yours, but I will not show you mine.”

---

Furthermore, despite the J3’s declaration, the Joint Chiefs of Staff was not in the chain of command (the Chairman is the Senior Military Adviser to the President and the Secretary of Defense and serves as a communications and coordinating activity for the Secretary of Defense in the execution of his authorities) and therefore did not possess a mechanism to coordinate the efforts of the services, who were now striking out on their own to develop their own, separate capabilities.\textsuperscript{338}

In the aftermath of the NSA M program cancellation, the issuance of TS3600 and the curious MOP 3\textsuperscript{339} created various types of conflicting messages and confusion regarding the future of IW and computer network attack. This would prove to be

\textsuperscript{338} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
\textsuperscript{339} MOP 30 contained the unclassified implementation orders for TS-3600.1. Chairman Powell’s Memorandum of Policy 30 (MOP 30) promulgated a version of IW which, according to interviews and published reports, confused DoD for years. MOP 30 used terminologies that were not delineated in the classified directive and did not bear directly on CNE or CNA developmental activities or use. Supposedly meant to provide joint policy and guidance for IW capability implementation under the rubric of C2W, MOP 30 stated that Command and Control Warfare was “the military strategy that implements TS-3600.1 on the battlefield and integrates physical destruction”; however, the “forces used in C2W are, in most cases, the same forces used to conduct other aspects of warfare.” MOP 30 cancelled the use of the term Command and Control Countermeasures that was successfully operationalized in the Gulf War and codified C2W as “The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict.” This definition does not align very well with “the exploitation, corruption or destruction of an adversary’s information system through such means as signals intelligence and command and control countermeasures,” nor does it provide guidance for the development of IW within the service components. The DoD historian commented that “MOP 30 gutted the Atwood IW directive and confused everyone by changing IW to C2W…the possibility exists that IW was too pie in the sky at this time—more aspirational than real. At the time the concept of IW was driven by science fiction and popular imagination but no one really knew what IW actually was” (Chairman of the Joint Chiefs of Staff (CJCS), “Memorandum of Policy (MOP) 185, Command, Control, and Communications Countermeasures” (December 20, 1983); Michael Warner, “Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014,” The Cyber Defense Review, August 27, 2015, accessed August 28, 2016, http://www.cyberdefensereview.org/2015/08/27/notes-on-military-doctrine-for-cyberspace/; Michael Warner, “What is This Thing Called Cyber? Notes on the Evolution of Thought in the US Department of Defense,” paper presented at the International Studies Association Conference, March 27, 2014; Department of Defense Historian, interview by the author, Maryland, May 22, 2015.
problematic over the years arguing over “who is in charge” because McConnell knew the resident expertise and capability needed for effective IW were housed at NSA.\textsuperscript{340}

Despite NSA possessing the technical capabilities for IW, according to Black, from an internal NSA standpoint, the bureaucracy did not believe they had to prepare for the onset of Information Warfare. SIGINT/Cryptology was something they had to be prepared for: NSA considered Information Warfare as “Not Their Business.”\textsuperscript{341} In fact, NSA would not even participate in the IW meetings and activities.

Although undermined by Congressional direction and the fears or intransigency of the internal bureaucracy, as McConnell settled into the DIRNSA position, he recognized that he “needed the smartest guy I could find to further the IW mission thinking and planning.”\textsuperscript{342} The person was Captain Rich Wilhelm who had served with McConnell as the NSA representative to the J-2 during Operations Desert Shield and Desert Storm. McConnell said, “I pulled him out of his current position at Naval Security Group Activity Misawa, in Japan, named him Director of IW at NSA, and Rich started to put it together.”\textsuperscript{343} Bill Black recollected that during this time frame, NSA’s Information Warfare element had only one person (Wilhelm) the entire time that Admiral McConnell was in charge of NSA.\textsuperscript{344} McConnell, who was intent on consolidating the direct reporting structure at NSA after he took over the organizational reins, decided to reorganize the agency. Faced with 91 direct reports when he became the new Director, McConnell asked a group of seniors and his Deputy Director how NSA should be

\textsuperscript{341} William Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
\textsuperscript{342} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
\textsuperscript{343} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
\textsuperscript{344} William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
configured for the future. Although his staff requested 60 days to accomplish the task, McConnell instead required a one-week turnaround time for their recommendations. He also took on the task himself. When the three plans were turned in, they were almost identical in streamlining the agency. The agreed restructuring also allowed McConnell to embed some changes for the future that would serve not only the interests of effective SIGINT operations but also enhanced IW capabilities.\(^{345}\) Reportedly, NSA Seniors (Senior Executive Service members) would not accept that the signals intelligence world needed to go from passive to active SIGINT collection.\(^{346}\) McConnell recollected that only Bill Crowell, the former head of A Group, who was now the Director of Operations (SIGINT Director), had become a believer in the need to address SIGINT and IW as a global network penetration mission. McConnell would later choose Bill Crowell to serve as his Deputy Director of NSA.\(^{347}\)

McConnell’s recognition that NSA would have to live on the Net was known internally for over ten years, although the changes had yet to be made. In September 1982, in a series of Cryptolog articles entitled “SIGINT 1990,” the SIGINT community at NSA was in effect warned that major developments in telecommunications technology and computer systems during the 1980s would have a profound effect on collection and


\(^{346}\) William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.

\(^{347}\) Richard Wilhelm had a 29-year career in government as a military intelligence officer and civilian appointee, including Executive Director for Intelligence Community Affairs during the Clinton Administration and service on Vice President Al Gore’s national security staff, where he was responsible for intelligence, terrorism, and a range of global national security issues. As a U.S. Navy officer, he co-directed the Joint Intelligence Center for Iraq during Operation Desert Storm and was the first director of Information Warfare at the National Security Agency (Booz Allen Hamilton, “Richard J. Wilhelm,” July 2014, accessed August 28, 2016, http://www.boozallen.com/about/leadership/executive-leadership/Richard-Wilhelm). McConnell later sent Wilhelm to the National Security Council to support Al Gore, and replaced him with Dave Henry who was to work on developing IW policy (Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015).
exploitation capabilities by 1990, resulting in more difficult collection in some cases, while offering more collection opportunities in others. The main technological advances cited in this prescient series of articles were the developments of new satellite systems, optical fiber cables, electronic switching, the coalescence of computers and communication nets, and the increasing complexity of telecommunications throughout the world.\textsuperscript{348} The analyst noted that the “classical ‘passive’ model of signals intelligence collection (SIGINT), which involved sitting back waiting for signals to reach a collection device would no longer be appropriate for the problems of 1990.”\textsuperscript{349} Furthermore, the author stated that “attacks against computer-communication nets, and against systems such as optical fiber, require operations based on physical and electronic penetration of the target links and nets, tightly coordinated with monitoring and analysis, to gauge how well the penetration is doing, and cannot be handled by multiple agencies trying to ‘coordinate’ a mission; the authority and operations must be unified into SIGINT.”\textsuperscript{350}

Part of the technology changes were due to improvements in materials science, specifically glass technology “bringing about a revolution in telecommunications by making landlines cheaper than radio relay or satellites,” thus allowing information to be sent at a much lower cost, in some cases 10x-20x less expensive. The NSA article recognized that many of the technical improvements in “switching, transmission, and security will make it harder for SIGINT to find and exploit the specific traffic that is worth” intercepting, while the “turnover time for equipment will decrease,” thus

\textsuperscript{348} Joseph Meyer, “SIGINT 1990,” Cryptolog 9, no. 9 (September 1982).
\textsuperscript{349} Joseph Meyer, “SIGINT 1990,” Cryptolog 9, no. 9 (September 1982).
\textsuperscript{350} Joseph Meyer, “SIGINT 1990,” Cryptolog 9, no. 9 (September 1982).
shortening the lifespan for certain interception techniques and methods, although SIGINT would “likely have the highest potential growth rate of any intelligence service, capable of the deepest and most extensive penetration into the activities of any target country providing it can be done successfully and is adequately funded.” The series of articles recognized the continued growth in computer manufacturing and the coalescing of computers and communications, including the impacts on “PBXs, interconnections, satellite links, data terminals, and even basic transmission and switches…” as well as the increase in computer memory storage and anticipated reduction in costs to maintain this data.

Additionally, the “impact on SIGINT of the development of transoceanic and overland optical fiber trunks is that traffic which now must go primarily by satellite will disappear onto fiber. Optical fiber will be a preferred transmission medium because it is so difficult to intercept.” The articles were in effect describing the development and growth of computer and communications networks that would one day be globally interconnected. Furthermore, the issue of diseconomies of scale was presented.

---

354 As described and depicted in the November article, “C&C networks consist of a number of components, viz., computers, on-line storage, telecom circuits, switching, software, data bases, terminals, users, and projects or activities that use the C&C net.” Additional elements that helped integrate and move the data included Electronic switching and Packet networks, Digital processing and Communication control (National Security Agency, redacted author, “SIGINT 1990,” Cryptolog 9, no. 11 (November 1982)).
355 Furthermore, the issue of diseconomies of scale was presented: “SIGINT faces the special hazards that the target telecom nets are expanding inexorably in a way that will defeat any small analytic and processing effort…the combination of secret and unknown information, and technical complexity, will force more and more internal coordination—through the ‘unified integrated’ centralized analytic centers. With this combination of an increasing volume of data and greater coordination and decision cost per datum, any mathematical model of the process would explode.” This statement recognized the need for what is now
“SIGINT faces the special hazards that the target telecom nets are expanding inexorably in a way that will defeat any small analytic and processing effort…the combination of secret and unknown information, and technical complexity, will force more and more internal coordination—through the ‘unified integrated’ centralized analytic centers. With this combination of an increasing volume of data and greater coordination and decision cost per datum, any mathematical model of the process would explode.” This statement recognized the need for what is now called big data analytic problems with specialized high performance computing as early as 1982.\textsuperscript{356} In response to these technological changes and potential operational impediments, a solution set was proffered:

As computers become more tightly integrated into telecom nets, the central problems facing SIGINT will become what to target and how. The most useful data, from an intelligence or a SIGINT viewpoint, may be resident in the system in a computer memory, rather than passing over a communication channel. SIGINT, instead of waiting for data to be transmitted and then passively collecting and exploiting them, will have to penetrate into the nets, find what is there, and extract it.\textsuperscript{357}

As a case in point, Bill Black’s interest in computer network exploitation and IW/IO had grown since his introduction to the concept in 1992. According to Black, “only one small pocket at NSA was doing it [computer network exploitation]…‘G Group,’” which was led by Dennis Chiari. “Chiari, who at the time was the Chief of G44, was, in many SIGINT circles, ‘ostracized’ by other elements of NSA due to the internal political/policy view of these activities.”\textsuperscript{358} Bill Black and Denis Chiari started collaborative efforts. Black was still running A Group at the time, and began mandating

\textsuperscript{357} National Security Agency, redacted author, “SIGINT 1990,” Cryptolog 9, no. 11 (November 1982).
\textsuperscript{358} William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
that his analysts go back to school to understand the growing digital domain.\footnote{William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015. The course instructors reported back to Black that more than a few students, upon their arrival, declared “Black made me come here”; years later they personally thanked him for ordering them to learn about the domain of computer network operations.} According to Black, the activities G Group engaged in, which involved penetration into non-US computer networks, were considered compartmented during this time period.\footnote{William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015. In a 1994 Cryptolog, a heavily redacted article entitled “Information Warfare: A New Line of Business for NSA” was published. The article states “One of the new buzzwords in the hallways these days is Information Warfare (IW). IW is defined as the preservation of the integrity of our information systems from exploitation and corruption by potential adversaries while at the same time exploiting and degrading adversary information systems” (National Security Agency, redacted author, “Information Warfare: A New Line of Business for NSA,” Cryptolog 20, no. 2 (July 1994)).}

According to historian Bill Nolte, during the 1993-95 time frame, NSA attempted to address and reconcile the emerging concept of cyberspace and how it would (or would not) fit within NSA’s structures, missions, and authorities. An “active effort [was undertaken], led in large part by the personal involvement of NSA directors John M. (Mike) McConnell and Kenneth Minihan, and involving NSA, DoD, and Intelligence Community personnel, to understand a new and potentially important national security realm.”\footnote{William M. Nolte, “Anticipating Cyberspace Security: NSA’s Experience 1992-1997,” Cryptologic Quarterly, 2012, 26-37.} (See Appendix B for the full Nolte article.) NSA personnel were just beginning to understand that “something new was out there…that may or may not align with traditional understandings of information warfare and electronic warfare…that had potential implications both for NSA’s ‘offensive‘ (signals intelligence) and ‘defensive’ (then known as communications security or COMSEC, more recently as information assurance or IA) missions.”\footnote{William M. Nolte, “Anticipating Cyberspace Security: NSA’s Experience 1992-1997,” Cryptologic Quarterly, 2012, 26-37.} Nolte’s review of internal documents during this time
period revealed a “small measure of ‘protecting rice bowls and other bureaucratic pathology’” as well as a recognition that “possible responses to it may not fit easily within either mission or within the legislation and regulations with the new development—that is, attacking or exploiting the systems of another nation—would, at the very least, approach a war-making role beyond that assigned NSA within the U.S. Code.”

Hackers, Cyber War! and the Digital Explosion: 1995

As NSA was sorting out and adjusting to these developments, a new dynamic was injected. “The Tofflers wrote a book on Information Warfare, the Internet exploded, and it was very clear we were going to have to live on the net to be effective in our SIGINT mission and to conduct any effective IW.”

Three external events helped set the stage for deeper NSA involvement in CNE/CNA during 1995. According to Black, influencing event number one was the “takedown” of Kevin Mitnick, the hacker whose real-life escapades dating back to 1982 were the inspiration for the Matthew Broderick hit film Wargames, and whose alleged endeavors over a 2.5 year period included hacking into computers, stealing corporate secrets, scrambling phone networks, and breaking into the North American Aerospace Defense Command (NORAD) national defense warning system. After going to prison for a year and apparently reforming, Mitnick was accused of violating the terms of his probation by hacking into voice mail systems at Pacific Bell in 1991 and after a warrant

---

was issued, became a fugitive. During that period, he allegedly hacked into computers at Motorola, Nokia Mobile Phones, Fujitsu, Novell, NEC, Sun Microsystems, Colorado SuperNet and the University of Southern California.  

The second event Bill Black cited as propelling the development of computer network attack forward was a book written by Nicolas Negroponte called *Being Digital*. Negroponte, amongst a deep number of future projections, successfully predicted that “the entire economic model of telecommunications—based on charging per minute, per mile, or per bit—is about to fall apart. As human-to-human communications become increasingly asynchronous, time will be meaningless (five hours of music will be delivered to you in less than five seconds). Distance is irrelevant: New York to London is only five miles further than New York to Newark via satellite.”

The third seminal event cited by Black as a major driver for CNE/CNA development was the public launching of the Netscape internet browser. Netscape

---


368 Netscape was the first widely popular Internet browser (Internet access application) which was launched in early 1995. This application was developed by Mark Andressen, who worked at the National Center for Supercomputing Applications (NCSA). Microsoft licensed the underlying technology to create its first version of its web browser, Internet Explorer (IE). In 1998, Netscape released the source code for Netscape Communicator to the public, which gave rise to the Mozilla Organization, but also created a market advantage for Microsoft to gain market share for expanding the reach of IE, which became the world’s most used browser late on in 1998, a market penetration advantage it has never relinquished. See Sean
Navigator almost instantly became the way millions of people around the world were able to access the World Wide Web.\textsuperscript{369} According to Black, “That was the turning point of the digital world.” Within 5 years of Tim Berners-Lee’s creation of the World Wide Web on a single computer leveraging the ARPANET/Internet backbone, millions of people now had the ability to access and share information around the world (almost) in an instant.\textsuperscript{370} Computer Network Operations as an exploitation and attack method now had a simple, high-speed and easy-to-use delivery system, with a willing and growing number of systems and adopters of the integrated technology in both the government and the private sector throughout the world, each opting in as a potential target using a unique identifier for their location. Black realized that traditional way of doing SIGINT exploitation and analysis would soon become outdated.\textsuperscript{371}

The concept of Information Warfare was entering the public imagination via newsstands around the country, which seeded a public debate on the issue and indirectly pressured the bureaucracy to push forward on the next phase of post-Gulf War technological warfare. On August 21, 1995, the cover of \textit{Time Magazine} showed an illustration of a soldier with a futuristic pilot’s helmet with a heads-up display entitled

---

\textsuperscript{369} A variety of pervasive web technologies and standards that are used and exploited today such as Secure Sockets Layer (SSL), Java, Javascript, open Application Programming Interfaces (APIs) and support for online media, were innovations that Navigator made mainstream (Brian McCullough, “On the 20th Anniversary: An Oral History of Netscape’s Founding,” \textit{Internet History Podcast}, April 3, 2014, accessed August 28, 2016, http://www.internethistorypodcast.com/2014/04/on-the-20th-anniversary-an-oral-history-of-netscapes-founding/).

\textsuperscript{370} “The World Wide Web went live, on my physical desktop in Geneva, Switzerland, in December 1990. It consisted of one Web site and one browser, which happened to be on the same computer. The simple setup demonstrated a profound concept: that any person could share information with anyone else, anywhere” (Tim Berners-Lee, “Long Live the Web,” \textit{Scientific American} 303, no. 6 (2010): 80-85).

\textsuperscript{371} William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
“Cyber War: The US Rushes to Turn Computers into Tomorrow’s Weapons of Destruction….” The article, a harbinger of future capability development, described “information warfare as the hottest concept in the halls of the Pentagon,” where the US military “has wide-ranging plans to revolutionize the battlefield with information technology much as tanks did in World War I and the atom bomb in World War II.” While seemingly more aspirational than fact based, the article highlighted a series of developmental efforts. It described a “CIA clandestine program that would insert booby-trapped computer chips into weapons systems that a foreign arms manufacturer might ship to a potentially hostile country—a technique called ‘chipping’” and furthermore reported that “NSA, along with top-secret intelligence units in the Army, Navy and Air Force, has been researching ways to infect enemy computer systems with particularly virulent strains of software viruses that already plague home and office computers.” Citing senior military officers, the article stated that “the President’s black bag containing the instructions for launching a nuclear strike may also (one day) have inside it the codes for U.S. infobombs.” However, the MMI had not yet developed, and even internal commentators at NSA acknowledged the ongoing confusion over the terminological meaning and descriptions of activities and capabilities that actually fell under the definition of IW.

373 There is no widely accepted taxonomy of IW. Consequently, it covers a multitude of high-tech material including command and control warfare, perception management, computer warfare, gathering intelligence from computers, using computer viruses to destroy data, affecting an adversary’s infrastructure through the use of computers, esoteric weapons such as electromagnetic pulse devices and microwave beam guns and
What had developed at NSA, however, was the concept of Global Network Intelligence, which according to a Cryptolog article, which was in existence for at least two years prior. The article was entitled “Global Network Intelligence and Information Warfare” SIGINT and INFOSEC in Cyberspace,” and Global Network Intelligence or GNI was described as a new and comprehensive SIGINT activity that was critical to NSA’s future, although no further information is provided due to redaction. See Appendix C for a diagram of GNI. “GNI is a response to the dramatic changes in global telecommunications that began with the transition from analog to digital communications in the 1980s—the rapid evolution of digital communications and concurrent advances in transmission media—especially fiber optics and networking technologies have radically altered the complexion of the global telecommunications infrastructure.”

The article described, at a conceptual level, the effects that telecommunications and information transmission technology changes were likely having on NSA’s ability to collect intelligence, a change in an operating environment that GNI’s technical approach was apparently being designed and developed to address. Furthermore, from an

so forth” (National Security Agency, redacted author, “Book Reviews: Recent Publications on Information Warfare,” Cryptolog 20, no. 3 (Fall 1995)).


376 The article described rapidly evolving modern communications technology protocols of the time period, underscoring the SIGINT collection challenges: “A call overseas from the US might involve use of a digital fiber optic network, undersea fiber optic cable then a transition to another continent’s fiber optic cable system which is then transmitted to a local phone exchange. A cellular call might traverse the local cellular, microwave and fiber optic systems, then overseas through a fiber optic cable or via satellite, back to a fiber optic network to an office building; the signaling information (1’s and 0’s), which provide key information for the telephone companies to route and bill the call may travel over an entirely different path. As networks expand, users will be able to contact other users anywhere in the world without ever knowing how their calls were completed—the same is true for data communications, and personal computing” (National Security Agency, redacted author, “Global Network Intelligence and Information Warfare: SIGINT and INFOSEC in Cyberspace,” Cryptolog 21, no. 1 (1995)).
Information Warfare perspective, the former G4 chief acknowledged that “the sophisticated telecommunications and data networks now being deployed worldwide make it possible to deny and degrade a potential adversary’s command and control communications and sensitive commercial and diplomatic communications from great distances with little or no risk to life and limb.”

Although the transition from analog to multimodal digital communications presented technical challenges to NSA, what was more worrisome to the former Chief of G4 seemed to be the challenges for NSA’s organizational culture and traditional ways of doing business: “institutionally we still tend to function too much as a collection of stovepipes in the development of new capabilities [which]...requires the need for cross organizational communications so those responsible for developing new GNI or IW capabilities can keep abreast of all relevant activities [and engender] ‘cross fertilization.’”

Minihan Moves Over to Lead NSA: 1996

Soon after his move to become the new Director of DIA, Minihan began discussing NSA with Deputy Secretary of Defense John P. White. Dr. White had recently suggested the phrase “they don’t get it,” referring to NSA’s orientation toward line-of-sight signals intercepts, not network/Internet attack capabilities. Soon thereafter, Secretary Perry called Minihan and told him that he was reassigning him to

---

380 General Kenneth Minihan, Interview by author, Washington, DC, January 14, 2015
become the new Director of NSA; Dr. Perry said “NSA doesn’t get it, I need you to fix it.” Perry’s decision was a direct result of his knowledge of the capabilities Minihan envisioned in 1992 and built during his time at AIA. Outgoing Deputy Secretary John White was also aware and approved of his initiatives, however, he was about to be replaced by a new Deputy Secretary, Dr. John Hamre, whom Minihan knew was intent on continuing cuts to NSA’s budget. NSA’s budget was cut by one third during Admiral Studeman’s and Admiral McConnell’s tenure at NSA while Hamre was the Under Secretary of Defense (Comptroller).

Minihan said “no thanks” to NSA billet based on his shared belief with Perry and White that NSA did not understand the need for a new method of warfare (i.e. 21st century Information Warfare exploitation tools). Additionally, Minihan believed that NSA was “broken” due to the clipper chip encryption controversy, among other deficits he knew about. Despite his declination of the position, William Perry ordered him to go to NSA, and presented him with a challenge to change the organization, stating “I’ll know you are doing a good job if I hear the complaining.” As Minihan was about

---

384 The Clipper Chip was a NSA-designed encryption microprocessor that the US government wanted installed on a variety of devices that might use encryption for communications. Under this proposal, the US government would legally be able to decrypt communications as delineated by statute, by holding the decryption key in “escrow.” A variety of privacy concerns were generated, and eventually the initiative was dropped (Steven Levy, “Battle of the Clipper Chip,” The New York Times, June 12, 1994, accessed August 29, 2016, http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all). Minihan later disestablished the controversial Clipper chip program. He indicated Admiral McConnell, his immediate predecessor, was being a “good soldier” in his advocacy for the effort (General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015 and November 24, 2015).
to transition to NSA as the new DIRNSA, CIA was starting to configure itself differently to address the changing nature of information in transit and information exploitation.

Secretary of Defense William Cohen and the Chairman of the Joint Chiefs of Staff General John Shalikashvili briefed DIRNSA Minihan on what they wanted accomplished in the realm of computer network attack capability development, and Minihan volunteered to execute the mission.\footnote{General Kenneth Minihan, interview by the author, Washington, DC, January 14, 2015.} Director of Central Intelligence John Deutch gave Minihan three months to stand-up NSA’s organizational capability, although it actually took one year.\footnote{William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.} Bill Black stated that Secretary of Defense William Cohen was directly involved in the movement ahead for CNA development. In fact Black stated that, “I don’t know anyone else who would have had the guts to give us the authority he did.”\footnote{William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.}

From Chris Inglis’s vantage point, Ken Minihan set out to resolve these issues through a series of organizational and systems component integrations which had a cumulative, transformational effect. Inglis started at NSA as a Branch Chief in 1986, and the topic of his first day was a lesson in NSA culture: “So-and-so embarrassed me in a meeting yesterday, and now we have to figure out a way to get even with him.”\footnote{James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.} Inglis was shocked: Clearly the time, thought and energy going into obtaining revenge for a perceived slight meant these managers were not focused on the adversary, and the working environment was not for the faint of heart. Inglis notes that the individuals who possess group-level responsibilities are where most of the power actually lays at NSA.
Each of these Group leaders had a “warlord mentality” when it came to their discrete mission areas. Inglis made a point to note that these leaders were not trying to do the wrong thing, just what was right for their group’s specific parochial interests.\footnote{Inglis noted that the organizational and cultural transformation that was started by General Minihan, continued and matured with General Hayden, and concluded during General Alexander’s tenure “took forever” due to institutional intransigence, including a pre-existing “warlord culture” amongst the major Group leaders in A, B, G etc. He observed that “culture eats strategy for breakfast.” Meaningful, lasting change was only completed by the end of Alexander’s time at NSA, the longest tenure of a DIRNSA in NSA history. Between Hayden and Alexander, 14 years of continuous leadership finally accomplished the changes being sought (James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015). An outsiders’ group was convened as well, both during a sixty-day study period meant to provide feedback to the new DIRNSA.}

When DIRNSA Minihan took over at NSA, he took several steps that changed NSA. COMSEC was renamed Information Security (INFOSEC) to better reflect the nature of what was really being protected. Furthermore, to address the inherent segregation of institutional duties at NSA, which were bifurcated literally and figuratively between INFOSEC and signals intelligence collection and drive integration, Minihan decided to embed an Information Assurance Officer into the National Security Operations Center, the 24/7/365 center of NSA.\footnote{James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.} The lead managing position, the Senior Operations Officer (SOO) (pronounced “sue”) was the key integrator of all inbound Signal Intercept reports and was effectively the “Director after Dark.” The SOO position was actually staffed by five people due to the 24/7 nature of the position’s requirements.\footnote{James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.} According to General Minihan, he approached NSA IA Director Mike Jacobs and asked him for his “best and brightest guy,” whom he put through a series of rotational assignments, starting with the NSOC. He was provided Chris Inglis’s name.\footnote{Inglis recalls that he was actually the second choice for the job; the first choice went through six months of training and quit as he was about to start the job, citing the stress his new position would bring and a}
Inglis described the NSOC apparatus to provide a sense of the operational environment: Each of the regions of the world had a senior coordinator in the NSOC, i.e. A Group Senior Coordinator, B Group Senior Coordinator, G Group Senior Coordinator, etc.\(^{394}\)

The SOO integrated all information that flowed through the NSOC, reading and analyzing discrete bits of information from SIGINT collection and the COASTLINE system that flowed through a database and created a mental picture of what was occurring in the world.\(^{395}\) Inglis, by his own admission, did not know a lot about SIGINT at the time, “so I had to find some people who did”—the senior group coordinators, and “gave them a voice and ability to collectively integrate the information with me,” thus creating a more effective collaborative approach to a mission critical position.\(^{396}\)

During this time period, other aspects of NSA internal culture manifested themselves as well. “One day General Minihan called me up during my time as SOO and needed a time-sensitive answer to a problem to make an important decision; I tasked the Directorate of Operations [what is today the SIGINT/Signals Intelligence Division] and the Information Assurance to get back to me to offer possible solutions for DIRNSA by close of business that day. At the end of the day, after working feverishly to provide a response to the Director’s tasking, a breathless member of the DO staff came to the NSOC floor to provide the group’s best possible options based on the time constraints. The IA staff came back to me as well and said “we will give you a proper answer in six

---

\(^{394}\) James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.

\(^{395}\) James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.

\(^{396}\) James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
weeks,” based on a belief that anything short of that would have been inappropriate for something of high priority—yet offered nothing else for the time-sensitive tasking for the DIRNSA.397

Significant stovepiping still existed at NSA despite Minihan’s best efforts at integration, based in part on the power of each Group leader, the warlord culture and the parochial interests within each group’s organizational structure.398 Although each NSA element was “doing the right thing within their smaller domains,” the collective effect was suboptimized. As a result, “important intelligence or operational information had the possibility of being missed.”399 Inglis observed that a transformational leader either has to kill this behavior or create a compelling story to sway the embedded interests to enact meaningful positive change. One method that was tried during the time period was to take a typical mission support activity and recast it as an operational support element; however, this had unintended consequences: over time “every element sees itself as operations, or at least enabling them,” and is therefore critical.400

However, nomenclature changes and partial modifications of existing internal organizations alone were insufficient to successfully execute the new mission space. To further develop and/or create the CNA capability, Minihan “had to take it out of hide.”401

397 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015. General Hayden was interviewed by CIA in 2000 regarding the organizational change underway at Ft. Meade. Hayden was quoted as saying, “NSA as an institution is methodical and it is thoughtful in its decision making. It’s comfortable deferring decisions until it has more precise data, taking it to the sixth significant digit” (Central Intelligence Agency, “Overseeing an Era of Change: An Interview with NSA Director Lt. General Michael V. Hayden,” Studies in Intelligence 44, no. 2, 2000, accessed August 29, 2016, https://www.cia.gov/library/readingroom/docs/DOC_0005393249.pdf).
398 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
399 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
400 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
Minihan closed NSA A Group to offset the Hamre cuts named Bill Black Special Assistant to the Director for Information Warfare, and established an entire staff for Information Warfare development during this time period. Minihan noted that by closing A Group, “the winning team” was being disestablished, “but I needed the whole of NSA on board to be able to focus on CNE/CNA development. I needed A Group to know I thought that they succeeded with their offensive and defensive model, but now I needed them to let go of some of the activities that made them successful in the past. Closing A Group allowed me to put ‘real money’ against (toward) Chiari’s activities, which were boutique at the time.”

402 In 1996 Black was still the Chief of A Group.
403 According to Jeffrey Richelson, the “A Group of NSA’s Directorate of Operations was responsible for intercept operations directed at the Soviet Union and the East Bloc. Other regional groups at the time were B Group (Asian Communist Countries) and G Group (all other countries). After the collapse of the Soviet Union, the directorate was reorganized” (Jeffery T. Richelson, A Century of Spies: Intelligence in the Twentieth Century (Oxford, UK: Oxford University Press, 1997).
404 General Minihan offered this insight: “Bill Black was a maverick the entire time he was at NSA—people either loved him or hated him; one thing is clear: He knew exactly how the system worked.” At the time Minihan met Bill Black, he was the head of NSA “A” Group (General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015).
405 As Black started to build out the IW component, a colleague at NSA pointed out Tim Denison, telling him to “add him to your staff. He’s had a hard time working for other people, but he’s your style….“ Black took the suggestion and today specifically credits Dennison as critical to the overall stand-up of the Information Warfare staff (William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015). NSA analyzed whether Information Warfare was in and of itself something new, concluding that indeed IW was something new: a combination of expanded, yet refined Electronic Warfare capabilities plus a destructive capability and qualitatively different from those measures executed in previous conflicts under the rubric of “Electronic Warfare” or “Command and Control Warfare,” and even expanded it to Information Infrastructure Warfare (I2W): “The question/occasionally arises whether there is anything fundamentally new about IW…. [since] the application of Electronic Warfare dates back to 1942…[where the] combination of EW and physical destruction set the pattern for defeating enemy air defenses for the next fifty years. [Similarly] C2W dates to early 1991 in Desert Storm. IW extends this logic by making possible infinitely scalable, infinitely accurate strikes on infrastructure targets by means of cyber-attacks on the information infrastructure needed to operate it (hence the term Information Infrastructure Warfare, I2W [emphasis added] (National Security Agency, redacted author, “The Role of Information Warfare in Strategic War,” Cryptolog 23, no. 1 (March 1997).
As Special Assistant for Information Warfare, Black was finally able to help “break it [the G section CNE capabilities] loose from the compartment”\(^{407}\) and utilize the resident capabilities more freely under the moniker of “active SIGINT.” During this time frame Black introduced Dennis Chiari, his collaborator over the course of the prior two years, to all the NSA seniors, and explained the capabilities G44 possessed and outlined the activities the Group engaged in. To further punctuate the impact of this revelation, Black told the NSA SES cadre “this is what we are doing and this is where our future is…. ” There was resistance within NSA from people who were fearful that Information Warfare would compromise its core missions, reducing budgetary resources for traditional SIGINT and information security, which many saw as the Agency’s core mission.

Black explained the term “active SIGINT” was used to ensure the capabilities and implementation strategy being developed for CNE and CNA fell under NSA’s legal authorities. According to Black, NSA attorney Kevin Powers developed the “active SIGINT term and wrote the legal justification;” Black stated, “we just kind of did it…. ”\(^{408}\) General Hayden explained it in the following way: “At NSA we had to develop a whole new language. We were moving to active SIGINT, commuting to the target and extracting information from it, rather than hoping for a transmission we could intercept in traditional passive SIGINT. This was all about going to the end point, the targeted network, rather than trying to work the midpoint of a communication with a well-placed...


\(^{408}\) William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
antenna or cable access. We also knew that if we did this even half well, it would be the golden age of signals intelligence since mankind was storing and moving more and more data in digital form with each passing day.”

Black, who was actively involved with this recasting of NSA’s traditional mission space, highlighted the importance of these types of specific terminology and nomenclature changes in a bureaucracy. NSA’s interpretative change had implications for [Executive Order] 12333 Authorities that underpinned an ongoing bureaucratic battle between NSA and CIA.

According to General Minihan, the terminology controversy over the use of the phrase Information Warfare (IW) versus the more innocuous Information Operations (IO) came to a head, resulting in an official nomenclature change. Minihan indicated that “IO was a term of choice and was delineated into two categories: active versus passive SIGINT or active versus passive Information Operations.” He indicated that he did not want to be distracted by the IW v. IO issue, “in fact I preferred IO as I wanted NSA to be less visible so I could build out mission capability for CNA and CNE.”

He would soon

---


410 Ronald Reagan, “Executive Order (E.O.) 12333: United States Intelligence Activities” (December 4, 1981): 36, https://www.archives.gov/federal-register/codification/executive-order/12333.html. “Intelligence Community and agencies within the Intelligence Community” refer to the following agencies or organizations: (1) The Central Intelligence Agency (CIA); (2) The National Security Agency (NSA); (3) The Defense Intelligence Agency (DIA); (4) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; (5) The Bureau of Intelligence and Research of the Department of State; (6) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; (7) The staff elements of the Director of Central Intelligence.

411 The belief that the term “Information Warfare” was a politically unacceptable description.

412 General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015. From a US perspective, Admiral Studeman offers this assessment, which is applicable to any time period under examination in the modern era: “There are three principles of information operations intelligence: the need for deep penetration and collection capabilities, counterintelligence and espionage and operational technologies to collect intelligence” (Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015).
get his chance. On December 9, 1996, DoD itself changed the nomenclature for Information Warfare to Information Operations with the issuance of a new, at the time classified order, DoD S3600.1, which cancelled DoD Directive TS-3600.1, “Information Warfare,” initially issued in December 21, 1992. This revised Directive defined Computer Network Attack (CNA) for the first time as “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.” Although partially redacted, the implication is that CNA is a specific capability within the Information Operations umbrella. Historian Michael Warner states that “the new term essentially amounted to a…’cosmetic’…[change] and perhaps even a political (though not partisan)[one] in its motives.”

When asked why this 1996 White memo changed IW (C2W) to Information operations, a DoD historian replied that “the government did not want the inference to be drawn that we are militarizing cyberspace, however, there can be militarized operations….”

The former DoD official responsible for IO in OSD was more direct:

---


415 Department of Defense Historian, name withheld upon request, interview by the author, Maryland, May 22, 2015.
“The State Department made us change terminology from Information Warfare to Information Operations for political reasons.”


James (Jim) Gosler, future director of CIA’s Clandestine Information Technology Office, was trained in a background of physics and mathematics and spent five years in the US Navy Nuclear Propulsion Program before joining Sandia National Laboratories. Gosler’s experimentation on the mainframe supercomputers and analyses of hardware and software interfaces garnered him expertise that directly bears on the origins of computer network operations. In 1985, as a result of his developing expertise, Gosler transferred to the Sandia Adversarial Analysis Group where he was engaged in projects conducted on behalf of the United States nuclear weapons program pertaining to Permission Action Link (PAL) development and related analyses. According to Gosler,

416 Department of Defense Former DoD Official, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
417 James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015.
418 The Sandia Adversarial Analysis Group consisted of independent “technical folks” whose skill sets were used to analyze contemporary nuclear weapons use control countermeasures as part of a red teaming process to enhance nuclear weapons systems security. This was an iterative process, and as various types of technology embedded in the weapons changed, personnel with applicable (or non-applicable) skill sets were swapped out. This ensured that engineers working on the projects stayed very independent, and not beholden to a bureaucratic mindset. Gosler credits senior manager Peurifoy as exceptional in making sure this happened, by allowing sufficient top cover for engineers like Gosler to experiment and improve the systems by seeking to overcome the countermeasures being designed for weapon safety, security and reliability (James (Jim) R. Gosler, interview by the author, Tysons Corner, VA, August 2015).
419 James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015. Sandia developed Permission Action Links (PALs) to prevent unauthorized people from obtaining access to nuclear weapons and to improve presidential control of the stockpile; Sigma 14 and Sigma 15 are special categories of nuclear weapons design information (NWD) that pertain to Protection of Use Control Vulnerabilities and Designs; Sigma 14 and Sigma 15 information is defined as use control information that can significantly enhance an adversary’s ability to obtain an unauthorized nuclear detonation or to deny the authorized use of nuclear weapons, explosives, or devices. For further information see Department of Energy, “DOE Order 452.7, Protection of Use Control Vulnerabilities and Designs,” May 14, 2010, accessed August 28, 2016, https://www.directives.doe.gov/directives-documents/400-series/0452.7-Orden; Department of Energy, “DOE Order 452.8, Control of Nuclear Weapon Data,” July 21, 2011, accessed August 28, 2016, https://www.directives.doe.gov/directives-documents/400-series/0452.8-Orden.
this is a key point in time to the future development of computer network operations—
due, at least in part, to the fact that the technical approach to designing and building use
control systems was beginning evolve from utilizing discrete electronic control
mechanisms to those which incorporated microelectronics and microcontrollers—the use
of which, Gosler learned, could hypothetically leave residual vulnerabilities residing in
systems.420

In time, based on the knowledge he acquired examining software/hardware
interfaces and the residual vulnerabilities the use of microelectronics and
microcontrollers engender, Gosler convinced Sandia management to perform proof of
principle technical studies that came to be known as the CHAPERON 1 and
CHAPERON 2 exercises.421 The premises of the CHAPERON exercises were simple:
Can a person design a secure application? Can a person insert malicious constructs that
are not detected even through detailed evaluation? Two groups were created as part of the
study: Group 1 was designated as Subverters and Group 2, which consisted of two
subteams of evaluators, was responsible for uncovering the subversion. As a practical
matter, the design of the exercise purposefully provided all advantages to the Evaluator:
The subverter would inform evaluators that one or two vulnerabilities were placed in a
system, within certain parameters and constraints, and provide them comprehensive
system documentation. Gosler was designated as a subverter and immediately set out to
undermine a specific security-critical application. As part of the study, he created a
“Guideline for Subversive Software Development” to outline principles for subversion

420 James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015.
421 James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015.
design and implementation, which included prohibitions against the use of extraneous code: Any code utilized must have a justifiable reason for being a part of the system, and the subversive design could not compromise the encryption algorithm. Through a painstaking trial-and-error process, Gosler developed and implanted two subversions in the system which none of the evaluators were able to find: (1) the insertion of Zork text which revealed secret system variables, and (2) another subversion.\footnote{James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015.}

The Sandia evaluation team spent several months examining the doctored system, to no avail. In fact, it took three 8-hour-long days of briefing the evaluators on how the subversive design worked. Gosler initially planned to train future Sandia evaluators to uncover the more complicated subversion using the CHAPERON 1 exercise as a teaching tool, but the subversion he created was so complicated that no one could solve it and led the evaluators to become extremely frustrated. This required the creation and development of the CHAPERON 2 exercise, which was designed to be less complex.\footnote{James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015.}

Sandia employee Tom Barger created the follow-on exercise as the subverter, which was severely limited to 692 machine-level instructions. Close to 100 people were given an opportunity to be evaluators of the subversion, but only Gosler successfully identified the exploit (although a couple other evaluators came very close to discovering the exploit), which was a spoofed code execution sequence embedded in a particular machine instruction.\footnote{James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015.}
The CHAPERON 2 exercise came to the attention of Rick Proto, and Robert Morris Sr., Chief of Research and Chief Scientist at NSA National Computer Security Center respectively (among others in the IC), who thought these exercises were insightful and could be helpful. Upon meeting, Gosler asked Morris, “How complex can software be for you to have total knowledge of what it would do?” Morris replied, “100% confident at 10,000 machine level instructions or less. We would have no confidence at more than 100,000 machine level instructions.” Immediately after this interaction, Gosler shared the subversion he created for the CHAPERON 1 exercise with Morris and Proto. Clearly, the implications of what Gosler achieved in the CHAPERON exercises was not lost on NSA technical leadership, and their assumptions about their abilities to detect subversions in computer hardware and software interfaces would need to be adjusted accordingly. Soon thereafter, Rick Proto brought Gosler to Ft. Meade as a Visiting Scientist (to what is now NSA’s Information Assurance Directorate (IAD)) to work with NSA technologists and discuss subversive design principles for the purpose of developing better evaluation techniques. During his time as a Visiting Scientist, Gosler was introduced to what he called the “Dark Side” of NSA (what is now known as the Signals Intelligence Division), and he was extremely impressed. He told the members of SIGINT portion of the organization that “I can’t think of anything else I’d rather do in my life, but I have a commitment to IAD and Sandia.” In fact, Gosler was so committed to the efforts he saw being made by the SIGINT directorate, he volunteered to work during

---

425 James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015.
426 Gosler indicated that one of the techniques involved a microprocessor anomaly.
427 James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015.
his vacation time at the Agency and arranged to have Admiral Studeman (now DIRNSA) assign him to NSA as part of his Naval Reserve duty activities so he could contribute to the mission-related activities. Upon completion of his assignment at NSA in 1990, Gosler was named Manager of the Software Adversarial Analysis Department and continued to serve the country.\footnote{James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015.}

Glenn Gaffney, future Director of CIA’s Information Operations Center and the Directorate of Science and Technology, was the CIA representative to a STO cell in the late ‘80s and early ‘90s. Gaffney worked with a group of Navy personnel including Jake Schaeffer, Jim Bob Powell, Chuck Tambrillo and Captain Al Ross from NSA. According to Gaffney, this small team of men began to ask “What do we need to do to move IW/IO/Cyber into the mainstream?”\footnote{Glenn Gaffney, interview by the author, McLean, VA, November 23, 2015.} Gaffney ruminated on the question for a period of time, and then took action. In 1993 he authored a white paper that asked “What does IW mean for CIA?” from an operations, analytic and technical perspective. Gaffney indicated that he was “heavily influenced by STO meeting discussions with the Navy guys. I was leaning toward the idea of a Center or some entity to focus on this.”\footnote{Glenn Gaffney, interview by the author, McLean, VA, November 23, 2015.} During the 1994-95 time frame, Gaffney, now a GS-15, was asked to stand-up a new organization based around the white paper he authored in 1993. “The white paper now had internal traction, circulated in the building, and made it to Director Tenet and the head of the Directorate of Intelligence (DI). Frank asked me to stand-up the first IW branch in the DI. Our new IW organization had a total of 12 people. Half of the team was focused on offensive
analysis and half of the team was focused on defensive analysis. The first computer tools we [IW Branch] developed were on giant old floppy discs that could be physically loaded onto computer systems.”

Throughout this time period, Jim Gosler continued his work at Sandia on behalf of DOE and the Intelligence Community. As the notion of “cyber” started to percolate at CIA, two studies were undertaken to answer a simple question: What should CIA do to posture itself in this new field? CIA’s concern that it “might not be ready to exploit the rapid expansion and utilization of advanced technology in various target domains led to the establishment of a ‘Special Projects Staff’ to study the issue. The staff was comprised of key IC partners and customers as part of the review.” The principal finding of the study concluded CIA was “not prepared to ‘seize’ the collection opportunities in the rapidly emerging high tech environment;” the SPS “recommended the creation of a new office to ‘tackle’ these new targets.”

Crumpton put it succinctly: “digital systems stored secrets worth stealing.” The conclusions from the Herd study led to the creation of CITO.

---

432 In 1993, he established and directed the Vulnerability Assessments Program and was named Assistant Director of the Systems Assessment and Research Center. In 1990, the organization Gosler managed at Sandia received $500k Program, funded solely by NNSA, and by 1995 his organization had a $50M Program, $500k funded solely by DOE, with the remainder coming from sources within the Intelligence Community (James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015).
433 The first study was led by Dr. Craig Fields from DARPA, which essentially concluded that “we need to do something”; the second study, led by Bob Herd, sought to answer the question “now what are we going to do?” (James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015).
436 James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015. Admiral Studeman and Jim Gosler also spoke of the “Sorkin Study at CIA,” which concluded that CIA was not well positioned for
In September 1995, Ruth David, most recently the director of Sandia National Laboratories Strategic Thrust in Advanced Information Technologies group, took over as the new Deputy Director for Science and Technology (DDS&T) at CIA. Her primary emphasis as DDS&T was in the information technology arena—an area that a 1995 blue ribbon review panel had recommended be a key area of DS&T activity. DS&T’s core mission space (as described today) is “worldwide/regional requirements for clandestine collection,” advising and assisting the clandestine service (Directorate of Operations) “on the full range of technical operations” and augmentation of tradecraft as well as “researching, developing and applying advanced technologies to provide the national significant intelligence advantage, and much more.” Once in place, David created three new offices: the Clandestine Information Technology Office (CITO), the Office of Advanced Analytical Tools, and the Office of Advanced Projects, which was accomplished, at least in part, by cutting the budget of the DS&T’s Foreign Broadcast Information Service and terminating the Office of Research and Development, which according to Jeffrey Richelson was extremely controversial at the time.

Once the expansion of the mission need was determined, a leader for the new hybrid organization needed to be selected. Gosler, still working away at Sandia, was asked to interview for the position, and met with Nora Slatkin. She was obviously

impressed and offered Gosler the Executive Director job on the spot. Gosler indicated that “there was great anxiety at CIA when I arrived—everybody was hunting for mission ground in the cyber area.” Gaffney noted that “Elements of the DI, DO and DS&T collaborated to form this thing. However, the DI opted out of what was to become CITO, as organizationally the DO and DS&T worked better together. We put the IW offensive branch into CITO, while the Defensive IW branch stayed in the DI. The IW offensive branch became the core of the new targeting element and I started to grow it in size.” Gosler, who was Gaffney’s boss, praised his efforts at CITO: “Glen was in the CITO analytic shop at first, and he separated himself from the pack in a short period of time. I moved him around the organization to get him exposure to a variety of activities so that he could take my job one day—which he did.”

Gosler said “CITO, as an organizational entity, was a collection of technical operations, not just cyber, and as Executive Director I reported directly to the heads of the Directorates of S&T and the Directorate of Operations.” Members of the Clandestine Service, including Crumpton, were directed to take training that emphasized

---

439 James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015. Nora Slatkin was CIA Executive Director at the time. Interestingly, she worked with John Hamre when they were both Congressional aides for the Senate and House respectively (Stan Crock, “Nora Slatkin’s Mission Impossible: The CIA,” Bloomberg.com, February 26, 1996, accessed August 29, 2016, http://www.bloomberg.com/bw/stories/1996-02-25/nora-slatkins-mission-impossible-the-cia). Bob Herd, the leader of the study that ultimately provided the impetus for the creation of CITO, wanted the Executive Director position, but unfortunately was not offered the job. When Gosler was offered the job, he asked Bob Herd if he should take it. Herd told Gosler that there is no better job. To this day, in his speeches, Gosler only thanks one person: Bob Herd, for his selflessness. According to Glenn Gaffney, “I knew Jim Gosler was going to be my new boss before he did” (Glenn Gaffney, interview by the author, McLean, VA, November 23, 2015).


443 James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015.
“espionage as the key to digital intelligence,” where the Clandestine Service members would be the “pathfinders for the CIA’s cyber offensive against an array of targets. As adversaries grew to acquire and use digital data (as the Internet expanded) so would the CIA’s cyber operations.” Crumpton acknowledged that the “advent of espionage in cyberspace was nearly instantaneous…its rapid growth and impact on [CIA’s] operations was stunning and even revolutionary; the amount of raw data stolen and exploited became hard to measure—instead of pages, it was terabytes.” Gosler indicated “the differentiating strength for cyber at CIA was the involvement of the DO, although there was a lot of cultural inertia and antibodies against the development of these capabilities” at this time.

In early 1996, after the creation of CITO was completed, Gaffney, who was still in touch with his colleagues from the STO cell, added a new member to their IW action group, and started an attempt to create what was conceptualized as an Information Operations Center (IOC). Ruth David and Director Tenet were now on board with the

---

445 Crumpton notes that by 1999 most of CIA DO technical operations were based in cyberspace and became symbiotic with traditional ops; he also opined that “technical collection is much harder, because of massive amounts of data, new requisite skills, diverse operational risks, organizational challenges, bureaucratic competition, archaic law, uniformed politics, and social norms. In spite of these hurdles, technical collection, especially when combined with effective HUMINT operations, has proven sometimes wildly successful.” Crumpton also credits Gosler, who clearly was a technical expert in a variety of areas, as understanding a simple premise: “people were the primary access points, given that somebody held the data room combination, the encryption codes, the passwords, and the firewall manuals. People had written the software. People managed the data systems. Ops officers should recruit computer hackers, systems administrators, fiber-optic techs, and even the janitor if he could get you into the right data-storage area or fiber-optic cable” (Henry A. Crumpton, The Art of Intelligence: Lessons from a Life in the CIA’s Clandestine Service (New York: Penguin, 2012).
447 Members of the old STO cell included Al Ross, Jim Bob Powell. The new member of the IW action group is the anonymous former high ranking DoD official responsible for IO at the OSD.
creation of the IOC concept. While CIA was putting an organizational framework together and readying itself to propose the new cyber entity (IOC), NSA was also organizing their approach to an Information Operations Center under Ken Minihan’s direction.

**NSA and CIA Information Operations Interagency Competition: 1996**

Glenn Gaffney related a story from this time period that crystalized NSA and CIA interagency competition in the cyber domain: “While we [Gaffney, CIA and his former STO colleagues] were trying to put an organizational framework together for the new Center [IOC], Ken Minihan and NSA made a move to own the entire operational area. General Minihan asserted himself during a coordination meeting held at National Defense University and said ‘I [NSA] will own it.’” Gaffney, who was in attendance at the meeting to make a presentation on the creation of new measures of effectiveness for cyber, similar to the methods used for Battle Damage Assessment, was not pleased. Minihan’s move, which was an attempt to pre-emptively claim the cyber operational area for NSA, resulted in the conclusion at CIA that “We can’t let NSA own this organization or else we will be shut out.”

Hank Crumpton provided some insight into CIA’s perspective on networked information flow and its relations with NSA. Crumpton reflected that upon “the advent of cyberspace…NSA struggled to reinvent itself, pursuing SIGINT not only in the atmosphere but also in fiber-optic cables and in databases. In a slick leverage of vocabulary to expand its authority from dynamic atmospheric interception to static

---

terrestrial collection, NSA called this targeted data ‘SIGINT at rest.’ This push for NSA relevance, of course, encroached on the CIA’s HUMINT turf. Using human sources, the CIA had been stealing computer data since foreign secrets first landed on a hard drive. The CIA had been filching foreign intelligence from cyberspace since its inception.”

General Michael V. Hayden provides some additional perspective on the underlying issues: “NSA’s job was all about communications. Historically that was electronic data in motion: global high frequency communications, shorter range microwave signals, photons and electrons moving along a cable. Agencies like CIA handled other materials—human sources, purloined documents, pilfered codes—more or less physical data sitting at rest. The division of labor was clear. Electronic data in motion—NSA. Physical data at rest—CIA. But the new digital domain had created a different state of nature: electronic data at rest.”

The technology changes now underway affected the methodologies under which data could be intercepted. For example, in the 1980s, the transmission of secure messages used paper outputs from optical character reader (OCR) typewriters which were scanned and electronically transmitted and then reprinted. However, with the rise of email technology and storage of data in electronic form, “many types of documents, including spread sheets, files, notes—would never be electronically transmitted.” Email was “clearly a communication (electronic data in motion)” but the digitally stored documents

---

were something new. "To NSA it was electronic and hence fair game. To CIA it wasn’t moving and hence was equally fair game."\footnote{Michael V. Hayden, \textit{Playing to the Edge: American Intelligence in the Age of Terror} (New York: Penguin Press, 2016), Chapter 8.}

Gaffney recalls this time period vividly. “Some policy pieces from NSA started coming out—specifically Bill Black’s concept of ‘active SIGINT’ which showed that NSA was trying to take the mission area by sheer force—that’s when we [CIA] went to battle stations over SIGINT at Rest, and I was the one who rang the bell.” CIA believed that exfiltrating “data at rest” was akin to safecracking (hardened safes being a traditional way of protecting hard copy sensitive information that might provide insight into the plans, intentions and capabilities of adversaries that may be seen as legitimate targets for intelligence collection). “To us, a computer is no different than a safe: The secrets are in the computer and it is our job to get them. Our perspective is that there is no difference between an asset walking physical documents out of a building or handing me a floppy disc with the information on it. The information on the computer disc was actually safer for the asset to have back then.”\footnote{Glenn Gaffney, interview by the author, McLean, VA, November 23, 2015.} “To CIA, ‘data at rest’ was not within the purview of NSA’s SIGINT (radio signals, telephonic communications et al.) collection domain of operations, but a legitimate CIA area of intelligence collection activity. Black described CIA’s view of NSA’s legitimate and traditional collection as being limited to midpoint interception, and therefore should not be tunneling into computers where data resided ‘at rest’ and then exfiltrate that information. NSA and CIA fought over this.”\footnote{William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.} This controversy pitted CIA’s conception of their traditional clandestine collection areas of
responsibility versus the NSA’s more expansive “active SIGINT” conceptualization of their authorities, which was an outgrowth of broader worldwide technology changes in communication pathways. During this time period Gaffney moved to the CIA Policy, Plans and Resource group to deal with NSA trying to take the area by force. Gaffney agreed that the debate was over who owned the mission space, and whether the information was considered what CIA called “HUMINT in Motion (CIA) versus SIGINT at Rest (NSA)”: “Although we were battling over this, it did not have operational effects as the job trumped politics for any particular mission we had.”

According to Bill Black, when NSA’s attorney ruled that the term “active SIGINT” fell under EO 12333 authorities, CIA effectively lost the argument that computer network exploitation at the endpoint (inside computers) was an exclusive CIA domain of operations. Black’s approach to this was to leverage NSA’s industrial-size SIGINT capacity in the active SIGINT arena and “take the field by sheer dominance” of the operational domain. Later on, as the terminology changed from IW/IO to cyber, an “unintended consequence of modifying the descriptive language from active SIGINT to cyber arose: NSA would not and did not have exclusive 12333 authorities to engage in cyber activities.” In fact, according to Black, no one did: The Order is silent on the matter and only NSA, which has sole responsibility for SIGINT under codified authorities, with a carve out for a possible delegation of authority to another Agency, was able to conduct...

---

these operations whether couched or actuated as passive or active collection. “Therefore the implication of this change is that everyone (in the IC theoretically) could do it.”

**CNO MMI Analysis of 1992-1996**

*Civilian–Military Relations Theory 1992-1996*

A review of the case history during the first half of the 1992-1996 time period indicates significant pressure was brought to bear by external civilian organizations in regard to IW development. However, the pressure, which included threats of disruptive budgetary intervention at NSA made by external civilian authorities, was antithetical to Barry Posen’s explanation as to why MMIs occur. Admiral McConnell was forced to kill (the polite term is disestablish) the IW program known as “M” by a congressional staff member for John Murtha, who was seeking to acquire more money for targeted defense spending in Pennsylvania, within his electoral district. McConnell believed this to be a significant mistake, but capitulated to Congressman Murtha—even though an internal review recommended keeping the capability intact for the Air Force and the Navy—due to Murtha’s threat to cut other NSA budget lines if McConnell insisted on keeping the program. As a result, NSA was forced to defund the M security program, despite the capability development progress made through 1989, and the success of certain NSA IW capabilities as exhibited during the First Gulf War referenced by Admiral Studeman. Posen predicts that the external intervention by civilians provides the positive impetus to innovate in a manner consistent with the threat environment.

---

457 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
461 Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.
civilian intervention during this time period was clearly neither positive nor supportive for IW development. Additionally, Posen does not predict negative civilian intervention explicitly designed to inhibit an emerging major military innovation during times when a country is operating in lower-level threat environment.

During the first half of this time period civilians did not push the IC or intervene in an effort to stimulate innovation in the offensive IW sphere. This was due to policymakers who looked to derive a financial peace dividend from the fall of the Soviet Union, basked in a significant US victory against Iraq based on previous technological investments, and needed to realign themselves with the domestic focus of the Clinton Administration. This evidence is counter to Posen’s prediction that the push to innovate was a result of a previous military or intelligence failure. It is important to note, however, that the Top Secret IW order was issued by ASD Andrews during this time frame, underscoring the internally generated nature of MMI development. John Podesta, Chief of Staff for President Clinton, was made aware of the US IW capabilities developed during the preceding time period early on in the Clinton Administration.\footnote{Richard L. Haver, interview by the author, Tysons Corner, VA, December 11, 2015.} Rather than support the continued development of this capability, Podesta chose to focus on potential US critical infrastructure vulnerabilities to these methods, and defensive countermeasure implementation.\footnote{Richard L. Haver, interview by the author, Tysons Corner, VA, December 11, 2015.} This is also counter to Posen’s theory of MMI development which predicts that civilian intervention to create a MMI would occur as a result of a demonstration of an adversary’s technology, either through a test or combat use which is sufficiently stark and frightening to shake civilians’ faith in their own military or
intelligence organizations’ ability to handle it, thus creating the impetus to create a MMI. Podesta was apparently worried about the implications of the US’s development of the technology, and what it might potentially mean if an adversary developed something similar in the future. Counter to what Posen’s theory predicts, US adversaries did not display IW capabilities, and even if Podesta was scared by the proxy US capabilities as a leading indicator for what an adversary might develop, he did not intervene to push the offensive IW program forward as Posen would predict. Instead, Podesta pushed forward the requirement to develop defense countermeasures, which eventually were codified in a Presidential Policy Directive.\textsuperscript{464} As a result, there is no evidence that he, or other civilian leadership, exerted control over appointments of senior officials that would carry out policies deemed necessary for offensive innovation in this area of operations targeted to address perceived or hypothesized future capabilities’ development by a US adversary. In fact, Chairman Powell acquiesced to Congressman Murtha’s demand to cut the M program despite Admiral McConnell’s appeal, and offensive IW capability development ceased.\textsuperscript{465}

Moreover, there is no evidence of internal pushback or resistance occurring after a civilian-led external intervention called for an expansion of intelligence areas of operations during the first half of this time period. Again, in fact, the opposite was true: The IW M program was killed. As the time period progressed, there is evidence of internal pushback related to the creation of the IOTC, however, this was not a result of


external civilian intervention to expand the CNE/CNE intelligence areas of operation, but more of a function of intraservice rivalry. Civilians clearly changed or modified budget requests submitted by NSA to reallocate resources: NSA’s overall budget was severely cut by Congress during this time period, in part to fund the domestic agenda of the Clinton Administration in an attempt to realize the so-called peace dividend. These budget cuts, coupled with the specific actions to kill the M program, are antithetical to Posen’s assertion that these moves would be targeted to foster innovation for a CNA-focused MMI. On the surface, the lack of an IW organization after Murtha’s intervention would provide some evidence that Admiral McConnell was carrying out the wishes of Congress as a result of their intervention and focusing on programmatic areas for traditional SIGINT collection in lieu of CNA development. However, the activities of G Group and Denis Chiari in the CNE domain essentially went on unabated throughout this time period, albeit as a limited, small-scale “boutique” capability until brought out of the shadows by Bill Black in 1996. Arguably, since CNE is technologically indistinguishable from CNA, the ongoing research, development and exploitation efforts conducted by G Group would not have been directly supported by Congress if presented as dual use capabilities also applicable to IW, even though they clearly could have been considered as such. This activity serves as disconfirming evidence that NSA adopted R&D activities or policies favored by civilians as a result of their intervention. There is no evidence that a heightened degree of attention was paid by senior civilian officials to a particular area of operational concern within the overall threat environment that drove

---

466 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
them to pressure the IC to develop CNA tools during the first half of this time period. What pressure existed was related to the development of computer network defensive measures and critical infrastructure protection. The latter portion of this time period is another matter.

Elements of civilian intervention are evident in the second half of this time period. The reassignment of MG Ken Minihan from DIA to NSA has elements of civilian intervention. Minihan was moved to carry out innovation operations deemed necessary to create CNA capabilities at a notionally resistant NSA organization. However, the leaders involved in his reassignment were internal DoD personnel, and not congressional staffers, elected members, or from the Office of the President. Furthermore, when reactivating the IW/CNA mission at NSA, Secretary of Defense William Cohen and Chairman Shalikashvili briefed DIRNSA Minihan on what they wanted accomplished in the realm of computer network attack capability development, but left the execution of the technical approach and execution to him. This can reasonably be considered minimalist civilian intervention.467

The lack of intelligence or military failures as a motivating factor for the decision to reactivate NSA IW efforts in early 1997 also belies Posen’s predictions. However, the results from the ELIGIBLE RECEIVER (ER) 97-1 exercise, and later, high-profile intrusions that came to be known as MOONLIGHT MAZE and SOLAR OPTION, underscore why further support for this newly reinvigorated effort occurred. ELIGIBLE

467 There is also no evidence of this dynamic at CIA during this time: CIA entry into IW was essentially an internally generated phenomena, although to be evenhanded in the analysis, two internally generated studies led by civilians did investigate what role IW/CNE/CNA should play at the Agency (James (Jim) Gosler, interview by the author, Tysons Corner, VA, August 2015; Henry A. Crumpton, The Art of Intelligence: Lessons from a Life in the CIA’s Clandestine Service (New York: Penguin, 2012).
RECEIVER 97-1 was meant to test the premise that the US could win in an Information Warfare conflict. Instead, the exercise provided a demonstration sufficiently stark and frightening to shake civilians’ faith in their own military or intelligence organizations’ ability to enact computer defense, thus creating the impetus to support significant improvements in offensive activities. Based on the interviews conducted, it clearly became a priority for a variety of civilian leaders to help facilitate the development of additional computer network exploitation and attack tool development via the IOTC. The genesis of IOTC, however, was internal to the IC, although it required a variety of top cover from senior officials in multiple IC entities. US adversaries did not display offensive IW/IO capabilities in perfect alignment with Posen’s theory, but the red team exercise, based on a minimum display of NSA capabilities, served as a proxy for what an adversary might develop—and this time US leadership pushed the offensive (and defensive) IW/IO program forward as Posen would predict. After the ER 97-1 exercise was conducted and the results became known, there does not appear to be pushback or resistance from the Intelligence Community related to an external call to expand CNO development activities. The creation of the IOTC to service the entire interagency as a R&D and applied technology organization was clearly in alignment with civilian wishes. There is a lack of sufficient evidence in the case history to determine whether civilians (Congress) changed or modified budget requests to support the stand-up of the IOTC, as it was funded through internal NSA and interagency partner contributions, although over

---

469 LTG Ken Minihan, DIRNSA, volunteered to take on one of the actions that emerged from this exercise that dealt with a shortfall in offensive capability. This is what led to the stand-up of the IOTC (William P. Marshall, email correspondence with the author, Washington, DC, October 2015).
time it is likely that appropriations were made to support the organization’s sustainment.

See Table 10 for a summary.
Table 10. Civilian–Military Relations Theory 1992-1996 MMI Hypotheses Analysis

<table>
<thead>
<tr>
<th>Civilian–Military Relations Theory 1992-1996</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>The push to innovate was a result of a previous military or intelligence failure.</td>
<td>No</td>
<td>In fact the opposite is true. There was no previous military or intelligence failure driving this innovation.</td>
</tr>
<tr>
<td>A civilian intervention occurred as a result of a demonstration of an adversary’s technology, either through a test or combat use that was sufficiently stark and frightening to shake civilians’ faith in their own military or intelligence organizations’ ability to handle it.</td>
<td>Yes</td>
<td>Yes, as initiated at the end of this time period resulting in the findings of the ELIGIBLE RECEIVER 97-1 exercise. However, this was an internal test of our offensive capabilities, not a foreign actor’s demonstration. There is no evidence of this dynamic at CIA.</td>
</tr>
<tr>
<td>Evidence indicating a heightened degree of attention was paid by senior civilian officials to a particular area of operational concern within the overall threat environment.</td>
<td>Yes</td>
<td>Yes, as a result of the implications for CND based on our offensive capability development as well as various intrusions in USG systems.</td>
</tr>
<tr>
<td>Pressure was brought to bear by an external civilian organization(s) on the IC or DoD.</td>
<td>Yes</td>
<td>Yes, although it was civilian repression of NSA activities during first half of time period and some civilian supportive pressure at NSA during the second half of this time period. There is no evidence in the case history of external pressure brought to bear at AIA or CIA during this time period.</td>
</tr>
<tr>
<td>Civilians exerted control over appointment of senior officials that would carry out policies deemed necessary for innovation in this area of operations to address the perceived external threat.</td>
<td>Yes</td>
<td>Yes, via the reassignment of MG Ken Minihan to NSA from DIA during the second half of this time period. However, it must be noted that the civilians were internal to DoD, and not congressional members of staff. There is no evidence of this dynamic at CIA during this time period.</td>
</tr>
<tr>
<td>Civilians changed or modified budget requests submitted by an IC or DoD agency to reallocate resources in order to foster innovation to be applied against the threat they wanted addressed.</td>
<td>Yes</td>
<td>Yes, although it was civilian repression of NSA IW activities with application to AF and USN during first half of time period via Murtha’s activities. This was not intended to foster innovation. Additionally, overall NSA budgets continued to be cut throughout this time period.</td>
</tr>
<tr>
<td>Internal pushback or resistance occurred after a civilian-led external intervention called for an expansion of intelligence areas of operations.</td>
<td>No</td>
<td>No, not in first half of time period at NSA. Some evidence of this dynamic exists during the second half of this time period at NSA. No evidence of internal pushback at AIA or CIA exists in either portion of the time period according to the information compiled in the case history.</td>
</tr>
</tbody>
</table>
Evidence indicating that intelligence agencies adopted research and development or applied science policies favored by civilians as a result of their intervention. | No | There is no evidence in the case history that the intelligence agencies adopted research and development or applied science policies favored by civilians as a result of their intervention during this time period.

Doctrine preceded technology. | No | There is no evidence of this dynamic in the case history.

**Interservice Rivalry Theory 1992-1996**

The main tenet of interservice rivalry theory states that conflict is due to (financial) resources needed to execute a primary mission(s) are limited or perceived as being limited. While resources were scarcer across the board during this time period, this became an impetus for internally focused creative innovation at AIA, not the cause of conflict between constituent service elements per se as the interservice rivalry theorists would predict.

However, a rivalry between service branches over AIA-developed IW technology did occur over time, and it was related to future mission relevance. This was driven, at least in part, by the 1992 IW order and the MOP 30 implementation instruction, which led the services to create IW elements, and attempt to stand-up a capability, although by several accounts the non-Air Force service branches lacked both mission clarity and technological capabilities. AIA’s successes in creating demon dialers and associated IW tools resulted in interservice turf wars regarding ownership of the mission space between the Intelligence, Research and Development (R&D) and Communications entities, among others.\(^{470}\) Principally, the resultant bureaucratic battle was “fought over who owned the

---

access points...and focused on divvying up the pie between the Title 10 and Title 50
organizational elements. Each of the services rushed to develop new (tool)
capabilities, while refusing to share the results with each other due to a perceived
competition over status in the new domain. This shows that the armed services sought
to maintain their current mission responsibilities while attempting to capture a share of
the new IW mission space. Although there is no evidence of a formal evaluation
mechanism to indicate that one service component’s technical approach was more
effective than another’s during this time period, it is clear that the Air Force Intelligence
Agency, a NSA cryptologic element, had the most advanced capabilities according to the
interviews conducted. AIA’s success led to a scramble at the Pentagon to “divvy up the
pie,” the pie being tools and/or capabilities created at AIA. There is no direct evidence
that any one service intelligence component impinged on or co-opted the traditional
mission space of a sister agency, although it is clear from the interviews that the Navy
has a long and storied history of SIGINT collection, and saw themselves as an
organization that predated NSA/CSS, and therefore an expert in the realm for many,
many years prior. However, since IW/IO was effectively a new mission area it would
be difficult to argue that co-option actually occurred.

473 During this time frame the Navy Information Warfare Activity (1994) and the Army Land Information
Warfare Activity (1994) were created and stood up (Michael Warner, “Cybersecurity: A Pre-History,”
474 Minihan describes CNO. General Kenneth Minihan, interview by the author, Washington, DC, January
14, 2015.
475 Admiral William O. Studeman, interview by the author, Severna Park, MD, August, 2015; William
Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.

179
The case history shows evidence that technology development preceded doctrinal development, and this is consistent with interagency rivalry theory. The development of 1980s and early ‘90s IW technology preceded the issuance of the 1992 IW order and the MOP 30 instruction, and continued to advance in the absence of any concrete guidance as to how to achieve the amorphous goal of “computer network attack” called for in the IW order or “destruction” as called out in MOP 30. In fact, MOP 30 emphasized that IW did not really require any new capabilities, but was in fact based on existing systems and modes of operation.

Additionally, DoD, writ large, apparently focused on computer network defense, not offensive development, as a response to the growing threat environment during this time period. This inclination is to be expected: It is expected that DoD would want to ensure that computer systems would work on demand as designed and intended, as assured functionality was fundamental to mission needs. IT systems were seen only as an enabling or support component for warfighting—not a warfighting component themselves. Indeed, the Defense Science Board crystalized this thinking in 1994 with its observation that “the threat causes concern over the specter of military readiness problems caused by attacks on defense computer systems,” which was underscored by the recent hacking of the Air Force Research lab in Rome, NY.\(^476\)

At the macro level, both NSA and CIA experienced substantial cutbacks in funding and personnel during 1992-1996 according to the interviews conducted, although there is no evidence that the main interagency conflicts that developed were about budgetary allocations or resource scarcity per se.

What drove the NSA and CIA interservice rivalry were concerns related to current and future mission relevance for both organizations. According to the case history, at a basic level, this was due to technological considerations and who was considered to “own the target.” Unless each organization adapted accordingly, the changes in ICT were likely to result in a diminution of intelligence collection capabilities. At NSA, the concept of Global Network Intelligence was viewed as a new and comprehensive SIGINT activity that was critical to NSA’s future. This was driven by the realization that computers were becoming more tightly integrated into telecom nets, where the most useful data from an intelligence or a SIGINT viewpoint would be resident in a computer memory, rather than passing over a communication channel. This change resulted in an internal realization by Bill Crowell that success in both SIGINT collection and IW attack capability development would require NSA to establish a global network penetration mission.

Similarly, CIA was concerned that it “might not be ready to exploit the rapid expansion and utilization of advanced technology in various target domains.” This concern over future mission relevance and the need for associated capability development drove the stand-up of Glenn Gaffney’s IW analysis group, which soon morphed into the

Clandestine Information Technology Office, which brought Jim Gosler’s technical experience from his time at Sandia and NSA to bear on behalf of CIA. CIA came to view “espionage as the key to digital intelligence,” where the Clandestine Service members would be the “pathfinders for the CIA’s cyber offensive against an array of targets. As adversaries grew to acquire and use digital data (as the Internet expanded) so would the CIA’s cyber operations.” Ultimately who “owned” the rights to access the targeted system and the associated electronic data at rest drove a significant portion of the rivalry.

Both NSA and CIA sought to maintain their current mission responsibilities and attempted to capture a share of the new mission area through leveraging their core competencies in SIGINT and HUMINT. NSA sought to establish dominance in this emerging domain of operations and claim ascendancy over the targets. A reasonable reading of the case history would indicate that NSA and CIA came to the same conclusions regarding the threats they were trying to address, which were related to national intelligence collection priorities; however, based on the core competencies that each organization possessed, the technical approaches were somewhat different. Clearly, NSA and CIA had differing operational and doctrinal preferences for how to meet intelligence collection requirements which substantially influenced how targets were approached, perceived ownership of those targets and which exploitation methodologies were used. This ultimately impacted how the organizations interacted with each other, which led to an ongoing interagency conflict. NSA preferred an “active SIGINT” approach, which sought to leverage “the sophisticated telecommunications and data

---

networks now being deployed worldwide [that] make it possible to deny and degrade a potential adversary’s command and control communications and sensitive commercial and diplomatic communications from great distances with little or no risk to life and limb.\textsuperscript{481} NSA chose a unilateral and permissive reading of its essentially exclusive authorities for SIGINT collection under EO 12333, and made a conscious choice to legally justify and utilize its network collection capabilities under the concept of “active SIGINT.” This strategy ensured the capabilities and implementation strategy being developed for CNE and CNA fell under NSA’s legal authorities.\textsuperscript{482} Furthermore, NSA, under LTG Minihan’s leadership, sought to preempt the entirety of the technological approach and the mission field at large through interagency dominance as part of the initial discussion for what came to be known as the Information Operations Technology Center (IOTC). This differed from CIA’s approach, which at the time included the insertion of “giant old floppy discs” by assets or operators on site or other HUMINT-Technical operational techniques.\textsuperscript{483} Minihan’s assertive move to claim the entirety of the cyber operational area for NSA resulted in the conclusion at CIA that it could not “let NSA own this organization or else we will be shut out.”\textsuperscript{484} CIA’s institutional perspective was that it had been “stealing computer data since foreign secrets first landed on a hard


\textsuperscript{482} William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.


\textsuperscript{484} Glenn Gaffney, interview by the author, McLean, VA, November 23, 2015.
drive…[and in] cyberspace since its inception.”485 “To CIA, ‘data at rest’ was not within the purview of NSA’s SIGINT (radio signals, telephonic communications et al) collection domain of operations, but a legitimate CIA area of intelligence collection activity. CIA believed NSA’s legitimate and traditional collection should be limited to midpoint interception, and therefore it should not be tunneling into computers where data resided ‘at rest’ and then exfiltrate that information….”486 NSA clearly had a differing perception regarding the levels of effectiveness between the two organizations: It believed it rightfully should be the master of electronic or computer-based information collection, and even went as far as to seek to create a new category of intelligence collection, alternatively called INFOINT or COMPUINT in 1994,487 although the new category did not gain traction and was never formalized as a separate collection discipline.

NSA and CIA appeared to co-opt portions of each agency’s traditional mission space as the targets, and the targeted information, converged onto computer systems. Clearly, both organizations took adaptive approaches based on their core competencies and institutional perspectives to reach for the same types of coveted information on these systems. This essentially made both organizations less susceptible to external interference as they built out their respective capabilities. Essentially, up until the end of 1996, technological innovations at NSA and CIA were largely the product of long-term development projects within the community without significant external civilian direction or support. There is no evidence that an evaluation by senior civilian leadership led to the

486 William Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
selection of a “winner” based on the perceived effectiveness of one IC organization’s approach to innovation over another’s. Based on NSA and CIA activities during this time period, IW/CNE technology (and tradecraft) development preceded in absence of any doctrinal formalization in the IC. In late 1996, DoD produced a revised IW doctrine, now broadly called Information Operations, which formalized the term computer network operations. While this DoD doctrine is interesting as persuasive authority, this document essentially described activities both organizations were already engaged in for some time. See Table 11 for a summary.
<table>
<thead>
<tr>
<th>Interservice Rivalry Theory 1992-1996</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources for the service’s primary mission(s) are limited or perceived as being limited.</td>
<td>Yes</td>
<td>Due to a search for the so-called peace dividend, NSA experienced budget cuts.</td>
</tr>
<tr>
<td>Rivalry-based behavior between IC or DoD organizations was driven by concern for current or future mission relevance.</td>
<td>Yes</td>
<td>A rivalry developed between service branches over AIA-developed technology; NSA/CIA experienced a substantive rivalry in the latter part of this time period.</td>
</tr>
<tr>
<td>IC or DoD organizations sought to maintain their current mission and attempted to capture a share of the new mission area.</td>
<td>Yes</td>
<td>Both NSA and CIA sought to maintain their current mission and attempted to capture a share of the new mission area; AIA also did this under Minihan’s tenure.</td>
</tr>
<tr>
<td>IC or DoD organizations came to different conclusions or perceptions regarding the threats they were trying to address, which resulted in different mission need requirements and operational doctrine preferences that substantially influenced or defined how the organization interacted with other services.</td>
<td>Yes</td>
<td>NSA and CIA came to different conclusions as described by this dynamic that substantially influenced or defined how the organization interacted with other IC elements; DoD also came to a different conclusion, and as a result saw this issue from a CND perspective.</td>
</tr>
<tr>
<td>The Intelligence Community leveraged its traditional operating experience and allowed it to expand into a new mission domain making it less susceptible to external interference.</td>
<td>Yes</td>
<td>IW derived from SIGINT and EW and IW to target.</td>
</tr>
<tr>
<td>Co-option of one IC or DoD organization’s traditional mission space by another organization occurred.</td>
<td>Yes</td>
<td>NSA co-opted aspects of what CIA thought was their traditional mission space through CNE methodologies.</td>
</tr>
<tr>
<td>An evaluation mechanism utilized by senior civilian leadership during an interservice competition led to the selection of a winner based on the perceived effectiveness of one IC organization’s approach to innovation over another’s.</td>
<td>No</td>
<td>There is no evidence of a formal evaluation mechanism in the case history during this time period for NSA and CIA. However, DoD leadership recognized AIA’s initial successes in IW during this time period and sought to “divvy up the pie” related to their capability developments.</td>
</tr>
<tr>
<td>Technology development preceded doctrine development.</td>
<td>Yes</td>
<td>Ongoing IW and CNE technology development and activities during this time period preceded doctrinal development and publication.</td>
</tr>
<tr>
<td>Technological innovations were largely the product of long-term development projects conducted within or at the direction of the Intelligence Community with important civilian support but without significant civilian direction.</td>
<td>Yes</td>
<td>Ongoing IW CNE activities during this time period were a result of JSSG and STO cell developments that occurred in the previous time period.</td>
</tr>
</tbody>
</table>

Note. Gray cells identify common hypothesis elements that overlap across theories.
Intraservice Rivalry Theory 1992-1996

The case history shows the presence of strong senior intelligence officer within the Intelligence Community who served as a champion for the creation of computer network operations as a major military innovation. The case history also shows significant internal conflict as a result of a battle over maintaining the status quo activities of NSA versus implementing activities necessary to execute a new theory of victory on the battlefield. The assembled evidence does not indicate any significant role being played by the international threat environment during this time period as a driver of the innovation. There is strong evidence of a predoctrinal new theory of victory as well as evidence that technological advances preceded the creation of doctrine. There is minimal evidence of civilian intervention during this time period. This time period is directly consistent with Stephen Rosen’s Intraservice Rivalry theory as an explanation for the creation of a major military innovation.

Elements of CIA’s IW/IO program development during this time period include the presence of strong intelligence officer championing and minimal internal conflict over implementing a new theory of victory. The case history does include evidence of competition over who would “own” the new capability and manage the activities of CITO, which led to a dual reporting structure to the heads of both the Directorate of Science and Technology and the Directorate of Operations. Although potentially suboptimal in some instances, this compromise seemed to be a workable arrangement that did not cause significant operational impediments or implementation issues, and therefore will not be addressed any further in this section.
The NSA portion of the case study shows direct evidence that LTG Minihan formulated an innovation strategy that clearly includes both intellectual and organizational components. This strategy began to take hold during his tenure at AIA and became fully realized in his capacity as DIRNSA. This was accomplished by overcoming an apparently ideologically driven bureaucratic mandate to disestablish the AF Intelligence Command (AFIC) issued by the AF Chief of Staff, who had a pro-flight (aircraft) bias, and apparently concluded there was no need for AFIC to exist—although according to the interviews, this decision was made without significant justification or elaboration. To achieve the organizational basis of his IW strategy, Minihan was able to successfully advocate for and carry out a combination and conversion of existing AF Intel organizational components into the newly branded AIA, which was then coupled with a newly created entity, the Air Force Intelligence Information Warfare Center (AFIWC). The intellectual component of Minihan’s vision of how the next war would be fought and won was articulated as a visionary and forward-leaning approach to operationalize “Information Warfare” as a multi-intelligence (MULTI-INT) disciplinary approach. In addition to his organization’s traditional intelligence officer cadre, Minihan began to create new career pathways by converting young electronic warfare technologists into innovative “demon dialers” dedicated to Information Warfare tool and strategy development, and who were free to create capabilities without the impediment of pre-existing requirements. Once these newly developed capabilities were successfully demonstrated, follow-on capability needs flowed from AIA’s operations, IW warfighting.
and cryptologic centers to create fulsome versions of 21st century Information Warfare exploitation tools. These successes led to the allocation of more resources to support the emerging effort, and brought the attention of other AF and armed service components who became interested in the IW capabilities being created. As a result of Minihan’s initiatives, these capability development activities continued throughout the 1990s and resulted in usable CNE and CNA tools.

Once Minihan was ordered to lead NSA, he continued to leverage the totality of the lessons learned from previous Gulf War-era telecom exploitation activities and his IW capability development experience at AIA. At NSA, Minihan championed the development of computer network exploitation and computer network attack capability through a strategy designed to establish “access access access” and the use of computer network tool technology templating. This continuing tool development, which was designed to operationalize a new theory of victory, soon became known as Information Operations, and was ultimately designed to wage “warfare in cyberspace’ utilizing specific types of weapons including viruses, worms, logic bombs, trojan horses, spoofing, masquerading, and ‘back’ or ‘trap’ doors…that could be extremely destructive to any society’s information infrastructure.”

---

Information Operations, an extension of the technical work started during the 1980s, drew upon elements of compartmented CNE activities conducted during Adm. McConnell’s tenure as DIRNSA. This advanced capability development did not come to fruition easily and was met by direct bureaucratic resistance from status quo constituencies within NSA. Throughout this time period, the vast preponderance of the permanent NSA bureaucracy did not believe it was necessary to prepare capabilities for the onset of the Information Warfare age and would not participate in interagency IW meetings and activities. This attitude was likely driven by NSA Seniors (Senior Executive Service members) who would not accept that signals intelligence strategies needed to evolve from passive to active SIGINT collection, despite ongoing evidence of a rapidly changing information and communications technology environment that would soon leave NSA collection effectively deaf and blind unless a course correction was made. Their overriding belief was that traditional SIGINT/Cryptology was the mission that needed to be prepared for, invested in and executed. Essentially NSA, as an organization, considered Information Warfare as “Not Their Business.” Key constituencies within NSA still possessed an institutionally based fear that Information Warfare would compromise the Agency’s historically key, core missions: Any movement in to the realm of IW would cause a reduction in budgetary resources for traditional efforts that revolved around SIGINT and information security. These constituencies, over time, created significant structural stovepipes based in part on the power of each

492 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
493 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
494 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
individual Group leader, and various internal parochial interests within each group’s organizational structure. This resulted in intransigent bureaucratic pathologies leading to suboptimal outcomes that tended to preserve existing missions, operational methods, and crush efforts at technological innovation.

Minihan methodically ordered a series of organizational and systems component integrations which eventually had a cumulative, transformational effect to remake NSA into an organization that could successfully fight and win the next war, although these initiatives were only partially completed during this time period. To help institutionalize the warfighting future LTG Minihan envisioned, he named Bill Black as his Special Assistant for Information Warfare and empowered Black to start instituting the necessary changes to operationalize the new theory of victory. This essentially provided the basis for a new distribution of power within NSA, as Black placed various like-minded personnel in key positions with NSA as part of strategy to establish the technological capabilities necessary to achieve the new theory of victory. The technological approach initiated by Minihan and Black was designed to advance the wholesale creation of advanced IW capabilities that would “irrevocably change the SIGINT world within NSA.” These moves clearly activated a bureaucratic imperative to preserve existing passive SIGINT collection missions and ways of operating at NSA, and can viewed as an ideological struggle between the agents of change and an entrenched bureaucracy that “doesn’t get it.”

495 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
496 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
497 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
Throughout this time period, it appears a conscious effort to support the technical approach of Denis Chiari and his G44 work group was made by Studeman, McConnell and Minihan, and Bill Black as they strove to foster the development of mainstream, acknowledgeable CNE capabilities. G44, and elements of its predecessor organizations, were engaged in compartmented activities, and therefore operating outside of traditional NSA SIGINT channels for a substantial period of time. Bill Black fostered a relationship with Chiari, who was “ostracized” by other elements of NSA due to the internal political/policy view of these activities, and endorsed Chari’s technical approach as the future of NSA once he was placed in charge of IW by Minihan. Black specifically introduced Dennis Chiari to all the NSA seniors, explained the technical CNE capabilities G44 and successor organizations like K 7 possessed and explicitly told them “this is what we are doing and this is where our future is.” Elements of G group, which essentially started operating in the mid-1980s, engaged in self-sustaining organizational activities and were empowered to create CNE capability innovations that allowed NSA to maintain collection access despite dynamic changes in the ICT. This work was achieved—albeit on a small scale—by a small group, without the need for organizational changes elsewhere at Ft. Meade, until the innovation was ready to be brought forward and institutionalized with NSA.

As part of this process, LTG Minihan realigned NSA, disestablishing the largest NSA component, A group, to be able to focus on CNE/CNA development which allowed

---

498 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
significant funding allocations to be applied against the G group-developed technical approach as part of the overall strategy for “winning the next war.” G Group’s capabilities and activities can be categorized as a long-term development project that was evolutionary, not revolutionary in nature, and set the stage directly for this technical approach to become a strategically useful option for the Unites States over time. See Table 12 for a summary.
Table 12. Intraservice Rivalry Theory 1992-1996 MMI Hypotheses Analysis

<table>
<thead>
<tr>
<th>Intraservice Rivalry Theory 1992-1996</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respected senior officers formulated a strategy for innovation which possessed both intellectual and organizational components.</td>
<td>Yes</td>
<td>NSA’s strategy with respect to Minihan’s theory of access coupled with G Group’s technical approach provides evidence of this dynamic. Similarly, CIA’s strategy for IW was influenced by STO cell activities, IW analysis and National Lab activities to create CITO.</td>
</tr>
<tr>
<td>An ideological struggle manifested within a particular IC or service component revolving around “a new theory of victory,” which included an explanation of what the next war will look like and how leaders must fight it if it is to be won.</td>
<td>Yes</td>
<td>NSA’s IW activities triggered a struggle around a new theory of victory in late 1996.</td>
</tr>
<tr>
<td>A bureaucratic imperative to preserve existing missions and ways of operating attempted to crush the impulse to make technological innovations.</td>
<td>Yes</td>
<td>Yes, NSA’s G44-related activities led to the group leader being ostracized. Similarly, that same type of dynamic played out through Congressional appropriations, resulting in the disestablishment of IW programs by Rep. Murtha.</td>
</tr>
<tr>
<td>A conscious effort was made by leadership to empower a small group of talented individuals to operate outside of normal bureaucratic channels to foster bureaucratic change.</td>
<td>Yes</td>
<td>Bill Black was empowered by Minihan. Black in turn consciously empowered G44 as the future of NSA’s operational approach to collection.</td>
</tr>
<tr>
<td>The innovation program was promoted as an evolutionary rather than a revolutionary system.</td>
<td>Yes</td>
<td>This dynamic can be seen at both NSA and CIA; AIA’s approach was actively promoted as revolutionary at first.</td>
</tr>
<tr>
<td>Initiating the innovation and bringing it to the point where it provided a strategically useful option was accomplished when money was tight.</td>
<td>Yes</td>
<td>This dynamic can be seen at NSA and IOTC for foundational CNE and CNA capability development; this dynamic seemed to exist at CIA as well due to overall budget reductions during this time period.</td>
</tr>
<tr>
<td>A more decentralized organization was created within the agency that was designed and empowered to create and effectively execute an innovation without the need for organizational changes elsewhere in the agency.</td>
<td>Yes</td>
<td>Both G44’s CNE activities, as well as NSA IW activities, can be seen to have benefited from this dynamic.</td>
</tr>
</tbody>
</table>
New career paths were created from within the organization by senior leadership to ensure incorporation of key skills necessary to support the new theory of victory.

Yes

The IW special assistant to the Director provides evidence for this hypothesis. Similarly, the creation of AIA’s demon dialers supported the new theory of victory during this time period. The creation of an IW branch at CIA initiated this new career path, which was then pushed forward by additional methodologies taught by the head of CITO at CIA.

A new distribution of power within the IC or service emerged as a result of an ideological struggle manifesting itself as a new senior leadership rank, billet, or command.

Yes

The creation of the Special Assistant for IW at NSA is indicative of this dynamic. This same type of new senior leadership rank was created at CIA, although it was less controversial. What was at issue was who would control the capability.

Technology development preceded doctrine development.

Yes

Ongoing IW and CNE technology development and activities during this time period preceded doctrinal development and publication.

Technological innovations were largely the product of long-term development projects conducted within or at the direction of the military with important civilian support but without significant civilian direction.

Yes

Ongoing IW CNE activities during this time period were a result of JSSG and STO cell developments that occurred in the previous time period.

Note. Gray cells identify common hypothesis elements that overlap across theories.
CHAPTER 5. 1997-2004

Introduction

Chapter 5 continues to trace CNO development efforts at NSA, CIA and DoD during the seminal 1997-2004 time period. Ken Minihan and Michael Hayden, supported by the efforts of Bill Black, championed significant advances in computer network exploitation and computer network attack capability developments. These advances were produced through the creation of the interagency Information Operations Technology Center (IOTC) domiciled at NSA and later, the creation of a large Tailored Access Operations component within the newly formed Signal Intelligence Directorate for computer network exploitation.

The first part of this chapter recounts granting computer network attack capability development to NSA and simultaneously chartering the interagency Information Operations Technology Center as the incubator for advanced cyber weaponization approaches. These efforts were bolstered by findings of an After Action report of the ELIGIBLE RECEIVER 97-1 exercise and subsequent evidence of the USG’s own vulnerabilities to computer network exploitation. The chapter examines the NSA 2000 Transformation, a disruptive organizational change management effort designed to industrialize computer network exploitation approaches developed during the 1980s and early to mid-1990s. By the end of the time period, NSA and CIA’s interagency
competition over 12333 authorities and targets was reconciled. DoD, perhaps as a result of STRATCOM’s involvement with the IOTC, recognized the maturity of the intelligence-dependent computer network operations model and began the process of organizing, training and equipping for a computer network attack capability in its planning. This planning, which appears to be heavily dependent upon the capabilities created by the IOTC and TAO, was empowered by the purposeful convergence of CNE and CNA upon reabsorption of the IOTC by NSA in late 2004.\footnote{Michael V. Hayden, “IOTC Mission Accomplished,” Director’s Message: DIRgram-345, posted September 28, 2004.}

The second part of this chapter examines the case history from 1997-2004 against the hypotheses of each of the main MMI theories. Stephen Rosen’s theory of intraservice rivalry possesses strong explanatory power for CNO development during this time period.

**NSA, CNA Development Authority and the Creation of the Information Operations Technology Center: 1997**

On March 3, 1997, the Secretary of Defense officially delegated to the National Security Agency the authority to develop Computer Network Attack (CNA) techniques.\footnote{DoDD 3600.1, Information Operations, dated December 9, 1996, defines CNA as “operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves” (William B. Black, Jr., “Thinking Out Loud About Cyberspace,” Cryptolog 23, no. 1 (March 1997), https://www.nsa.gov/public_info/files/cryptologs/cryptolog_135.pdf).} According to Bill Black, writing in NSA internal publication *Cryptolog*, this delegation of authority was “sure to be a catalyst for major change in NSA’s basic processes and its workforce.”\footnote{William B. Black, Jr., “Thinking Out Loud About Cyberspace,” Cryptolog 23, no. 1 (March 1997), https://www.nsa.gov/public_info/files/cryptologs/cryptolog_135.pdf.} NSA was beginning to understand the new operational domain of cyberspace, which consisted of real elements: “physical assets (computers,
network terminals, satellites, fiber optic cables, etc.) that are virtually “interconnected…
networked…compatible…[and] interoperable.” Black foresaw that cyberspace…will
“emerge as an organizing concept upon which our future operations must focus.”⁵⁰³ The
result is an operational domain where “physical geography becomes less and less
important, and affords opportunities to work with greater and greater amounts of
information at any distance.”⁵⁰⁴ NSA understood the potential for operations in this new
domain.

Black noted, “IW for us, however, is ‘warfare in cyberspace…’” There are
specific types of weapons associated with Information Warfare. These include viruses,
worms, logic bombs, trojan horses, spoofing, masquerading, and ‘back’ or ‘trap’ doors.
They are…very powerful, and, if effectively executed, extremely destructive to any
society‘s information infrastructure.” Further, “For IW purposes, access to…computer-
controlled infrastructures can permit the degradation, disruption, or destruction of the
network and/or the functions they serve. As a result, the ‘computers’ become the
intelligence ‘targets’ of highest priority.”⁵⁰⁵

Simultaneously, the Information Operations Technology Center (IOTC) was
stood-up, at least on paper: “The Director’s authority as Executive Agent for the
Information Operations Technology Center (IOTC) stems from a Memorandum of
Agreement between the Department of Defense and the Intelligence Community which

---

established the IOTC as a joint activity of the Department of Defense and the Intelligence Community. Director of National Security Agency (DIRNSA) has been designated as the Executive Agent (EA) for the operation of the IOTC. In his capacity as EA, DIRNSA, after consulting with the SecDef and the DCI, appoints a Director for the IOTC. The purpose of the IOTC was to serve as a “single center to integrate diverse service and Intelligence Community offensive IO technology development efforts and establish and maintain a national repository for these techniques, expanding a warfighting commander’s options beyond traditional kinetic solutions.”

From Minihan’s perspective, the purpose of IOTC was to take various technology and technology gadgets and make them into cyber exploitation and cyberattack solutions. Minihan had a specific strategy related to the IOTC: He wanted NSA to own the computer network attack and computer network exploitation technology. Minihan believed that NSA needed a technology engine room, and the creation, care and feeding of IOTC would “impregnate” NSA with computer network attack technology capabilities. “The IOTC was a Minihan brainchild: He was applying his concept/theory of Technology Templating for IW/IO; everywhere he went was the center of gravity for this approach.”

---

508 Bill Black was interested in having what was then initially referred to as the Information Operations Center be a NSA-centric covert action arm. Leadership was not convinced of this approach. Another reason he took this approach was because NSA’s budget was declining and the organization needed a “new vision” (General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015).
509 Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
Minihan explained his approach for IOTC to Secretary Perry and Deputy Secretary White that “the emphasis was on the T (Technology) in IOTC, not the O (Operations) as is emphasized in NTOC (NSA Threat Operations Center).” Minihan was acutely aware that several big DoD services did not want NSA to stand-up what was initially, informally called the Information Operations Center (IOC). This was due to the use of the term “Center,” which would indicate that NSA was in charge of the mission area. To overcome this bureaucratic sensitivity, NSA called it IOTC. When DoD tried to locate the new organization at a different location, Minihan insisted to Secretary Perry that the IOTC had to be at Ft. Meade because the SIGINT technology base is at Ft. Meade. Minihan’s overall strategy related to housing IOTC at Ft. Meade was directly related to the fact that NSA understood the underlying technology, and could scale it to “industrial strength” to fill the entirety of the mission space. He also recognized that CIA did not have the technology NSA possessed, nor could CIA scale the technology.

511 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015; Gaffney stated that CIA was still in the process of organizing for its conception of an IOC, which was intended to be a whole government effort when Minihan made his move (Glenn Gaffney, interview by the author, McLean, VA, November 23, 2015). This approach was due to Minihan’s belief that a cybercommand-type structure was going to be stood-up eventually, thus making cyberattack a military enterprise. However, whenever this change might be decided up, it would be too expensive to replicate the technology being developed and held by NSA (General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015).
512 Minihan stated, “Think of Ft. Meade as the Global Center of Excellence for Cyberwar”; everything that exists today at Ft. Meade is a result of decisions made during this time period (General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015).
513 Based on NSA’s previous experience in operating a large-scale, global SIGINT collection enterprise.
514 Part of this approach, as indicated from a now-declassified NSA Cryptolog, might have included the concept of Technology Templates: “The Information Operations knowledge base is ‘envisioned…as a series of…nine distinct templates’ that, when combined together, form a very powerful and essential tool for the effective prosecution of any information operation.” The templates are Domains of Influence, Information Infrastructure, Technology, Vulnerabilities, Capabilities, Access, Measures of Effectiveness (MOE)/Impact, Rules of Engagement (ROE)/Motivation and Plan (National Security Agency, redacted author, “Thoughts on a Knowledge Base to Support Information Operations in the Next Millennium,” Cryptolog 23, no. 1 (March 1997)).
based on their core competencies, although he recognized the organization possessed some indigenous capability. Minihan summed up his approach to CNA/CNE technology development in the following way: “If you don’t want it to scale, then it can be a CIA (CITO) capability with NSA technical assistance.” The DoD historian stated that as a result, today, NSA is a chainsaw and IOC is a scalpel.

The IOTC faced formidable opposition from several quarters: from within NSA, from CIA, and from the military services. The top cover provided by Minihan, Perry, Tenet and Shalikashvili proved instrumental in establishing the organization. At first, DIRNSA Minihan was IOTC’s only champion inside of NSA. In fact, Don Lewis, the first IOTC director, left after just six months, and soon retired; Bill Black became a casualty of the stand-up process as well. Bill Black stated that after creating the Information Operations Technology Center in 1997 (which was conceptualized with General Minihan over the course of a single weekend planning session, and described later in the press as a bruising process), he informed Minihan that he would need to retire.

---

515 According to Minihan, CIA had their own “G Group” at the time (General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015; also, National Security Agency, redacted author, “Thoughts on a Knowledge Base to Support Information Operations in the Next Millennium,” Cryptolog 23, no. 1 (March 1997)).

516 And presumably, successor organizations like the Information Operations Center (IOC)


518 Both tools are highly effective, just different mechanisms to achieve a goal (Department of Defense Historian, name withheld upon request, interview by the author, Maryland, May 22, 2015).


from NSA because the Center would irrevocably change the SIGINT world within NSA. As Black described it, he “had to get out of the way so that the [institutional] changes I was championing could be put into place.” To accomplish these changes Black, as the special assistant for IW, purposefully made himself the personal lightning rod for the totality of institutional push back and negative attention. Black, a consummate NSA maverick who, over 35 years, honed extremely effective bureaucratic skills, purposefully stacked the staff with personnel he knew would carry out the paradigm shift for NSA once he was gone. If he stayed, he feared that the bureaucracy would galvanize their dislike for him and align to stop the initiative from taking root in the organization. His position, “centered around technology and NSA’s role as the dominant provider and ‘understander’ of that technology. No one replaced Black in the IW post when he left.”

Bill Marshall was asked to interview for the IOTC Director’s position and soon took over as the new Director. Marshall was painfully aware that the IOTC was controversial. According to Michael Hayden, Bill Black, who was “disillusioned and frustrated, warned Marshall that, one way or another, he was bound to fail. If he actually succeeded operationally, NSA seniors would hate him. On the other hand, if he simply failed, he would just be viewed as incompetent. Similarly, when DIRNSA Minihan hired Marshall, he told him that everyone believed that the IOTC was only Power Point deep in substance. He challenged Marshall to produce real results; to build coalitions across DoD and the IC, and to get the resources he needed to do the job. In return, Minihan promised

---

him top cover against those who would oppose him and try to starve the project." \(^{522}\) In fact, Marshall encountered significant internal resistance to the changes the new organization represented: “The O6 level\(^{523}\) personnel for Concept of Operations were trying to kill the new organization while standing it up!”\(^{524}\) Moreover, the personnel in the mid-tier level management also fought the IOTC’s creation and operation due to rice bowls (parochial interests)…”\(^{525}\) However, the organization had very senior leadership top cover—specifically, the Chairman of the Joint Chiefs of Staff, the Director of Central Intelligence (DCI) as well as Secretary of Defense William Perry. As a result of this high-level interagency protection, the joint organization was stood up successfully.\(^{526}\) Bill Marshall provided his perspective, “Some Generals did not have the vision that DIRNSA Minihan had: They only saw cyber as an M-16—a tactical tool that must be folded into the battle concept.”\(^{527}\)

After its creation, and in order to achieve its aims, the IOTC needed a formalized concept of operations (CONOP) document, which Marshall said was “fought over and bled over within DoD—Blood was poured over the creation of the IOTC CONOP

---

523 O6 is the military rank of a Colonel or Navy Captain, equal to a GS-15 level civilian government official. O7 ranks are Brigadier Generals or Rear Admiral level, and the corresponding civilian flag officer level is Senior Executive Service or Senior Intelligence Service.
525 One key NSA insider who did not try to kill IOTC, although he had a bureaucratic incentive to do so, was Denis Chiari, the head of NSA section G44 that was a precursor to NSA’s Tailored Access Operations (TAO). Chiari sympathized with Marshall as he experienced the same institutional intransigency years before with the TAO precursor organizations (William P. Marshall, interview by the author, Washington, DC, May 2015).
Marshall was well aware that the service components did not want the IOTC to be created in the first place, as the IOTC was taking money and authorities away from the services.

From an Air Force perspective there were a variety of issues in the beginning. “There was no way in hell we would put our source code in there until we knew that our close hold special programs would be protected.” Additionally, “some of the tools developed were for specific purposes and needed Air Force capabilities to be useable,” while “other tools were not fully useable yet. We didn’t want to share all of our capabilities until we knew that the first three items were addressed.” Furthermore, “funding became an issue—everyone became enamored with cyber—however, there were X number of dollars available; there were bright ideas, but no money; in order to fund the bright ideas programs were going to have to give up some capability that had already programmed for—this was a zero sum game—what was programmed for already might have a higher mission salience in some other area. Part of the issue was that cyber was treated in stovepipe and not integrated across the enterprise.”

Other issues also arose. The “1st IOTC director jumped [forward] more quickly than the services seemed ready for in light of concerns mentioned above and therefore not much happened fast—also we were committed to providing capabilities through the air

---

530 Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
531 Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
532 Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
component commander—'joint’ had not been worked out yet for cyber.”533 The mission
space for “what IOTC did, did not fit the traditional apportionment system…. DoD was
unsure of value of the IOTC versus the normal R&D and apportionment system.”534

Bill Marshall, the second IOTC Director, provides his perspective: “Prior to the
creation of IOTC there were only a handful of capabilities in the services and they were
all in special access programs. There was no integrated use of tools between services—
the IC had the same problem: nobody was talking to each other—the programs were
standalone and the money was protected.”535 Hayden noted, “The label Information
Operations was broad and gave the Center the license to touch on all the IO things you
might ever want to do against an adversary: spy on him; corrupt his network or his
information; or capture his computers to use them to create physical destruction. NSA
could legally only do the first, but since this was a technology rather than an operations
center, it was free to develop tools that could be used by others with different
authorities. It was an elegant solution that got the toolbox for all kinds of cyber
operations filled quickly.”536

533 Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD,
name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
534 Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD,
name withheld at individual’s request, interview by the author, McLean, VA, October 2015. An
apportionment is an OMB-approved plan to use budgetary resources (31 U.S.C. 1513(b); Executive Order
11541). It typically limits the obligations you may incur for specified time periods, programs, activities,
projects, objects, or any combination thereof. It may also place limitations on the use of other resources,
such as FTEs or property. An apportionment is legally binding, and obligations and expenditures
(disbursements) that exceed an apportionment are a violation of, and are subject to reporting under, the
Antideficiency Act (31 U.S.C. 1517(a)(1), (b)). See section 145 for more on reporting violations of the
Antideficiency Act (United States Office of Management and Budget, OMB Circular No. A–11, 2016,
s120.pdf).
536 Michael V. Hayden, Playing to the Edge: American Intelligence in the Age of Terror (New York:
The IOTC Concept of Operations describes the IOTC’s primary customers as “CNA, exploitation, and related technology developers and operational users from throughout the DoD and IC. Specifically, the IOTC anticipate the following organizations to be major customers for its products and services: Office of the Secretary of Defense (OSD), Joint Staff, Director for Operations (J-3), Joint Staff, Director for Command, Control, and Communications Systems (J-6), Unified Commands, Military Services, Air Force, Army Marine Corps, Navy, Central Intelligence Agency (CIA), Defense Information Systems Agency (DISA), Defense Intelligence Agency (DIA) and National Security Agency (NSA)/Central Security Service (CSS).”

Most of the internal IOTC personnel were to be assigned by their parent organizations to serve with the IOTC for a specified period of time and be fully integrated members, with assignments varying in accordance with Memorandums of Understanding established between the IOTC and the participating organizations. The Joint Staff, J-3, was to coordinate the operational interface between the Center and the Unified Commands and their Service Components and “facilitate development of CNA, exploitation, and related technology support requirements, as well as support operational

---


planning.”

CIA was to provide support to for analysis, technology development, and community coordination and offer its expertise in conducting clandestine overseas operations and gearing technology development for those types of operations through existing partnerships with NSA and new partnerships with the IOTC. DIA analysts and action officers were assigned to the Analysis and Assessments Group (AAG) and the Community Coordination Group (CCG) in direct support of the IOTC mission and provide all-source collection support to the Advanced Technology Office (ATO), as appropriate. The CCG’s role was to coordinate IOTC technology development efforts “in satisfaction of validated CNA, exploitation, and related requirements and provide the DoD/IC Steering Group appropriate information and recommendations to facilitate Steering Group decisions and guidance.”

Bill Marshall described the IOTC as having two general components: “The first component consisted of all source intelligence analysts to determine what and who was vulnerable. The second component was responsible for a whole range of tool development, a portion of which was malware and very complicated tool development endeavoring to develop potential capability to affect weapons systems and attempt to

integrate with a service platform.”⁵⁴³ Bill Black offered further specificity as well: “The Information Operations Center [using the proto term for IOTC] is capable of planning and implementing an information operations system in a weapons sense,” and added that “the information operations approach is so different that it will not fit into the older military paradigms. The services must organize and attack the problem differently, coming to grips with the development of new systems that provide powerful weapons, if handled properly.” An official was quoted in a Signal Magazine article as saying that “technology begets doctrine, and doctrine begets organization; we need that sequence of events badly. We have the technology, and now we need a clear-cut strategic doctrine at the national level for information operations.”⁵⁴⁴

**ELIGIBLE RECEIVER: 1997**

The IOTC mission would continue to evolve and mature—and was directly influenced by the After Action Report from the ELIGIBLE RECEIVER 97 Exercises. “In 1997, the Joint Chiefs of Staff (JCS) mandated the conduct of the first ever No-Notice Interagency Exercise (NIEX) based on a Joint Operations (JO) scenario as part of the ELIGIBLE RECEIVER exercise series.”⁵⁴⁵ The ELIGIBLE RECEIVER 97-1 exercises

---

⁵⁴⁵ Stephen W. Magnan, Safeguarding Information Operations Are We Our Own Worst Enemy? (Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 2000), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/summer00/art08.html. No-Notice Interoperability Exercises (NIEXs) (ELIGIBLE RECEIVER) are conducted in accordance with CJCSI 3510.01, “No-Notice Interoperability Exercise Program,” and provide training that is planned and executed with little or no notice to the participants. NIEXs focus on C4I and interoperability issues. Normally, two of these exercises are conducted each year. The ELIGIBLE RECEIVER series of exercises are directed by the Chairman of the Joint Chiefs of Staff and are designed to test DoD planning and crisis action capabilities. ELIGIBLE RECEIVER 97-1 was the first-ever No-Notice Interoperability Exercise (NIEX) based on an IO scenario (Global Security, “Eligible Receiver,” May 7,
were “pitched” to the Joint Chiefs of Staff, partly in response to the pressure DIRNSA Minihan and Deputy Secretary Hamre were receiving from unnamed four-star generals, who were “pummeling them.”

Minihan indicated that the Four Stars were not supportive of the new entry into the computer network attack realm. “They were putting their heads in the sand and not making any attempt to try to understand the new technologies that were now available to us.” The General recounted, almost metaphorically, “when I would go into their offices, there would be a computer on the desk, but it was not turned on.”

In response to the pressure, Hamre sponsored the ELIGIBLE RECEIVER 97-1 exercise and provided the requisite leadership top cover for NSA to showcase a portion of its capabilities, however, “the Army refused to participate in ER 97—they did not see a problem.”

ELIGIBLE RECEIVER was the “first Information Warfare (IW) exercise in this country,” and according to Minihan, NSA “aced it.”

The exercise was set up to give a pass/fail conclusion in response to the question “Are we vulnerable to computer network exploitation/attack?” The rules of play included

---


548 According to William P. Marshall, General Jack Sheehan, who was Commander of the US Atlantic Fleet at the time, believed it was important to test US assertions of superiority in this IW/IO/Cyber domain and, at least in part, also conceived ELIGIBLE RECEIVER 97 (William P. Marshall, email correspondence with the author, Washington, DC, October 2015).


a requirement that NSA had to obey US law. The exercise was broken down into three parts: a Preparation Stage, an Attack Stage, and a Recovery Stage. The scenario was based on a simulated rogue state attack against vulnerable US IT power and communications networks in Oahu, Los Angeles, Colorado Springs, St. Louis, Chicago, Detroit, Washington, DC, Fayetteville, and Tampa. The attackers were to attempt to conceal their identity “and to delay or deny any U.S. ability to respond militarily.” Approximately “thirty-five people participated on the Red Team over 90 days using off-the-shelf technology and software.” The participants were DoD, Joint Staff, the Services, USACOM, USPACOM, USSPACECOM, USSOCOM, USTRANSCOM, NSA, DISA, NSC, DIA, CIA, FBI, NRO, and the Departments of State, Justice, and Transportation. William J. Marshall was NSA’s lead for the exercise—and before the beginning of the exercise Minihan said to Marshall, “if I go to jail, you go to jail.” As it turns out, the Exercise utilized actual attacks on key DoD information systems. NSA Red Team targets included: the National Military Command Center (NMCC) in the Pentagon,

---

551 Minihan’s lawyer was Rich Marshall, who was initially an Air Force Intelligence Officer, then a Judge Advocate General (JAG). Rick was Minihan’s lawyer during ELIGIBLE RECEIVER exercises (General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015; General Kenneth Minihan, interview by the author, Washington, DC, November 24, 2015).


556 Minihan expanded on this quotation in a follow-up discussion, stating that he wanted the legal issues surrounding CNE/CNA to be brought to the frontlines of the discussion: “Furthermore, as DIRNSA, “if I asked G Group to run an exploit and the team made a mistake, and NSA was uncovered, the adversary got to say whether it was an exploit or an attack—those were the types of complexities surrounding the issue at the time—G Group was stuck in that issue, but I had their back” (General Kenneth Minihan, interview by the author, Washington, DC, November 24, 2015).
USPACOM, USSPACECOM, USTRANSCOM, and USSOCOM. “The Red Team intruded computer networks, denied services, changed/removed/read e-mails, and disrupted phone services. The team gained superuser access in over 36 computer systems which meant they could create new accounts, delete accounts, turn the system off, or reformat the server hard drives,” achieving “unprecedented victories over the Blue Teams.” Director Minihan mused, “NSA did not cheat…we didn’t even play hard.”

He also stated that “Defense Logistics Agency was attacked, not exploited—they had to pull their servers offline.” Bill Black, NSA Special Assistant for Information Warfare, commented that “ELIGIBLE RECEIVER was a joke (we had fun…” He also went out of his way to clarify a particular issue as a point of pride: “The Pentagon leadership claimed to have caught our systems penetration at the onset of the exercise….” Black rejected this claim outright and confided that “it was actually during the 43rd intrusion when we were detected.”

560 General Kenneth Minihan, interview by the author, Washington, DC, November 24, 2015. The sponsor for the exercise, John Hamre, was quoted later as saying “The ‘red team’ playing the adversary in ELIGIBLE RECEIVER was restricted to using store-bought computers and hacking tools downloaded from the Internet, but that did not seem to hamper its work” (Michael Warner, “Cybersecurity: A Pre-History,” Intelligence and National Security 27, no. 5 (2012): 781-799).
562 Bill Black, interview by the author, Pasadena, MD, May 1, 2015. The former high-ranking DoD official responsible for IO at the OSD claims that NSA was caught hacking into systems in the early stage of ELIGIBLE RECEIVER exercise by DoD, but they let the exercise go on: “Bill Black (who I love dearly) may not have been knowledgeable about this—MG Casciano called LTG Minihan to tell him that we caught his team doing something. This resulted in our being read in to ER 97 and not able to play and provide guidance to Casciano’s AIA” (Department of Defense, former high-ranking Department of
Bureaucratic battles were embedded behind the scenes of the ER exercise. DoD wanted to incorporate Intelligence Community capabilities in the IW concept of operations. DoD asserted that stealing information from adversaries was a Title 10 (Information Warfare) authority, while the IC insisted that it was a Title 50 (intelligence gathering) authorized activity. As a way to rationalize stealing information under its Title 10 authorities for IW, DoD attempted to change the nomenclature from computer network exploitation (CNE) to computer network reconnaissance, with the premise being that “recon” is a recognized military activity, similar to what Army rangers do behind enemy lines. While this attempt by DoD to grab additional authorities for CNE under Title 10 was stopped, the battle continued for almost two decades. Moreover, the CNE versus recon issue does not just include NSA (Title 50) and DoD (Title 10) competitiveness, but also separately and similarly involved NSA and CIA Title 50 perceived lanes in the road over 12333 collection activities for electronic data.

---

567 William P. Marshall, interview by the author, Washington, DC, May 2015. This is the “Data at Rest versus Data in Motion” controversy discussed earlier. According to William P. Marshall, various rivalries developed: DoD interservice rivalry versus the Intelligence Community; an IC Interservice rivalry (mainly NSA/CIA, although DIA was involved in the early time period in the turf battle over cyber as well); and internal organizational intraservice rivalries at NSA and CIA. Interservice rivalries between each of the military services (i.e., USN, USA, and USAF) were particularly intense. Adding the IC agencies to the mix (e.g., NSA, CIA, and DIA) made this situation even more complex. Marshall asserted that “DIA’s role in the CNO area was more aspirational than real. As the organization charged with producing validated intelligence assessments in support of the military, DIA had to have a role in this new arena. The problem is that this agency lacked the resources and expertise to have a meaningful role in the cyber arena. During my tenures in the JSSG, IOTC, and NTOC, DIA was never a meaningful player. Their main focus in the analytic arena was on IO/CNO intelligence related to Order of Battle and Indications and Warning; however, this intelligence tended to be limited in scope and value and not timely” (William P. Marshall,
According to Jon Kyl, “ELIGIBLE RECEIVER demonstrated in real terms how vulnerable the transportation grid, the electricity grid, and others are to an attack by, literally, hackers—people using conventional equipment, no ‘spook’ stuff in other words.”\textsuperscript{568} DepSec Hamre commented, “We didn’t really let them take down the power system in the country, but we made them prove they knew how to do it.”\textsuperscript{569} Ultimately, “ELIGIBLE RECEIVER was meant to test the premise that the US could win in an Information Warfare conflict. Instead, the exercise found distressing things—that the US was not as good as we thought we were for offensive and defense activities.”\textsuperscript{570} LTG Ken Minihan, USAF, who was the Director of NSA at the time, volunteered to take on one of the actions that emerged from this exercise that dealt with a shortfall in offensive capability. This is what led to the stand-up of the IOTC.\textsuperscript{571}

**Stand-Up of Information Operations Technology Center: 1997**

By the time Bill Marshall took over as Director of the IOTC, it was clear the new organization needed to address one of the key takeaways from the ELIGIBLE RECEIVER 97-1 exercise: The USG needed more arrows in the quiver—“a toolbox” as it was later called—one where capabilities were to be recorded, developed, analyzed,

\begin{itemize}
\item \textsuperscript{570} William P. Marshall, interview by the author, Washington, DC, May 2015.
\item \textsuperscript{571} William P. Marshall, email correspondence with the author, Washington, DC, October 2015.
\end{itemize}
validated and put into use.”\textsuperscript{572} However, “the IOTC was never meant to be an operational entity. The purpose of the IOTC was to be prepared for future conflicts in cyberspace and have tools and capabilities available for those entities authorized to use them.”\textsuperscript{573} IOTC was “designed to understand the USG’s primary adversaries, develop an advanced technological understanding of CNO and create the right tools to operate in the cyber domain—as well as to explore and identify the legal and policy issues for the use of tools and capabilities being developed as well as be the repository for the whole of government CNO tool sets.”\textsuperscript{574} IOTC was a joint DoD and DCI organization that received its strategic direction and resources from OSD (USD(I)) and ODCI.\textsuperscript{575} Despite the misgivings of the service components,\textsuperscript{576} the IOTC was activated in 1998 and housed at National Security Agency headquarters as intended by Minihan and Black as a joint interagency organization. “IWSC (Information Warfare Support Center), a part of the SIGINT Directorate, was NSA’s IOTC interface and interface with the rest of IC and DoD.”\textsuperscript{577} According to the \textit{Washington Post’s} William Arkin, the IOTC brought together a variety of capabilities: NSA’s P42 information warfare cell, CIA’s Critical Defense Technologies Division, and the Pentagon’s “special technology operations.”\textsuperscript{578}

\textsuperscript{575} William P. Marshall, email correspondence with the author, Washington, DC, October 2015.
\textsuperscript{576} According to Michael Hayden the military services were “pushing back hard…[as another agency’s] growth was usually at the expense of their budget top line.” John Hamre, the Deputy Secretary of Defense, finally enlisted DCI George Tenet’s support and then just plain overruled the reflexive service objections to the enterprise (Michael V. Hayden, \textit{Playing to the Edge: American Intelligence in the Age of Terror} (New York: Penguin Press, 2016) Chapter 8).
In public and in private, Secretary of Defense William Cohen supported the new organization. In his annual report to the President and Congress, Cohen discussed the IOTC: “The new Information Operations Technology Center (IOTC) acknowledges a transition in viewing IO threats and targets as technology-centered rather than geography-centered. Through a formal DoD/DCI agreement, the IOTC will enhance IO cooperation throughout the Intelligence Community. Also, the Joint Staff is evaluating potential changes to joint warfighting organizations and processes, to centralize command responsibilities for executing IO campaigns and responses to strategic IO attacks. This requirement was identified during the two primary 1997 IO exercises. Exercise Evident Surprise (March 1997) highlighted the interagency coordination process required to deconflict and execute IO, and Exercise Eligible Receiver (June 1997) highlighted Indications and Warning issues, as well as coordination of responses to IO attacks.”

Similarly, just as Secretary Cohen publicly supported the IOTC, so did the Director of Central Intelligence George Tenet in his public statements: “Our very considerable efforts with the Department of Defense have produced organizational, policy and capability improvements and efficiencies for use in information operations. We recently established a senior-level forum to address Information Operations policy and process issues, responding to long-standing congressional interest in the development

---

579 “Of particular importance early on in the IO developmental period of 1998-2000 were the Bilateral IO Steering and Working Groups (BIOSG/BIOWG) that helped to define IO policy and deconflict IO issues between the DoD and other agencies. Typical members of the BIOWG were at the one-star level, and these members defined the issues and laid the groundwork for the BIOSG, which actually made the decisions and wrote policy at the three-star level to include representatives from OSD, the Joint Staff, and the IC” (“Leigh Armistead, Information Operations: Warfare and the Hard Reality of Soft Power (Dulles, VA: Brassey’s, 2004)).

of just such a policy body. We also created, one year ago, the Information Operations Technology Center at Ft. Meade, MD. The IOTC is another of our joint DoD and Intelligence Community activities, providing advice and developing techniques that can protect US infrastructure and systems.”

Tenet did not mention CIA’s own organization, the Clandestine Information Technology Office, which was now three years into its creation.

Interestingly, Marshall believes that “CIA would have basically preferred that DoD had not undertaken an initiative to enhance offensive capabilities in the CNO arena in the first place, however, CIA seemed to appreciate being a part of IOTC as it provided the agency with a window into what DoD was doing from a policy, technology, and operational perspective.”

“CIA saw IOTC as a window in DoD plans, which were of potential concern to them from an operational standpoint. CIA was concerned that DoD would make mistakes that could or would negatively affect ongoing operations—in practice deconfliction processes never worked perfectly, and therefore left open the possibility for inadvertent errors to be made.”

DIRNSA Minihan’s perspective was that

---

581 George Tenet, “Testimony of Director of Central Intelligence George J. Tenet before Senate Select Committee on Intelligence on the Worldwide Threat 2003: Evolving Dangers in a Complex World,” DCI Worldwide Threat Briefing 2003 (Washington, DC: U.S. Senate, 2003), https://www.cia.gov/news-information/speeches-testimony/1998/dci_testimony_062498.html; Peter S. Duklis, Jr., The Joint Reserve Component Virtual Information Operations Organization (JRVIO): Cyber Warriors Just a Click Away (Carlisle, Pennsylvania: Army War College Carlisle Barracks, 2002), accessed August 30, 2016, http://www.iwar.org.uk/iwar/resources/jrvio/Duklis_P_S_02.pdf. Marshall noted, “The DCI, George Tenet, provided a significant amount of funding to the IOTC in the early years and CIA provided a relatively small number of personnel to the organization. Although the number of analysts and technologists that CIA provided were much smaller in number than those provided by NSA and the Services, the quality of the personnel were uniformly very high and made a disproportionate contribution to IOTC’s mission while I was Director” (William P. Marshall, email correspondence with the author, Washington, DC, October 2015).


“CIA would do the niche areas, and I had no qualms with CIA’s use of the IOTC as a window into DoD or NSA’s plans. I was okay with CIA getting a free look and allowing them to hijack what they wanted. What we had was a command and control issue on operations and therefore we needed a deconfliction mechanism.”

The issue of enhanced security approaches for special access programs and compartmentalization of activities led to Deputy Secretary of Defense John “Hamre’s decision to grant read-ins on special programs related to the IOTC mission space. This decision was made to avoid balkanization of capabilities or replication of efforts which otherwise might easily occur in absence of shared information and situational awareness. The purpose for granting these read-ins and the associated sharing of insights was to facilitate the success of the IOTC, otherwise it would be still-born.”

584 General Kenneth Minihan, interview by the author, Washington, DC, November 24, 2015; this was possibly addressed via the BIOSG Process cited earlier in the chapter as well as DCID 7/3 (1999) (Information Operations and Intelligence Community-related activities) which was the first attempt to put this all together in the IC and establish a deconfliction mechanism. Eventually a Trilateral MOA was created between DoD, DOJ and the IC related to CNE/CNA activities focused on the deconfliction of various activities (Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015). See also Central Intelligence Agency, Director of Central Intelligence Directive 6/3: Protecting Sensitive Compartmented Information Within Information Systems, Policy 1101, Number 6/3, 1999, https://fas.org/irp/offdocs/DCID_6-3_20Policy.htm.

585 According to Marshall, considerable effort had been expended by DoD and IC organizations to provide very tight security protections over the technologies involved; however, he found that “in many cases the technologies and associated vulnerabilities were already well known in the public domain. It would have been much better to have loosened the reins of tight security surrounding the technology aspects in many of these SAPs and other compartmented programs and instead tightly restrict access to information on specific targets, plans, and operational activities, which is where the greatest sensitivities existed.” Marshall indicated that perhaps this was a missed opportunity: “quite frankly, I do not think that we got there—a lot of effective work can be accomplished at the SECRET/NOFORN level of classification without having to go to TOPSECRET/NOFORN or SAP levels of security” (William P. Marshall, email correspondence with the author, Washington, DC, October 2015; William P. Marshall, interview by the author, Washington, DC, May 2015).

What started under General Minihan at AIA was bequeathed to Brigadier General John P. Casciano, who commanded the element from October 1994 - January 1996. When General Hayden took over as the head of AIA in January 1996, the organization he found was structurally mature, but did not have mature computer network attack tools; he described what AIA had developed up until that time as “spray painting and graffiti.”  

However, Hayden stated although he “had only 18 months in San Antonio,…the people were cutting edge and the education they gave me was invaluable when I got to Ft. Meade."  

Hayden and his AIA staff “set out to create our own mandate, namely building out a CNA capability by taking a Title 10 approach—training, organizing and equipping a national cryptologic element, which was possible to do since it was outside the spotlight of the nation’s capital.”  

After his arrival, the staff showed the General what was theoretically possible through computer network attack capabilities; he equated the concepts of operations described to him for the cyber domain as akin to the application of Air Power Theory—not the all-encompassing, yet ethereal Information Warfare definitions that were being slung around at the time (“I still don’t know what IW really means,” he said).  

“The Air Force was out ahead of everybody…it was more mature than NSA’s thinking at this time.”  

However, in addition to being commander, AIA, the General was also director, Joint Command and Control Warfare Center, Kelly Air Force

Base, Texas (known as Signal Hill). As the director for the JC2WC, Hayden was essentially responsible for the MOP 30 Command Control Warfare activities, which included EW, Psyops, OPSEC, Deception and Destruction, a five-element definition the General called “bigger than the great outdoors.”\textsuperscript{591} He made a conscious decision to focus on what is now called computer network operations during this time period. Fortunately, the Air Force did not really adhere to the doctrine in C2W, and Hayden was allowed to narrow it down to CNO, which he considered the most concrete element lurking within the IW and C2W doctrines.\textsuperscript{592} As a dual-hatted commander, his reporting lines were split: As Director for JC2WC, he reported to the head of the Joint Staff, while AIA was actually a component of NSA/CSS, considered a service cryptologic command element, and the two organizations he reported to were philosophically distinct.\textsuperscript{593} Regardless of serving two masters with distinct philosophies, Hayden and his team at AIA continued to develop the CNO capability set over the next 18 months.

Hayden stated, “In September, 1997 we had the chance to demonstrate what we wanted to do to a gathering of Air Force three and four stars. The Chief of Staff, General Ron Fogleman, invited me to Scott AFB [Air Force Base] in Illinois for his semiannual

\textsuperscript{591} General Michael V. Hayden, interview by the author, Washington, DC, December 10, 2015; ongoing conversations with the author, Washington, DC and Arlington, VA circa 2012 to present.

\textsuperscript{592} General Michael V. Hayden, interview by the author, Washington, DC, December 10, 2015; ongoing conversations with the author, Washington, DC and Arlington, VA circa 2012 to present.

meeting called Corona Top. Fogleman gave us an unprecedented two hours on the agenda to demonstrate live some of the tools then under development.”

Hayden’s team had indeed developed some usable tools that clearly progressed beyond “spray painting and graffiti.” However, shortly after the demonstration for Fogelman, Hayden was rotated out for his new assignment as Deputy Chief of Staff, United Nations Command and U.S. Forces Korea, almost 7,000 miles and an entire world away.

**SOLAR SUNRISE and MOONLIGHT MAZE**

As the IOTC was being stood up at Ft. Meade, two high-profile computer network intrusions occurred, perhaps underscoring the importance for the CNE/CNA capability development that was to follow in the coming years. In 1998, an intrusion into the Pentagon’s unclassified networks caused significant concern. The intrusion, code named SOLAR SUNRISE, was characterized to Congress as a tactical level attack by General Minihan, yet sufficiently serious enough for Deputy Secretary Hamre to brief the President on the penetration. According to a GAO report, “over 500 computer systems were compromised using a well-known vulnerability in the Solaris (UNIX-based) computer system, including military, commercial, and educational sites, by (high school-

---

aged) attackers using only moderately sophisticated tools and resulted in data exfiltration.” The Department of Defense called it “the most organized and systematic attack to date,” and although the Department of Justice stated that no classified information was compromised, the intrusion was in alignment with the outcomes of the ELIGIBLE RECEIVER 97-1 exercise.

*Newsweek* published an article regarding what it characterized as “one of the most potentially damaging breaches of American computer security ever” (code named MOONLIGHT MAZE) suspected to have been conducted by “the Russian Academy of Sciences, a government-supported organization that interacts with Russia’s top military labs” and characterized in the article by the Pentagon as “a state-sponsored Russian intelligence effort to get U.S. technology.” *Newsweek* reported that computer systems at the Departments of Defense and Energy, military contractors and leading civilian universities were successfully targeted and the exfiltrated data could have included classified naval codes and information on missile-guidance systems. Once

---


600 A May 2001 article in *Foreign Affairs* magazine stated that there was “a still ongoing operation that American investigators have code-named Moonlight Maze,” which DoD had detected in March 1998 (James Adams, “Virtual Defense,” *Foreign Affairs* 80, no. 3 (May-June, 2001): 98-112).

601 “One defense technician trying to track the computer intruder said to have watched in amazement as a document from the naval facility was ‘hijacked’ from a print queue to a location in Moscow right in front of him. The first Moonlight Maze attack was detected in March 1999. Three months later, U.S. agencies were able to monitor a series of intrusions as they occurred and traced them back to seven dial-up Internet connections located near Moscow” (Leigh Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power* (Dulles, VA: Brassey’s, 2004)).

again Deputy Secretary Hamre briefed congressional committees and was quoted as stating “We’re in the middle of a cyberwar.”

Whether or not the US was really in the middle of a cyberwar at the time is in hindsight, debatable. However, clearly, additional definitional sharpening for what CNA and CNE actually meant was occurring during this time period. On November 6, 1998, CJCSI 3210.01A, Joint Information Operations Policy, defined Computer Network Attack (CNA) as “Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves” and Computer Network Exploitation (CNE) as “Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident within foreign AIS that could be used to the benefit of friendly operations.” The previously issued S3600.1 made no mention of CNE whatsoever, so this represents a doctrinal change. The terminology and definitions of Information Operations were seemingly in a state of constant evolution, which was being compounded by the fact that “all US services-Army, Navy, Marine Corps, and Air Force-have approached IW/IO somewhat differently, viewing them through their individual warfighting lenses.”

NSA and CIA Cooperative Interagency Competition Continues

NSA and CIA continued to try to collaborate and deconflict their institutional perspectives and mission areas during this time period. Gosler said, “There was a lot of friction between Denis Chiari’s organization\textsuperscript{606} and CITO during the 1998 time frame. We held an offsite meeting to better understand each other and establish a partnership-based committee. Most of the junior guys at NSA and CITO had bonded and were carrying out the mission together. The NSA seniors in upper middle management above Chiari were part of the problem, as they were suspicious of CIA. ‘Just tell me why the hell I should trust you guys’…(the inference being that due to the nature of CITO’s mission space CIA had to engage in activities that were by their very nature, clandestine).”\textsuperscript{607} Despite some interagency friction, Gosler says today that “Denis Chiari is a hero for what he accomplished within the NSA culture.”\textsuperscript{608}

The NSA and CIA perspectives on this issue were clearer: It was a mission area of SIGINT and HUMINT technical operations that produces SIGINT.\textsuperscript{609} In 1998, a meeting was held in Rod Sorkin’s office. “Rod, who was the head of DDT [NSA’s Deputy Directorate for Technology] at the time, met with Jim Gosler, the head of CITO

\textsuperscript{606} Presumably K 7, a successor organization to G44. See Appendix A.
\textsuperscript{607} Admiral William O. Studeman and James (Jim) Gosler, interview by the author, Ft. Meade, MD, December 2, 2015.
\textsuperscript{608} Admiral William O. Studeman and James (Jim) Gosler, interview by the author, Ft. Meade, MD, December 2, 2015. See Appendix A.
\textsuperscript{609} Admiral William O. Studeman and James (Jim) Gosler, interview by the author, Ft. Meade, MD, December 2, 2015.
and Rich Taylor, the head of the DDO to answer a question: Is it time to create a senior executive service position for this cyber stuff? Gosler said ‘yes it is.’”

**Hayden, NSA’s Organizational Transformation and Legitimizing the New Paradigm: 1999-2000**

In February 1999, Major General Michael V. Hayden was nominated by the President to become the next Director, National Security Agency during a critical juncture in NSA’s new mission area development, which required a variety of organizational transformations in technology, management and organization restructuring to meet the future needs of signals intelligence collection, including “active SIGINT.”

NSA and the IOTC’s work continued throughout the transition period to the new DIRNSA; however, from the DoD perspective: According to observers the March 1999 intelligence agency cyberwarfare demonstration/exercise at the Information Operations Technology Center (IOTC) left “no question that the keyboard covert operators wowed the Joint Staff with their computer attack capabilities.” However “they are adamant in insisting that cyber bombs are more laboratory technologies than usable weapons.” MG Bruce A. “Orville” Wright, Deputy Director for Information Operations for the Joint Chiefs of Staff, the military head of the interagency center and the top cyber-warrior in the U.S. military “told the symposium that ‘Within the area of computer network

---

610 Gosler considers himself as an oddball at both NSA and CIA: “I was not aligned with either organization…I took a mission-oriented non-parochial approach” (Admiral William O. Studeman and James (Jim) Gosler, interview by the author, Ft. Meade, MD, December 2, 2015).

exploitation, there is tremendous investment, which, with a little bit of fine tuning, can be turned into a computer network attack capability.”

What is unclear from these comments is whether the DoD cadre understood that ultimately there is very little difference between the technical capabilities necessary to accomplish a CNE- or a CNA-based mission; in fact, today CNE is seen, in many cases, as a more difficult yet necessary precursor to CNA. Perhaps an implicit bias can be inferred from General Baker’s comments at the same conference where he stated that “Effects-based warfare,” that is, methods geared to achieve an outcome and not cause traditional damage, lacks the “visually pleasing destruction from an armed bomb.”

Despite General Baker’s apparent desire for a quickly developed kinetic type CNA ability that was “visually pleasing,” and the inherent tension in the statements from some DoD Generals that appear above, at the Secretarial level it was acknowledged that “Intelligence plays a central role in...offensive information operations

615 There were also clearly issues with use doctrine as the capability set for CNA was being developed. “Baker stressed that part of the problem in any kind of computer network attack is the concerns on the part of policy-makers in Washington with regard to legality and ‘traceability.’ Jumper described his experience: ‘I picture myself around that same targeting table where you have the fighter pilot, the bomber pilot, the special operations people and the information warriors. As you go down the target list, each one takes a turn raising his or her hand saying, ‘I can take that target.’ When you get to the info warrior, the info warrior says ‘I can take the target, but first I have to go back to Washington and get a finding.’ Seeking permission invariably results in artificial restrictions and hesitations in attacking targets, Jumper stressed. From a field perspective, he said, the process of seeking the ‘special’ operation cedes too much decision-making to inside the Beltway” (William M. Arkin, “A Mouse That Roars?” Washington Post, July 7, 1999, accessed August 29, 2016, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin060799.htm). The comments by General Jumper open the door to an inference that his perception or belief was that he would need the issuance of a Presidential Finding prior to engagement in CNA activities. The requirements for Presidential Findings are codified in 50 U.S. Code § 3093 (United States Code, “50 U.S. Code § 3093 - Presidential Approval and Reporting of Covert Actions” Legal Information Institute, accessed August 29, 2016, https://www.law.cornell.edu/uscode/text/50/3093).
[and]…necessary technical data on adversary information systems.” The IOTC was viewed as an entity that “enhance[d] cooperation between DoD and the Intelligence Community in developing capabilities to take advantage of advances in computers, telecommunications, networks, and other information technologies.” Furthermore, DoD and the IC created a new entity known as the “Bilateral Information Operations Steering Group with the Intelligence Community to work through the interagency issues related to information operations.” Capability development within the IOTC was progressing; however it was not without impediments from ongoing internal resistance at NSA. According to General Hayden he discovered after this arrival at NSA as DIRNSA that Bill Marshall’s “most difficult partner wasn’t any of the military services. It was the leadership of the National Security Agency below the eighth floor (where the director’s office was housed). A lot of folks just wanted to do the traditional SIGINT mission; this exotic IO stuff was a costly distraction from an already tough job and there was fear that IOTC tools in the hands of others would compromise NSA’s fragile endpoint operations.”

NSA clearly continued to push forward on its intelligence collection and “information operations” capability development to achieve its mission objectives,

---

616 William S. Cohen, Annual Report to the President and the Congress: 1999 (Washington, DC: US Government Printing Office, 1999), accessed August 30, 2016, http://fas.org/man/docs/adr_00/chap12.htm. The Bilateral Information Operations Steering Group (BIOSIG) was created and charged to serve the DCI and DepSecDef as the senior bilateral IO policy coordination and advisory group between the IC and DoD. The BIOSIG provided bilateral policy recommendations to the DCI and DepSecDef and supported them in ensuring coordination between the IC and DoD on IO-related issues. Specific membership, functions and responsibilities were set forth in the originating document (Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, email correspondence with the author, Washington, DC, December 2015).

although this would ultimately require some reworking. In 1999, a panel of the NSA Advisory Board convened, chaired by recently retired Lt. General James A. Clapper. The Board produced a study entitled “Digital Network Intelligence—the New SIGINT Paradigm.”\(^6\)\(^1\) The report references an “End-to-End Digital Network Intelligence Process.”\(^6\)\(^2\) According to Jeffrey Richelson, digital network intelligence (DNI) is “the intelligence from intercepted digital data communications transmitted between, or resident on, networked computers.” Richelson states that the heavily redacted study discussed the need to “re-tool: organizationally, programmatically, and technologically” and examines issues concerning the access and collection of digital network intelligence, processing and extraction of intelligence from the data collected, analysis and reporting, and dissemination.\(^6\)\(^3\) The report outlined a functional taxonomy that included specific elements of the technical approach to what is now known as CNE including definitions for Access and Collection, which was defined as the activity of identifying and acquiring target communications.\(^6\)\(^4\) Additionally, the report defined Processing and Extracting (P&E) as the process of converting machine language into human language—

manipulating huge volumes of heterogeneous complex data. P&E had four major functions, although additional information from this report describing these functions is not publicly available. A fair reading of this information would indicate a call to formalize operating procedures and refine technical approaches to information operations at NSA.

Within two months of the issuance of this study, DIRNSA Hayden commissioned a 60-day internal panel to produce actionable recommendations from the outputs of the NSASAB Panel report on Digital Networks, which were reported out to the House Permanent Select Committee on Intelligence (HPSCI), and address key issues in leadership processes, resource questions, partnerships, the need for flexibility and better mentoring identified through an internal analysis during the same time period. These actionable recommendations would lead to major changes in NSA operations in 2001. As Hayden learned more about the organization he now headed, he began to formulate an implementation strategy for significant changes that were necessary to be effective in the digital domain, and he planned accordingly.

---


625 General Michael V. Hayden, interview by the author, Washington, DC, December 2015.
was being surpassed technologically by the commercial industry. During this time period
“John Millis, who headed up the House staff overseeing the Agency, commented that
‘technology has been the friend of the NSA, but in the last four or five years technology
has moved from being the friend to being the enemy.’”626

The NSA reorganization, according to Inglis, was driven by a variety of factors
outlined in the NSA Director’s Study, including the DIRNSA’s ongoing attempts to
“cajole the Directorate of Technology and the Directorate of Operations, who were not
appropriately collaborating, to integrate their activities in a substantive way. Despite the
DIRNSA’s efforts at encouraging this mission-essential imperative, the two main NSA
elements could not accomplish the required integration through intra-organizational
cooperation, and were exposing organizational gaps with operational effects. In fact there
was at least one meeting with the DIRNSA where no one either believed they had
mission area responsibilities or actually did.”627

In the latter part of 1999, DIRNSA Hayden requested that Black have lunch with
him at a Korean restaurant. As they ate together, the General asked Black to consider
returning to government service as the Deputy Director, NSA.628 In July 2000, Hayden
selected Bill Black, General Minihan’s former Special Assistant for Information Warfare,

---

627 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
628 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
and one of the driving forces behind the creation of the IOTC to be his Deputy Director and set out to implement a major transformational effort.

Planning the NSA Transformation

On December 13, 2000, Chris Inglis was brought into Bill Black’s office with at least one other SES, who was his manager at the time. Inglis was a member of the “Inside Team,” which was tasked to provide an analysis of what needed to change at NSA from the perspective of employees who currently worked in the organization. Black informed the men that the Directorate of Operations and the Directorate of Technology were going to be disestablished and pointedly asked Inglis, “Are you in or are you Bill is described by General Hayden, with admiration, as a bomb thrower and bureaucratic knife fighter, and Hayden’s most disruptive decision as DIRNSA (Michael V. Hayden, Playing to the Edge: American Intelligence in the Age of Terror (New York: Penguin Press, 2016) Chapter 8).

Inside Washington Publishers, “After 40 Years at NSA, Bill Black Is SIGINT World’s Agent for Change,” Inside The Pentagon 18, no. 27 (July 4, 2002). The article also stated that Black’s predecessor, Barbara (BAM) McNamara was widely perceived to be a roadblock to Hayden’s transformation program, believing that Hayden’s proposed reforms were over the top. Hayden was privately frustrated by McNamara’s resistance and knew that Black’s approach would be the opposite. Throughout his career at NSA, Black became the agency’s Mr. Fixit, moving from place to place developing operational or organizational solutions to problems: “If they needed something new for which they had no blueprint and they wanted it built, they called me.” According to Black, Hayden “knew his background, my history in regard to ‘I don’t like things as they are if they need to be changed’” (Inside Washington Publishers, “After 40 Years at NSA, Bill Black Is SIGINT World’s Agent for Change,” Inside The Pentagon 18, no. 27 (July 4, 2002)). From a business standpoint, NSA processes and methods were antiquated. “Bill Black was a feared guy at NSA. When Hayden became DIRNSA and Black was proposed as Deputy, some of the seniors tried to bureaucratically block him from getting the job. Once Black became Deputy Director and found out who tried to block his appointment, they were all dead bodies in the hallway” (Admiral William O. Studeman and James (Jim) Gosler, interview by the author, Ft. Meade, MD, December 2, 2015).

As noted earlier an outsiders’ group was convened as well, during a sixty-day study period meant to provide feedback to the new DIRNSA: “The 19 managers who made up the New Enterprise Team studied their agency for 60 days and urged Hayden to install a new executive leadership team, create strategic business plans, develop an agency-wide management information system and hire a financial management officer. Hayden said the NSA staffers who wrote the report were midlevel personnel, whom he described as ‘responsible anarchists.’ …The report, which one former NSA insider described as a ‘harsh but honest assessment,’ was part of Hayden’s strategy to overhaul the agency, starting with a sweeping ‘100 Days of Change’ initiative begun Nov. 15 [1999]” (Bob Brewin, Dan Verton, and William Matthews, “NSA Playing IT Catch-Up,” FCW, December 5, 1999, accessed August 29, 2016, https://fcw.com/articles/1999/12/05/nsa-playing-it-catchup.aspx).

Black and Hayden disestablished the organizations and created the Signals Intelligence Directorate by regrouping the relevant sub-organizational elements into a new operations-based organization. This
out?”633 Black showed the men NSA’s new organizational chart: The new organization, called SID, an acronym for Signals Intelligence Directorate, had three components, aligned into specific organizational mission areas with the responsibilities to “Get It (S3), Use It (S1) and Know It (S2).”634 “The ‘Get It’ guys were consolidated (K sections and G sections etc.) under a recast mission vision, with descriptive functional objectives and specific line objectives under the theory that if you are collecting, we are going to put you all together.”635 Inglis was highly surprised to see his name under a new operational element, while his manager’s name was nowhere to be seen.636 He was named to lead the newly consolidated S2 analysis group (the Know It guys), and started his own internal realignment because most resources were statically assigned with a bias towards geographical and nation-state issues. He believed the proper configuration was to take a flexible approach where resources were deployed on an as-needed basis from the center of the new organization (though often for years at a time). “I had to break the stovepipes in a world that was no longer static in its threats, shape or form.”637

underscored the need to accomplish integration by organizational design, not by integration processes that were shown to be ineffective (James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015).

633 According to Jim Gosler, Bill Black had poster on the wall of his office of a man pointing a gun: No matter where you sat in the office, the gun seemed to be pointing at you; Inglis indicated that Black could be a “very scary guy when he wanted to” and concurred with the author’s assessment that the Deputy Director may very well have engaged in a form of institutional psyops as a managerial tool during this time period (Admiral William O. Studeman and James (Jim) Gosler, interview by the author, Ft. Meade, MD, December 2, 2015; James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015).

634 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.

635 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.

636 Over the course of the next two weeks after the reorganization was unveiled at NSA, 60 NSA senior executive service members were effectively relieved of their positions. These seniors could stay as SES, but it would be under new organizational leadership where they were no longer in charge of the elements they previously led. Many said no thanks, and retired from the government. (Some were brought back after 9/11 for their domain expertise as after the 9/11 attacks under a specialized government program.) (James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015).

637 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
As an example Inglis recounted a circumstance where three linguists were needed to be transferred from one section to another. At the time there were 12 offices in the overall S2 Directorate. One of the Office Chiefs, whose personnel were to be transferred, blocked the transfer on the grounds that “they belonged to me,” although his Office had more than 1,000 persons working in it at the time.\(^{638}\) Inglis was forced to intercede, and told the Office Chief that NSA’s human capital belonged to the nation, not a particular manager. Thereafter Inglis instituted a policy known as “Deployment Services” with the managerial philosophy that “all bodies belong to the nation” to put a stop to this type of internally possessive culture, a hold-over from the warlord mentality. Inglis then devised an allocation schema necessary to reconcile the mid-level managerial inclination to stovepipe both talent and information and keep it for themselves.\(^{639}\)

**Living on the Net, Industrial Strength Exploitation and Tailored Access**

As part of NSA’s cultural and organizational transformation, DIRNSA Hayden released a document in December 2000 that formalized the analysis performed during the 1999-2000 time period into policy and laid out a new vision for the future of NSA.\(^{640}\) Hayden recollected that “We didn’t want stability, we wanted disruption.”\(^{641}\) This seminal document described the “shift in the operational environment resulting from the digital information revolution and the rise of a global, fiber optic-based, Internet

---

\(^{638}\) James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.

\(^{639}\) James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.

\(^{640}\) Hayden identified NSA’s missions as Signals Intelligence (SIGINT), Information Assurance (IA), Operations Security (OPSEC) and the Information Operations Technology Center (IOTC) and specifically identified NSA as both an Agency of the Department of Defense and a component of the National Foreign Intelligence Program (NFIP). NSA’s budget authority is derived from both sources (National Security Agency, “Transition 2001” (December 2000), accessed August 29, 2016, http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa25.pdf).

connected world” that required “a new strategy for NSA to perform…its offensive…missions. NSA must ‘live on the network.’” The new operating vision mandated that NSA “must shift significant emphasis and resources from current products, services, and targets to the modern and anticipated information technology environment for…SIGINT and be capable of operating with our partners seamlessly in the global network; and when necessary, succeeding through…the establishment of…tailored access to specialized communications when needed.” Furthermore, the strategy stated that as “resources permit, [NSA will] deploy technology to meet operational requirements in non-networked environments.” Hayden further stated that NSA is “prepared organizationally, intellectually and—with sufficient investment—technologically, to exploit in an unprecedented way the explosion in global communications, [which] represents an Agency very different from the one we inherited from the Cold War.” Based on this information, it is clear that the need for advanced technical collection

---

642 National Security Agency, “Transition 2001” (December 2000), accessed August 29, 2016, http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa25.pdf. NSA’s SIGINT collection was based around the previous dominant paradigm of analog point-to-point communications transmitted in the air, microwave or satellite via “dedicated voice channels that were rarely encrypted,” at a volume that was growing, but manageable collected, “processed and exploited.” The document noted that today “communications are mostly digital, carry billions of bits of data, and contain voice, data and multimedia transmitted by…fiber optic and high-speed wire-line networks and most importantly, an emerging wireless environment that includes cellular phones, Personal Digital Assistants and computers” (National Security Agency, “Transition 2001” (December 2000), accessed August 29, 2016, http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa25.pdf).


capabilities at both the “midpoint and endpoint” were driven by technology changes, systems development, systems integration and use doctrine. General Hayden expanded upon the change in the operational environment and the concomitant implementation strategy for “active SIGINT”: “Traditional signals intelligence used to be passive and ‘midpoint.’ If someone being targeted decided to send a message, [Intelligence] spy agencies tried to get between points A and B and intercept the communication. With the digital age…spies have gone to ‘active’ signals intelligence. They don’t just intercept at the midpoint, but go to the endpoint…. Go to a point where sometimes they have not even yet decided to transmit.”

Hayden discussed, as an example, the change in digital communications such as email: “Emails had been generally limited, dedicated, point-to-point communications that came to a program loaded on your machine…we were now on the cusp of Web-based email systems that promised…far greater volumes. Toying with the old point-to-point emails had us shooting way behind the target.”

In service of what the Transformation called the need for “tailored access,” Hayden says, “we set up an enterprise called TAO, the Tailored Access Office, in the

---

newly formed SIGINT Directorate (SID).” (“TAO was officially stood up in late 2000, but was not fully operational until 2002.”) Hayden continued, “We [NSA] had toyed with some boutique end-point efforts before, but this was different. This was going to be industrial strength. We actually divided up SID into end-point and mid-point boxes, the better to measure and meter the growth of the former even if it had to be at the expense of the latter.” General Hayden stated that “In a period of generalized growth (due at least in part to the 9-11 attacks), TAO became the fastest growing part of NSA…and…benefitted from the bursting of the dotcom bubble and the massive surge of patriotism after the 9-11 terrorist attacks. Talk about the best and the brightest: We got an incredible cohort of young, technically talented, innovative and adventurous new SIGINTers. We hired several thousand people in the four years after 9-11. Our new cohort…had a ‘no target impossible to penetrate mentality’ and, from the beginning, bypassed low-hanging fruit to attack the hardest targets. Some of these took years to penetrate.”

650 Department of Defense Historian, name withheld upon request, interview by the author, Maryland, May 22, 2015.
651 Michael V. Hayden, Playing to the Edge: American Intelligence in the Age of Terror (New York: Penguin Press, 2016) Chapter 8. As Hayden worked on furthering the CNE/CNA initiatives started under Minihan and ensuring they were fully operationalized through the NSA Transformation Strategy, he “tried to disinvest about $200 million a year from ongoing collection to invest in what we needed to work the end point and I heard about it from all over Washington. No one was willing to surrender any current take for future capability” (Michael V. Hayden, Playing to the Edge: American Intelligence in the Age of Terror (New York: Penguin Press, 2016) Chapter 8). According to Foreign Affairs magazine, TAO’s mission is to “collect intelligence information on foreign targets via computer network exploitation (CNE) techniques….and [it] is also responsible for developing the information that would allow the United States to destroy or damage foreign computer and telecommunications systems with a cyberattack if so directed by the president” (Matthew M. Aid, “Inside the NSA’s Ultra-Secret China Hacking Group,” Foreign Policy, June 10, 2013, accessed August 29, 2016, http://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/).
652 Michael V. Hayden, Playing to the Edge: American Intelligence in the Age of Terror (New York: Penguin Press, 2016) Chapter 8. According to Matthew Aid, “TAO…is now the largest and arguably the most important component of the NSA’s huge Signal Intelligence (SIGINT) Directorate, consisting
Maturing the IOTC

During this time period, Hayden also set out to mature the IOTC organization with Bill Marshall and Bill Black. “The end result was that Marshall’s expanding team doggedly developed, gathered, evaluated, modified, catalogued and stored tools that might prove useful to...spy on an adversary or to deny, degrade, disrupt or destroy an adversary’s network or information.”653

Marshall considered one of his most positive relationships in the formative years of the IOTC from an Intelligence Community perspective to be with Jim Gosler, who by this time was well into his tenure as head of CIA’s Clandestine Information Technology Office (CITO). Marshall characterized the strength of the relationship with CITO relative to IOTC activities as much better than what he encountered with the emerging NSA TAO organization at this point in time. Furthermore, the Intelligence Community interorganizational dynamics that revolved around IOTC membership and activities were clearly complex in their characteristics. “TAO possessed authorities for exploitation-related activities but did not possess authorities for offensive activities—this fell into the CIA area of CNO. Neither CIA nor TAO needed IOTC as an entity; the DoD crowd654 was much more interested in the IOTC tools being created.”655

---

654 Presumably both the services and OSD.
When asked to reflect about his time at IOTC, Bill Marshall soft-pedaled the enormity of the organization’s far-reaching accomplishments in his typical, humble fashion. “IOTC was…a link in a long chain of organizations that were developing new capabilities in this arena. The military Services, NSA, CIA, and our Allies had spent quite a bit of time, effort, and resources spanning decades in the development of new capabilities and maturing of operational concepts to deal with our foreign adversaries. IOTC…helped to keep moving…[the] ball down the field, by bringing disparate organizations together in a joint environment for the purpose of working to integrate intelligence, technology, operational concepts, and potential solutions to legal and policy issues.”

According to Hayden, “Marshall forced a whole series of legal and doctrinal and organizational questions. You can’t stockpile tools and weapons without compelling DoD lawyers and national policymakers to give you some guidance. And that engendered debate…controversy…forward-leaning thinking…[and kept] the doctrinal fire (and controversy) of cyber operations alive.”

As NSA was reforming itself to meet its mission responsibilities for SIGINT (both active and passive), and creating offensive computer network attack capabilities through its management of the IOTC and reorganizing to establish tailored access capabilities and meet the goal of “living on the net,” certain technical changes and systems development needed to occur as well. Chris Inglis explained that as part of the 2000-2001 organizational transformation, NSA set out to perform the “integration of the

---

SIGINT system to itself” (a system of systems integration)—a necessary change if NSA was to “accomplish the intended mission,” namely “endpoint and midpoint collection efforts that would be mutually reinforcing and interactive.” Seeking further integration of NSA’s capabilities, Inglis stated that “SIGINT system sensors were built to collect, process and disseminate information, which required a change from the typical architectures of a cryptologic sensor, and other associated changes to collection sensor design and implementation criteria.”

In addition to the flurry of activity at NSA during this time period, two important changes were about to occur at other USG organizations. DoD transferred the operational responsibility for the CNA (Computer Network Attack) mission to U.S. Space Command at Peterson Air Force Base, Colorado on October 1, 2000, and the Information Operations Center (IOC) at CIA was about to be created.

**The Sunset of CITO and Stand-Up of the Information Operations Center at CIA: 2000**

NSA was not the only organization experiencing some internal issues: CIA was as well. Jim Gosler indicated that in the 1999-2000 time frame Director Tenet was frustrated with the DO/DS&T tensions in regards to CITO activities, which was causing operational dysfunctionality. Gosler, as head of CITO, actually reported to both entities, in effect because they did not trust each other. Gosler was asked directly by Director Tenet if the

---

658 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
future of Information Operations was ever going to work in DS&T. Gosler responded “only if the DO lets it.” Based on these interagency dynamics, Gosler indicated “That’s why Fred Turco was brought in to run the newly established IOC.” To Gosler, “the management lesson is that leadership needs to get in the fray and take care of parochial people who are causing the suboptimization of the mission—the question is why they are parochial in the first place?—I could never figure it out.” Gosler gave another example of parochialism related to joint duty assignments (JDAs): “going native disease.” “Despite the purpose of JDAs, if these employees align themselves with their new organizational mission, then they become persona non grata when they return to their organization, where they will not be promoted.”

In January 2000, Joanne Isham was named as the new Deputy Director for Science and Technology and within the year announced a number of organizational moves that eliminated the Clandestine Information Technology Office (CITO). A portion of CITO’s activities were transferred to the Office of Technical Collection, while others were transferred to a newly created Information Operations Center in the Directorate of Operations. During the latter days of CITO, Gosler and Gaffney talked policy, feeling that the organization was artificially being bound (held back) by the institutional

---

660 Senior Intelligence Executive in CIA’s Directorate of Operations, later known as National Clandestine Service.
perspectives from the members drawn from DS&T and the DO, and needed to go further into the growing cyber mission space.\(^{664}\)

Soon thereafter, the “Information Operations Center (IOC), [was] chartered to conduct full spectrum cyber operations, sharpen cyber tradecraft, protect Agency systems and enhance CIA’s cyber analysis and grew steadily under three successive CIA Directors.”\(^{665}\) The “IOC didn’t try to replicate or try to compete with NSA (or later, the JFCC-NW)—its mission was to develop cyber power so that the Agency can perform its traditional missions, although each has to be aware of the other’s actions and those actions have to be de-conflicted. That actually works pretty well. There is plenty of work to go around.”\(^{666}\)

**Resolving NSA v. CIA Collection Controversy: 2001-2002**

As highlighted earlier in the chapter through the recollections of Bill Black, Michael Hayden and Hank Crumpton, a bureaucratic battle over lanes in the road and specific authorities over who was entitled to access what, where and how,\(^{667}\) was still unresolved. Claiming dominion over “Data at Rest is a ‘core birthright issue’ for CIA clandestine operations” according to Marshall, and CIA fought tooth and nail to maintain their claim stake to this area of computer network operations as NSA capabilities continued to grow.\(^{668}\) The position taken by personnel at all levels of the NSA organization was summarized in the following way: “if we can access data at rest

\(^{664}\) Glenn Gaffney, interview by the author, McLean, VA, November 23, 2015.
\(^{667}\) The Data-at-Rest (DAR), Data-in-Use (DIU) and Data-in-Transit (DIT) problem previously cited.
remotely, then it is crazy for us not to do it.”669 Ultimately, President Bush signed off on compromise in a memorandum after 9/11 declaring it fair game for both agencies, allowing NSA to collect data at rest, treating it in accordance with SIGINT rules, which was transformational for CNO, while CIA handles data at rest like HUMINT.670 (The civilian leadership intervention by the White House in 2002 to resolve the controversy was characterized as “I don’t care [who owns it]—just get it and share it.”)671 Fortunately, “this bureaucratic issue didn’t end up in a death match across the Potomac between the two agencies.”672 Hayden and NSA now, “at least in terms of law and policy pretty much had all we needed to thrive” for “CNE, the end point, active SIGINT, Tailored Access Office-centered activity.”673 “With little debate, we went from a world of letting radio waves serendipitously hit our antennas to what became a digital form of breaking and entering. We were penetrating foreign networks and were saying it was the same thing as scooping up signals from the ether and that the same rules applied. To us it was and they did, but in retrospect it was a remarkable transition…from our system of governance from the old world to the new.”674

671 Department of Defense Historian, name withheld upon request, interview by the author, Maryland, May 22, 2015.
The Information Operations Roadmap: The IC and STRATCOM: 2003-2004

A Summer Study was conducted by the Defense Science Board (DSB) in 2002 related to computer network operations. DIRNSA Hayden and his deputy Bill Black advised the DSB to look at what NSA was funding for CNE methods to gather a better understanding of the status for these capabilities, while also advising the group to recommend the “build out of infrastructure to enable CNE/CNA.” DIRNSA Hayden also advised the DSB “that DoD should build off of IC capabilities, including its knowledge of the threat space as well as the IC’s access into adversary systems.” The insights provided by General Hayden were incorporated into the outcomes of the Summer Study, and led to the publication of the Information Operations Roadmap by the Department of Defense in 2003. “The central idea provided was clear and unambiguous: Intelligence collection informs CND and enables CNA.” Hayden used the term/acronym GEDA (Gain, Exploit, Defend, Attack) during this time frame to describe these types of activities; a different terminology set was at one point used to describe CNE/CNA—one approach was deny, degrade, destruct, destroy, manipulate.

As early as February 2003, the US formalized authorities for militarily significant CNE and CNA capabilities. This is verified by the issuance of National Security Presidential Directives (NSPD)-16, which “provided guidance to determine how and
when the United States would launch a Computer Network Attack (CNA) against foreign systems, and who would be authorized to conduct such operations and is intended to clarify circumstances under which a disabling computer attack would be justified, and who has authority to launch such an attack.\textsuperscript{680} The issuance of this type of national security directive implied a robust capability that was continuing to develop over time.\textsuperscript{681}

During this time frame, perhaps not coincidentally, CRS detailed two types of computer network attack: “A computer network attack (CNA), usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organization or computer user. Other forms of CNA are enabled when an attacker uses stolen information to enter restricted computer systems. An electronic attack (EA) involves the use of the power of electromagnetic energy as a weapon, more commonly as an electromagnetic pulse (EMP) to overload computer circuitry, but also in a less violent form, to insert a stream of malicious digital code directly into an enemy microwave radio


\textsuperscript{681} Clay Wilson, Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues (Washington, DC: Library of Congress, Congressional Research Service, 2007), accessed August 30, 2016, https://www.fas.org/sgp/crs/natsec/RL31787.pdf. Richard A. Clarke, at this time the President’s Special Advisor for Cyberspace Security, was quoted in the Washington Post, “We have capabilities, we have organizations; we do not yet have and elaborated strategy, doctrine, procedures” (Bradley Graham, “Bush Orders Guidelines for Cyber-Warfare,” Washington Post, February 7, 2003, https://www.washingtonpost.com/archive/politics/2003/02/07/bush-orders-guidelines-for-cyber-warfare/dd8b4a18-140c-4690-88a5-0041d4ce1b1c/). Another ELIGIBLE RECEIVER exercise was conducted (ER 03) as a dual use exercise, and asked the question, “How should CNA/CNE capabilities be treated? We examined the implications of approaching the capabilities from both Title 50 and/or Title 10 authority perspectives. We looked at issues of deniability, versus non-deniable versus fuzzy…. The value of ER 03 was that it firmly established the need for DoD to properly train, organize and equip for cyber—this led to the creation of the Network Attack Support Staff (NASS), Joint Functional Combatant Command - Netwarfare (JFCC-NW) and CYBERCOM” (Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015).
transmission; cyberattacks usually require that the targeted computer have some pre-existing system flaw, such as a software error, a lack of antivirus protection, or a faulty system configuration, for the malicious code to exploit. However, as technology evolves, this distinguishing requirement of CNA may begin to fade. For example, some forms of EA can now cause effects nearly identical to some forms of CNA. For example, at controlled power levels, the transmissions between targeted microwave radio towers can be hijacked and specially designed viruses, or altered code, can be inserted directly into the adversary’s digital network.”

By October 2003, DoD published the Information Operations Roadmap, which is a remarkable document in a variety of ways, and can reasonably be inferred as the operationalization of NSPD-16. Now declassified and only partially redacted, the Roadmap authors believed that “when implemented, the recommendations of this report will effectively jump start a rapid improvement of CNA capability.” The Roadmap refined the December 1996 concepts of Information Operations, although it still utilized the core concepts of Electronic Warfare, Psychological Operations, Operational


\[683\] Department of Defense, “*Information Operations Roadmap*” (Washington, DC, October 30, 2003), accessed August 30, 2016, [https://www.nsarchive.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf](https://www.nsarchive.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf). According to The Roadmap Charter, the document was created at the direction of Secretary Rumsfeld to the DoD Undersecretary of Defense for Policy (USD(P)), the Assistant Secretary of Defense for Command Control and Communications as well as the Chairman of the Joint Chiefs of Staff.

Security, military deception, and incorporated the newer conceptualization of Information Warfare/Information Operations, now reframed and specified as Computer Network Operations. CNO (which includes CNE and CNA) was now “considered to be operational in a direct and immediate sense” and DoD must “clearly define the capabilities the Services and SOCOM are expected to organize, train and equip to provide to COCOM.” The report recognized that the “Services, Combatant Commanders (COCOMS) and Agencies do not have a common understanding of IO,” something that was clearly an issue since MOP-30 was issued in 1993 and acknowledged the “identification of a major deficiency in advancing IO as a core military competency was the ‘balkanization’ of IO responsibilities across OSD, Services and COCOMS.” The report delineated the balkanization of IO responsibilities across OSD: At the time ASD(C3I) promulgated overarching IO policy, but responsibilities for policy, strategy, plans, operations and programs for IO capabilities were diffused across OSD in multiple offices with USD(P), ASD(C3I) and USD AT&L; the recent creation of USD(I) to oversee the military intelligence programs (MIP) introduced another organization with responsibilities related to IO—highlighting the need for a more streamlined OSD IO construct.

A variety of organizational and operational capability changes were outlined in the report. One major outcome of the report was to recommend that STRATCOM should be designated as combatant command of CNA forces to “mature CNA into a reliable Warfighting Capability” and “guide development of desired capabilities, specific weapons development and employment, interagency coordination and declaratory policy,” in addition to addressing command and control issues within the service components.  

The report cited a Deputy Director for Information Operations (DDIO) study that recognized SPACECOM, although previously given the mission for CNA in 2000, “did not have the forces to accomplish the tasks required.” The recommendation to give STRATCOM the COCOM lead in this area was also due, at least in part, to the fact that SPACECOM itself highlighted the lack of indigenous CNA forces as a major impediment in advancing CNA into a robust warfighting capability when STRATCOM and SPACECOM combined in October 2002. The Undersecretary of Defense for Policy (USD(P)) was recommended to “actively improve and enforce interagency processes to deconflict CNE and CNA and enhance CNE activities as an essential

688 In July 2002 the Operations deputies requested the JCS conduct a “Proof of Principle” exercise to test command and control of CNA. The November 2002 ER 03 exercise was used for this purpose in a non-notice scenario; the exercise highlighted the need to revise and improve the command and control construct (Department of Defense, Information Operations Roadmap (Washington, DC, October 30, 2003), accessed August 30, 2016, https://www.nsarchive.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf).


precursor for DoD operations.” Furthermore, the report identified the need for extensive Information Operations preparation of the battlespace through intelligence, surveillance and reconnaissance and extensive planning activities during peacetime that are necessary to conduct full-spectrum information operations.

During conflict or wartime operations, the report indicated that “when executed to maximum effect, seizing control of adversary communications and networks will allow COCOMs to control the enemy’s networks and communications dependent weapons infrastructure, command and control and battlespace management functions.” The report recommended providing a CNA authority delegation to the COCOM to “use all CNA weapons except those that entail high risk of knowledge transfer to enemies,” and to identify “desired characteristics and capabilities for CNA.” As part of the command and control for these capabilities, the Roadmap recommended that STRATCOM be empowered to undertake critical precursor activities for successful IO planning and execution under a single four-star combatant commander, streamline CNA (and Psyop) organizational constructs as well as command and control. Furthermore, it was recommended that an IO career force be established “which will have to break some cultural norms,” and called for two career tracks: IO planner and IO capability specialists.

---

(CNO, EW or Psyop), with rotations in a core area plus as a planner. This career force would benefit from the identification of Joint and Service IO billets and include opportunities for enlisted and civilians to maintain proficiency with guarantee of advancement and continued opportunity. Additionally, the need for focused analytic and intelligence support that could “effectively characterize targets and improve weapon engineering was recommended” due to the fact that “COCOMS lack organic capability to rapidly analyze complex systems and generate IO target sets…including rapid, fully integrated nodal and network analysis providing COCOMs with holistic kinetic and non-kinetic solutions for a full range of electromagnetic, physical and human IO targets with…well tested and reliable CNA weapons that are aligned with appropriate target sets and integrated with other IO capabilities and weapons systems.” The report also called for “greater investment in all types of intelligence to develop and maintain network access in support of COCOM CNA requirements.”

Targeting and possible use cases were also discussed. “At the strategic level, targets include [redacted] and sensitive targets (national, nuclear command and control etc.) that may have a high operational and/or intelligence value. For most of these targets, effective exploitation of these targets will require…a high standard of stealth,
characterized not only by non-attribution.\textsuperscript{698} Therefore, the Roadmap laid out the possibility that the Commander STRATCOM could “delegate operational control to his subordinate commands” to allow for “unity of effort for [those] who have been responsible for exploiting a particular target in peacetime…to attack targets with high confidence of success when directed by Commander STRATCOM.”\textsuperscript{699} This effectively set the stage for a future delegation for CNA to the DIRNSA under certain circumstances.

The report also specifically recommended that “DIRNSA, as Executive Agent should engage IOTC to apply its technical expertise to make recommendations to STRATCOM on the categorization of [redacted]…and…should direct IOTC to use certain criteria to categorize CNA weapons. Additionally, DIRNSA should engage IOTC to employ its technical expertise in developing and applying assurance standards for validation and promulgation in conjunction with DOT&E (Directorate of Operational Testing and Evaluation) to determine whether CNA tools have gone through the assurance testing and been categorized as potential weapons.”\textsuperscript{700}

The report provided three categories of computer network attack weapons groupings:

Category I: capabilities allocated to a COCOM

Category II: capabilities pre-allocated to support a specific aspect of an operations plan (OPLAN) or contingency plan (CONPLAN)

Category III: capabilities not allocated to COCOMs therefore requiring Secretary or Presidential approval to employ.  

In 2002/2003, Hayden notes, “NSA still had no authority to engage in computer network attack (the authorities were limited to developing and creating the capability)—it was limited to defending American information and stealing other people’s….although defense, exploitation and attack were technologically and operationally indistinguishable even though they were separated in legal authority, funding streams and Congressional oversight.” 

During Ken Minihan’s tenure as DIRNSA, a closer relationship with STRATCOM was forming. Black, in addition to being the Special Assistant for IW, was also the NSA representative to the Strategic Air Command/STRATCOM and worked in close collaboration with the organization. Furthermore, General Minihan and Major General Robert Linhard started working together “cooking up IW,” but a new element of bureaucratic push back emerged: ”the Electronic Warfare cadre was ‘frowning’ on this IW thing.” At the time STRATCOM was looking for a new mission space and were

704 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015. According to Black, the same terms were being used for EW and IW that made them seem the same, although they were not.
looking hard at SIGINT and/or computer network attack (CNA) and expressed interest.\textsuperscript{705} NSA, Strategic Air Command and STRATCOM had a close relationship, and Black saw STRATCOM as an ally for covert action, although NSA had no experience in this area. “NSA never felt a part of DoD, although we had personnel from all three services embedded within our organization—however, it was easier for us to associate with the head of STRATCOM than with CIA, as we had a less natural relationship with them.” According to Black, “most of us saw these types of capabilities as effective covert action\textsuperscript{706} under the rubric of CNA; however, there were at least two limiting factors that prevented NSA and STRATCOM from moving forward in this area: CIA had covert action down cold and STRATCOM had a ‘Mother-May-I’ system that was so restrictive, the permissions needed were akin to what is necessary for a presidential finding.”\textsuperscript{707} However, in the intervening years, STRATCOM acquired the authorities for DoD’s CNA role. The new STRATCOM commander, General Jim Cartwright,\textsuperscript{708} now headed an organization that traditionally dealt with nuclear weapons and space, but also had responsibility for offensive cyber operations, “the CNA function that Ft. Meade could perform but didn’t have the legal authority to do.”\textsuperscript{709}

\textsuperscript{705} As Black relates it, when General Minihan told General Eugene Habiger that he was reassigning Bill to become his special assistant for Information Warfare, Habiger stated that “that is exactly what I want STRATCOM to do, and the STRATCOM CINC offered his assistance” (William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015).

\textsuperscript{706} “Indeed a number of communities of interest, with varying objectives, will need to perform Information Operations at various levels of secrecy. The methods used in the intelligence world—working sustainable clandestine and covert operations, across the entire spectrum, of economic, political, and military targets to exploit systems and produce intelligence in support of a variety of customers—match, very well, the needs of tomorrow’s Information Operations community” (National Security Agency, redacted author, “IO, IO, It’s Off to Work We Go...,” Cryptolog 23, no. 1 (March 1997)).

\textsuperscript{707} William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.

\textsuperscript{708} Cartwright assumed command of STRATCOM on September 1, 2004.

\textsuperscript{709} Michael V. Hayden, Playing to the Edge: American Intelligence in the Age of Terror (New York:
According to Admiral McConnell, starting with the new administration in 2000, “SECDEF started to move functions previously managed by the Joint Staff out to the Combatant Commanders for execution, effectively reducing the impact and influence of the Joint Staff. As part of this process SECDEF elected to move six lines of activity to STRATCOM in Omaha, Nebraska, far outside Washington, DC, including the information operations (IW) portfolio, thus denying a measure of regular in-person access to the Washington, DC leadership for a variety of mission areas.”\textsuperscript{710} McConnell notes, “As a result of the changes, GEN Hoss Cartwright recognized that (as the new STRATCOM Commander) he needed help in Washington, DC.\textsuperscript{711} He devised a strategy to create the Joint Functional Combatant Commands (JFCC) due to his recognition that without this type of mechanism, he could not maintain positive control of his disparate elements from his headquarters in Omaha. GEN Cartwright established the Director of NSA as the JFCC for Information Operations (the new name that evolved for IW).”\textsuperscript{712}

Meanwhile, back at NSA, the IOTC was entering its seventh year of existence, and had undergone some changes over time. According to Bill Marshall, “At first, IOTC was wholly NSA funded (but the intent over time was to zero out NSA funding and use funding from others). Although the capabilities, expertise and technology core was at NSA, by the end of 2002 most of the funding was coming from other external IC and DoD sources. Most all billets were reimbursable. The IOTC was not an expensive organization (it consisted of approximately 350-400 personnel), but was constantly in

\textsuperscript{710} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
\textsuperscript{711} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
\textsuperscript{712} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
need of funding sources. Maintaining the toolbox became a very complicated endeavor as well: This was the first time independent verification and validation (IV&V) was applied to document CNO tools, get legal approval, maintain and update and then make them available for operational use in IC and DoD.” Marshall also observed that the “IOTC was ‘unnatural’ since it was joint, co-led by DoD and IC and designed to keep folks with differing objectives on the same page.” The DIRNSAs, “[Minihan and Hayden], Bill Black and I performed program reviews on various CNA/CNE projects to remove redundancies—then we ‘purpled it up,’ which led to creation of CYBERCOM.”

**Transition of IOTC to JFCC-NW and Dual-Hatting the DIRNSA: A Blend of Title 50 and Title 10 Authorities for CNO: 2004-2005**

After discussions, at least in part due to the unwieldiness of STRATCOM’s diverse missions and the need for positive control detailed above, Hayden and Cartwright agreed that Cartwright would devolve his authority and responsibility for cyberattacks to NSA and dual-hat Hayden as the Commander, Joint Functional Component Command-Net Warfare (JFCC-NW), with authority to order CNA activities. Hayden stated, “We were essentially going to expand the IOTC, rebrand it, and give it operational authority through Cartwright’s position as a Combatant Commander. The combined team at Ft. Meade would access and conduct reconnaissance of a target based on my authorities as DIRNSA and then, on order, could manipulate or destroy the target based on Cartwright exercising his combat authority through me…essentially offering NSA’s resources to

---

715 Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015. Typically the use of the word purple in this context refers to joint duty or joint operations.
enhance DoD cyber combat power at little cost to the Services. Unlike their opposition to the IOTC in 1997-98, this time around they were open to the idea.\textsuperscript{716}

The plan, which was considered an interim step “to a full-up cyber command” did not need Congressional approval, and was supported Chairman of the Joint Chiefs of Staff Richard Meyers, Secretary of Defense Rumsfeld and President George W. Bush.\textsuperscript{717} Mindful that dual-hatting DIRNSA was “blending the traditional relationship between Title 50 (espionage) and Title 10 (war making) authorities” and could cause consternation within the oversight committees for intelligence in each legislative chamber, briefings and discussions commenced.\textsuperscript{718} Gaining at least tacit Congressional approval, the Joint Functional Component Command-Net Warfare (i.e., the nation’s Computer Network Attack force) stood up in January, 2005.\textsuperscript{719} Effectively, NSA (or at least the Director of NSA) now had both CNE and CNA authorities.

Now that the Joint Functional Component Command-Net Warfare was created, and acquired the capabilities developed over the course of seven years from the Information Operations Technology Center, Hayden acknowledged the “need (for) tailored handcrafted tools for (a) specific target. Some of the weapons in the IOTC’s toolbox were harvested…from the web…and would make attribution an even more difficult

challenge…but some…could be pretty ugly, [and] had to be modified to meet our operational and legal requirements [which included] standards of the laws of armed conflict, weapons that reflected the enduring principles of necessity, distinction and proportionality and produce an effect that was predictable and responding to a genuine military need [necessity].”  

Soon after, Marshall said, “Bill Black convinced General Hayden to break up IOTC, stating that it had succeeded in its mission. While the IOTC was not universally successful, it was the catalyst for everything we see today and helped create integrated joint cyber activities.” Tellingly, “after the IOTC dissolution, the analysts went to S2 (Know it), and the Advanced Technology Group (ATG) developers went to TAO.”

In 2005 NSA Director General Hayden established the NSA/CSS Threat Operations Center (NTOC) as a joint Information Assurance and SIGINT initiative to assess and report on foreign threats against U.S. information systems. “A few weeks before I left NSA, …and at the strong insistence of Bill Black, we launched the NSA Threat Operations Center (NTOC). If we were going to be throwing cyber rocks, we had better start protecting our glass house. I called on Bill Marshall again to head it. He began with ten people, no dedicated work space and no budget. Three years later the center was a thriving concern with almost a thousand folks in place.” While NTOC’s methods continue to change with technology, its mission remains “to look for new, creative, and collaborative ways to leverage our industrial strength SIGINT and IA capabilities to live

---

on the net always, shape the net sometimes, own the net when needed, and protect the net from those who wish to do the Nation harm.”723 Today, NTOC’s mission is “to establish real-time network awareness and threat characterization capabilities to forecast, alert, and attribute malicious activity and enable coordination of Computer Network Operations by NSA/CSS; U.S. Strategic Command (USSTRATCOM); and the broader community of the United States, its allies, and its mission partners.”724

CNO MMI Analysis of 1997-2004

Civilian–Military Relations Theory 1997-2004

On a broad basis, Posen’s theory of Civilian–Military relations predicts that the role of the external threat environment is a key factor in explaining the impetus for civilians to intervene in intelligence activities. The case history does not support this prediction as key factor behind the development of computer network attack capabilities, at least during the 1997-2001 time period. In fact the international operating conditions during this time period were relatively placid from a nation-state specific threat environment perspective, and substantially dissimilar from the late Cold War period during 1982 to 1989. What did exist from a threat perspective was a growing concern related to information security and critical infrastructure from adversarial computer network operations, similar to the 1992-1996 time frame, where some high-profile US


network breeches did occur. The placement of Minihan at NSA at the end of the previous time period was intended to reshape the organization for IW activities. However, this move was not precipitated by a demonstration of an adversary’s technology, either through a test or combat use that was sufficiently stark and frightening to shake civilians’ faith in their own military or intelligence organizations’ ability to handle it, nor could the ELIGIBLE RECEIVER exercise be construed to meet this criterion due to the timelines involved. The After Action Report from the ELIGIBLE RECEIVER 97-1 exercise certainly showed the existence of a potential threat from foreign adversaries, but there had yet to be a capability display to substantiate an equivalent level of proficiency from other countries such as NSA, as a proxy attacker, showed during the exercise. The MOONLIGHT MAZE intrusions in 1998 were clearly an adversarial capability display, but occurred well after the civilian interventions outlined in the case history, and therefore cannot be considered causative. Similarly, the development of CNE and CNA during this time frame was not the result of a push to innovate due to a previous military or intelligence failure. The possibility of future limitations on NSA collection capabilities due to dynamic changes in information and communications technology is a plausible type of organizational threat, and is a contributing factor for CNE capability development at NSA and CIA, but a threat that can be considered congruent with the thrust of Posen’s assertions. Ultimately, the threat environment cannot be seen as a substantial factor driving the creation of CNA as a MMI.

Posen’s theory also predicts that doctrine precedes technological innovation, however this is not supported by the case history. While DoD issued directive S3600.1 in
December 1996, the language simply clarified the definition of CNA, which had existed on paper since 1992 under the DoD TS-3600.1 Information Warfare Directive. CNE capabilities, which are the technological foundations of CNA, were in ongoing development and some limited use since at least the mid- to late 1980s and had still not appeared in a published doctrine. The revised definition of CNA, “operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves,” once again seemed to just codify the latent and patent technical approaches already underway, similar to the authority delegation that was made in the following months (until March 1997) granting NSA CNA capability development authorities. The holds true as well for the advancements in doctrine exhibited in the Information Operations Roadmap published in 2003 which identified the need for extensive Information Operations preparation of the battlespace through intelligence, surveillance and reconnaissance and extensive planning activities during peacetime that is necessary to conduct full-spectrum information operations. The categories of activities that would constitute intelligence preparation of the battlespace

---


were clearly already in development, as delineated in the IOTC ConOps document, to say nothing about the activities of TAO which maintained a “no target too difficult to penetrate” mentality, as part of the living on the net strategy at NSA. Furthermore, the Roadmap laid out the possibility that the Commander STRATCOM could “delegate operational control to his subordinate commands” to allow for “unity of effort for [those] who have been responsible for exploiting a particular target in peacetime…to attack targets with high confidence of success when directed by Commander STRATCOM.” This modest doctrinal change was a de facto recognition that the technology, capabilities—and in some instances, accesses—were already in place.

The case history does support an aspect of Posen’s predictions regarding pressure from civilian intervention as the key to the creation of a MMI. The move by DoD leaders William Perry and John P. White to reassign Ken Minihan from DIA to NSA, which was based on Perry’s knowledge of the capabilities Minihan envisioned and built during his time at AIA, clearly meets this criteria. This move was in direct response to Perry and White’s perception that NSA did not understand the need for a new method of warfare (i.e. 21st century Information Warfare exploitation tools), a situation they stridently believed needed to be rectified. There was clear continuity of support from incoming

Secretary of Defense William Cohen as well. Cohen (and the Chairman of the Joint Chiefs of Staff General John Shalikashvili) provided specific direction to DIRNSA Minihan as to what he wanted accomplished in the realm of computer network attack capability development, and was directly involved in the execution of CNA development during his tenure.\textsuperscript{734} Furthermore, another internal IC civilian leader, Director, Central Intelligence (DCI) John Deutch, gave Minihan instructions to quickly stand-up an organizational capability at NSA.\textsuperscript{735} This focus also provides evidence indicating a heightened degree of attention was paid by senior civilian officials to a particular area of operational concern within the overall threat environment.

Posen’s writings explicitly identify an alignment of external statesmen (civilian) with a maverick military officer as an operative mechanism in creation of a MMI. Under a broad reading of this theoretical tenet, the ongoing efforts of Perry, Cohen and Minihan to develop CNA capabilities at NSA via the IOTC would be consistent with Civilian–Military Relations Theory during the first portion of this time period. It is important to note that although civilian leaders were directly involved in formalizing and authorizing CNA capability development, an argument can made that the civilian intervention was internal to the IC, and not a result of Congressional or other types of external civilian-imposed personnel changes or operational mandates.

These moves provide proof that civilians exerted control over appointment of senior officials who would carry out policies deemed necessary for CNE/CNA

\textsuperscript{734} General Kenneth Minihan, interview by the author, Washington, DC, January 14, 2015; William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
\textsuperscript{735} William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
innovation, which was an expansion of operations, leading to resistance within the NSA bureaucracy. The internal pushback to the stand-up of the IOTC at NSA commenced almost immediately, at the GS-15 (O6) level and below due to parochial interests. During the early days of its existence, DIRNSA Minihan was IOTC’s only champion inside Ft. Meade, and the internal pushback was only overcome throughout the interagency due to senior leadership top cover from the Chairman of the Joint Chiefs of Staff, the Director of Central Intelligence (DCI) and Secretary of Defense William Perry.  

On the other hand, a reasonable reading of the history could not directly ascribe the IOTC’s establishment or mission origins to civilian intervention alone. The concept for the IOC was already generated within CIA while the need for a cross fertilizing entity CNE/IW development was internally recognized during 1995 at NSA, at least within G Group. Both precursor activities actually predate Minihan’s appointment as DIRNSA and the creation of the IOTC. Additionally, Minihan’s previous activities at AIA served as the center of gravity for IW development in the IC, and his thoughtful leadership and planning around this topic were transplanted to NSA upon his arrival. At best, Minihan’s placement at NSA can be seen as a galvanizing force for what was already a self-initiated IC activity that intersected with a renewed focus at the Director and senior civilian leadership level, ideas that were further shaped and refined with an injection of Minihan’s previous experience at AIA. What can be said about civilian

---

intervention at this time was that it provided the forcing function to integrate the capabilities to change the status quo.

All formative preconditions for CNE/CNA were already in place and developing in spite of the negative Congressional interventions in the previous time period. It is important to recall that Congress approved the continual cutting of NSA’s budget, essentially by a third during Admiral Studeman’s and Admiral McConnell’s tenure at NSA, and actively compelled the cessation of IW capability development.\(^{739}\) DIRNSA Minihan literally disestablished the largest internal NSA organization, A Group, to properly fund the start-up of large-scale CNE/CNA activities due to a lack of significant Congressional funding for CNE/CNA. There is no other evidence in the first half of the case study to demonstrate that civilians changed or modified budget requests submitted by the IC during this time period to foster the creation of a MMI. Although funding clearly was provided for the IOTC, by most accounts the allocation mechanisms for the organization over its lifespan were small scale, diffuse and needlessly complex.\(^{740}\)


Civilian–Military relations theory does not look to resource scarcity as an explanatory factor for innovation: It effectively is neutral, however, it recognizes that resource allocations go up with the level of the threat environment. The IOTC likely received additional funding between 2001 and 20004, as a function of the unprecedented growth of TAO as described by General Hayden. A portion of this money was likely allocated to tool development and analysis meant to support, among other things, anti-terrorism-related intelligence collection.741

The creation of the IOTC provides clear evidence indicating that intelligence agencies did adopt research and development or policies favored by civilians as a result of Minihan’s insertion at NSA, contrary to what Posen predicts. Secretary Cohen supported the new organization built on a foundation of NSA technical capabilities, which he believed would enhance IO cooperation throughout the Intelligence Community, and lead DoD to centralize command responsibilities for executing IO campaigns and responses to strategic IO attacks.742 See Table 13 for a summary.

<table>
<thead>
<tr>
<th>Civilian–Military Relations Theory 1997-2004</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>The push to innovate was a result of a previous military or intelligence failure.</td>
<td>No</td>
<td>In fact the opposite is true. There was no previous military or intelligence failure driving this innovation.</td>
</tr>
<tr>
<td>A civilian intervention occurred as a result of a demonstration of an adversary’s technology, either through a test or combat use that was sufficiently stark and frightening to shake civilians’ faith in their own military or intelligence organizations’ ability to handle it.</td>
<td>Yes</td>
<td>Civilian intervention occurred during the beginning of this time period as a result of the findings from the ELIGIBLE RECEIVER 97-1 exercise; however, this was an internal test of our offensive capabilities, not a foreign actor’s demonstration. There is no evidence of this dynamic at CIA.</td>
</tr>
<tr>
<td>Evidence indicating a heightened degree of attention was paid by senior civilian officials to a particular area of operational concern within the overall threat environment.</td>
<td>Yes</td>
<td>A heightened degree of attention was evident once the area of operational concern was brought to civilian attention by the IC; however, these threat briefings were bottom-up and informational, not top-down mandates.</td>
</tr>
<tr>
<td>Pressure was brought to bear by an external civilian organization(s) on the IC or DoD.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>Civilians exerted control over appointment of senior officials that would carry out policies deemed necessary for innovation in this area of operations to address the perceived external threat.</td>
<td>Yes</td>
<td>Although civilians could have exerted control, the officials were already in place and not inserted.</td>
</tr>
<tr>
<td>Civilians changed or modified budget requests submitted by IC or DoD agency to reallocate resources in order to foster innovation to be applied against the threat they wanted addressed.</td>
<td>Yes</td>
<td>Although budget changes were made, these changes were in support of IC internally generated activity.</td>
</tr>
<tr>
<td>Internal pushback or resistance occurred after a civilian-led external intervention called for an expansion of intelligence areas of operations.</td>
<td>No</td>
<td>Internal pushback was present at NSA due to the stand-up of the IOTC, although it was not a result of external intervention.</td>
</tr>
<tr>
<td>Evidence indicating that intelligence agencies adopted research and development or applied science policies favored by civilians as a result of their intervention.</td>
<td>No</td>
<td>The exact opposite of this dynamic occurred. The internally generated R&amp;D and applied science policies were already underway and were approved of by civilians.</td>
</tr>
<tr>
<td>Doctrine preceded technology.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
</tbody>
</table>
**Interservice Rivalry Theory 1997-2004**

The main tenet of interservice rivalry theory states that conflict is due to (financial) resources needed to execute a primary mission(s) are limited or perceived as being limited. Resources for IC CNE/CNA activities continued to be a zero sum competition during this time period. In early 1997, the IOTC was established as a joint activity of the Department of Defense and the Intelligence Community. This drove elements of interservice rivalry between NSA and DoD, principally over the stand-up of the IOTC, and the negotiations over the content of a formal concept of operations (CONOP) document, which was a source of significant bureaucratic infighting. This behavior was driven by antipathy from DoD service components who did not want the IOTC to be created in the first place, as it was taking money (and authorities) away from the services.\(^\text{743}\)

A more significant issue (although possibly indirectly to financial considerations) at the heart of the interservice rivalry between NSA and DoD and NSA and CIA were concerns for current and future mission relevance, coupled with various attempts to maintain current mission areas and capture new areas of operations within the CNO space. Minihan’s overall strategy for housing the IOTC at Ft. Meade was directly related to future mission relevance and control of the technological basis for CNE and CNA. The stated purpose of the IOTC was to serve as a “single center to integrate diverse service and Intelligence Community offensive IO technology development efforts and establish and maintain a national repository for these techniques, expanding a warfighting

commander’s options beyond traditional kinetic solutions.”

Minihan believed that NSA needed a technology engine room, and the creation, care and feeding of IOTC would “impregnate” NSA with computer network attack technology capabilities, and position NSA to be a major stakeholder in any future Cyber Command-style militarization of cyberattack capabilities. NSA was acutely aware that several Big DoD services did not want NSA to stand-up the IOTC, in what amounted to “reflexive service objections to the enterprise.” These reflexive objections were initially focused on the use of the terms “Operations” and “Center,” which would indicate that NSA was in charge of mission area as well as implications of an operationally focused entity that would tread on DoD and CIA perceptions of their authorities. Each of these concerns is representative of classic interagency rivalry issues of conservation of mission space and perceptions of organization prestige, and highlights the importance of linguistic nuancing in bureaucratic conflicts. NSA modified the nomenclature for the new entity as a concession to DoD’s bureaucratic sensitivities, but this did not dampen the organization’s motivation and intent to maintain its current responsibilities and capture a new share of an expanded IC and DoD CNE/CNA mission area.

---

745 Bill Black was interested in having what was then initially referred to as the Information Operations Center be a NSA-centric covert action arm. Leadership was not convinced of this approach (William P. Marshall, email correspondence with the author, Washington, DC, October 2015). Another reason he took this approach was because NSA’s budget was declining and the organization needed a “new vision” (General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015).
Minihan consciously leveraged NSA’s core competencies, expertise and industrial base with the explicit intention of filling the entirety of the mission space, at the expense of other agencies’ equities including CIA and CITO.\textsuperscript{748} As part of his overall strategy to occupy the mission space, and thus pre-empt other entities from gaining any measure of ascendancy, Minihan leveraged CIA’s lack of a comparable technological prowess.\textsuperscript{749} He knew that CIA, although capable, could not scale the technologies they did possess based on their core competencies, and sought to co-opt them by offering technical assistance limited to support for their niche technical operations.\textsuperscript{750} Clearly NSA was the largest element of the IOTC, with the most leverage across the board due to the location of the Center and the level of funding contributed to its start-up, and it sought to maintain this preeminence throughout its lifetime. Conflicts with DoD also arose due to the mission outlined for the IOTC, which did not fit the traditional DoD apportionment system conducted for the normal R&D processes.\textsuperscript{751}

DoD’s activities also serve to illuminate the elements of interagency rivalry that existed during this time period. Various objections to a truly collaborative interagency effort arose once DoD was committed to being a part of the IOTC, including efforts to maintain special access program stovepipes, concerns over sharing platform-specific

\textsuperscript{748} General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015.
\textsuperscript{749} General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015.
\textsuperscript{750} According to Minihan, CIA had their own “G Group” at the time (General Kenneth Minihan, interview by the author, Washington, DC, May 11, 2015; also see National Security Agency, redacted author, “Thoughts on a Knowledge Base to Support Information Operations in the Next Millennium,” Cryptolog 23, no. 1 (March 1997)).
\textsuperscript{751} Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
tools and previously committed programmatic funding allocated to other endeavors.\textsuperscript{752} At DoD “everyone became enamored with cyber,” although the efforts lacked funding. Title 10 DoD organizations also wished to advance their relatively minor capabilities, and stood to gain significantly from the technology transfer from NSA’s IW and CNE programs.\textsuperscript{753} This rivalry was also evident during the ELIGIBLE RECEIVER 97-1 exercises, where continual bureaucratic maneuvering occurred. DoD continued to engage in bureaucratic maneuvering throughout 1997, and attempted to grab enhanced authorities for CNE.\textsuperscript{754} For example, DoD asserted that stealing information from adversaries was a Title 10 (Information Warfare) authority, and attempted to change the nomenclature from computer network exploitation (CNE) to computer network reconnaissance, under the assertion that “recon” was a recognized military activity, similar to what Army rangers do behind enemy lines.\textsuperscript{755} The attempt by DoD to grab additional authorities for CNE under Title 10 was stopped, as CNE was ruled to be a Title 50 activity.\textsuperscript{756} Moreover, the CNE versus recon issue did not just include NSA (Title 50) and DoD (Title 10) competitiveness, but also separately involved NSA and CIA Title 50 perceived authorities over who owned what end-point targets as well.\textsuperscript{757} This is indicative of DoD’s attempt to co-opt the IC’s mission and authorities, and the ongoing battle over targets, operational methods and authorities between NSA and CIA.

\textsuperscript{752} Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
The case history does not contain any direct evidence that a formal evaluation mechanism was used by senior civilian leadership during an interservice completion that led to the perceived effectiveness of one IC or service organization’s approach to innovation over another’s. However it is possible to argue that NSA’s ability to totally dominate DoD’s computer network defenses at the Pentagon and elsewhere using only open source CNE and CNA tools during the ELIGIBLE RECEIVER 97-1 exercise was a sufficient display of capability to cement NSA’s position as lead for CNE and CNA development for the US government, and the IC in particular. This leveraging of NSA’s traditional operating experience also likely made it less susceptible to external interference and ensured ongoing support from civilian leadership champions Hamre, Cohen and Tenet, among others. NSA’s strength in SIGINT and information assurance vulnerability analysis, its longstanding core organizational missions, were tailor made for addressing the outcomes from ER 97-1: Namely that “the US was not as good as we thought we were for offensive and defense activities.”

General Minihan cemented NSA’s role in CNE and CNA development in the aftermath of ER 97-1 when he committed NSA to addressing the shortfall in offensive capability within the USG.

While it appears that during this time period the IC and service elements were in some general agreement regarding the threats they were trying to address, different mission need requirements between the IC and DoD existed. There is some evidence that the service components possessed differing threat perceptions related to IW/IO, although insight into this issue is limited to the Army’s refusal to be involved with the ELIGIBLE...

---

RECEIVER 97-1 exercise. This was probably influenced by the Army’s apparent lack of interest in the new technological capabilities available to the US in the cyber domain and the lack of a perceived threat to Army operations from adversaries that wielded similar capabilities.

This underscores the fact that Combatant Commanders (COCOMS) and Agencies did not have a common understanding of IO, which resulted in major deficiencies in the advancement of IO as a core military competency and led to the “balkanization” of IO responsibilities across OSD, Services and COCOMS. Some elements of DoD tried to incorporate CNO into their traditional activities, while other more traditional leaders continued to see “cyber as an M-16—a tactical tool that must be folded into the battle concept,” rather than a distinct, standalone AND cross-cutting capability. These differing perspectives likely influenced whether or not a capability was developed, incorporated or ignored in service of mission need requirements. The IC seemed to have a strongest grip on the possibilities and capabilities for CNE and CNA, and as a result NSA and the IOTC continued to lead the way with capability development.

Technology for CNE and CNA continued to develop during this time period, and clearly preceded doctrinal refinements. The revised definition of CNA, “operations to disrupt, deny, degrade, or destroy information resident in computers and computer


networks, or the computers and networks themselves,” once again seemed to just codify the latent and patent technical approaches already underway, similar to the authority delegation the following month granting NSA CNA capability development authorities. The IOTC created a variety of tools during this time period, with periodic demonstrations of technology, including a display in 1999 that “wowed the Joint Staff with their computer attack capabilities,” but in the absence of use doctrine, particularly with regard to legality and “traceability,” was not seen as fully mature. By 2003, the Information Operations Roadmap called for IOTC to categorize the CNA tools it developed or was developing and provide use cases for these tools, which provides strong evidence that technology preceded doctrinal development. CNO was now “considered to be operational in a direct and immediate sense,” although the use doctrine and other formalities had yet to follow. The document recognized that DoD must “clearly define the capabilities the Services and SOCOM are expected to organize, train and equip to provide to COCOM,” and sought to “mature CNA into a mature warfighting capability,” which is additional evidence that the technology itself existed by this time, and was in the process of being incorporated into the military’s Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) framework. The tools were also starting to be required to meet refined

quality assurance and independent verification and validation reviews to assess whether they met weapons categorization standards. Furthermore, deconfliction of CNE and CNA activities through interagency processes was an identified operational need, underscoring the interactive Title 50 and Title 10 operational and doctrinal refinements were still needed as capability developments and application to mission areas continued to evolve.

The case history supports the hypothesis that CNO technological innovations during this time period were largely the continuation of long-term development projects conducted within the Intelligence Community with important civilian support but without significant civilian direction. The concept and actualization of the IOC/IOTC came from within the IC. Senior civilian IC and DoD leaders embraced the concept and provided the top cover for the creation and maturation of the organization from 1997-2004 without any evidence of significant additional direction. The ER 97-1 exercise proved to be a catalyst for further internal and external “public relations” support of the organization over the time period, although an argument can be made that sufficient civilian support in terms of financial resourcing was lacking. At first the IOTC was wholly funded by NSA, most billets were reimbursable, and throughout its lifetime the organization was constantly in need of funding sources. Similarly, the scaling up of TAO as well as the creation of


766 William P. Marshall, interview by the author, Washington, DC, May 2015; the former high ranking DoD IO official described “wire brushing” Marshall when he was forced to ask DoD for financial contributions to sustain the Center. Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
CIA’s information Operations Center were based on a long history and were built on the backs of antecedent organizations which engaged in prototypical activities and operations involving computer exploitation and other methods of establishing computer network and information access.\textsuperscript{768} While civilians were supportive of these activities, or at least made no patent efforts to stop them in the manner that NSA’s early IW activities were stopped by Congress in the early ‘90s, there is no evidence to support a claim that civilians provided significant direction beyond the need for the USIC and the USG to create better CNA tools and a better overall CND posture. See Table 14 for a summary.


Table 14. Interservice Rivalry Theory 1997-2004 MMI Hypotheses Analysis

<table>
<thead>
<tr>
<th>Interservice Rivalry Theory 1997-2004</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources for the service’s primary mission(s) are limited or perceived as being limited.</td>
<td>No</td>
<td>Resource constraints were being addressed as an internal NSA issue, and did not fuel interagency rivalry.</td>
</tr>
<tr>
<td>Rivalry-based behavior between IC or DoD organizations was driven by concern for current or future mission relevance.</td>
<td>Yes</td>
<td>There is some evidence of tension between Title 10 IC organizations and the US Army. The Army was attempting to frame CNE as a reconnaissance activity, and therefore rightly to be considered Title 10 warfighting.</td>
</tr>
<tr>
<td>IC or DoD organizations sought to maintain their current mission and attempted to capture a share of the new mission area.</td>
<td>Yes</td>
<td>NSA strove to accomplish this through the IOTC; however, over the entirety of the time period this cannot be seen as an adversarial process.</td>
</tr>
<tr>
<td>IC or DoD organizations came to different conclusions or perceptions regarding the threats they were trying to address, which resulted in different mission need requirements and operational doctrine preferences that substantially influenced or defined how the organization interacted with other services.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>The Intelligence Community leveraged its traditional operating experience and allowed it to expand into a new mission domain, making it less susceptible to external interference.</td>
<td>Yes</td>
<td>CNE and CNA technical approaches were derived from traditional SIGINT; EW and IW activities and applied against new targets.</td>
</tr>
<tr>
<td>Co-option of one IC or DoD organization’s traditional mission space by another organization occurred.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>An evaluation mechanism utilized by senior civilian leadership during an interservice competition led to the selection of a winner based on the perceived effectiveness of one IC organization’s approach to innovation over another’s.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>Technology development preceded doctrine development.</td>
<td>Yes</td>
<td>Ongoing IW, CNE and CNA technology development and activities during this time period preceded doctrinal development and publication.</td>
</tr>
<tr>
<td>Technological innovations were largely the product of long-term development projects conducted within or at the direction of the military with important civilian support but without significant civilian direction.</td>
<td>Yes</td>
<td>Ongoing CNE and CNA activities during this time period were a result of IW and G44 and K 7 technical developments that occurred in the previous time period, and continued to draw on the 1980s IW experience.</td>
</tr>
</tbody>
</table>

Note. Gray cells identify common hypothesis elements that overlap across theories.
Intraservice Rivalry Theory 1997-2004

The case history shows the presence of several strong senior intelligence officers within the Intelligence Community who served as champions for creating computer network operations as a major military innovation. The case history also shows significant internal conflict as a result of a battle over maintaining the status quo activities of NSA versus implementing activities necessary to execute a new theory of victory on the battlefield. The assembled evidence does not indicate any significant role being played by the international threat environment during this time period as a driver of the innovation. There is strong evidence of a predoctrinal new theory of victory as well as evidence that technological advances preceded the creation of doctrine. There is minimal evidence of civilian intervention during this time period. This time period is directly consistent with Stephen Rosen’s Intraservice Rivalry theory as an explanation for the creation of a major military innovation.

There is direct evidence that LTG Minihan, Bill Black, Bill Marshall and GEN Hayden formulated an innovation strategy at NSA that clearly included both intellectual and organizational components. The contributions of Jim Gosler and Glenn Gaffney, who essentially created CIA’s information operations innovation strategy and built up its initial capabilities, must also be recognized for their significance as well, as part of the overall technical approach to computer network operations for the US government.

Once Minihan received authority to develop CNA capabilities and stand-up the IOTC, he was well on his way to building out an innovation strategy meant to irrevocably change the SIGINT world within NSA (serving here as the intellectual component
described in the hypothesis), although it was only partially realized during his tenure. Minihan and his special assistant, Bill Black, spearheaded the implementation of “active SIGINT” computer network operations, and set the stage for the buildout of the IOTC by Bill Marshall in the coming years. The strategy sought to ensure the successful execution of “exploitation,” “protection,” and “attack” activities\(^\text{769}\) leveraged against interconnected “physical assets (computers, network terminals, satellites, fiber optic cables, etc.)”\(^\text{770}\) thus making physical geography less important, while simultaneously expanding NSA’s global reach.\(^\text{771}\) This innovation strategy became a major catalyst for changes to NSA processes and the makeup of its workforce, which was being recast to successfully support “warfare in cyberspace.”\(^\text{772}\) The strategy, and the new theory of victory it represented, required NSA to “establish access to…computer-controlled infrastructures through the creation and use of specific types of weapons—viruses, worms, logic bombs, trojan horses, spoofing, masquerading, and ‘back’ or ‘trap’ doors to degrade, disrupt, or destroy networks and/or the functions they serve”\(^\text{773}\) in a wholesale fashion. To achieve this organizational paradigm shift, NSA partially relied upon the operation of the IOTC as an interagency NSA-controlled entity (organizational component of the hypothesis), which allowed Minihan to pursue his strategy to build out advanced CNA and CNE tools.

---

\(^\text{769}\) William B. Black, Jr., “Thinking Out Loud About Cyberspace,” *Cryptolog* 23, no. 1 (March 1997), https://www.nsa.gov/public_info/_files/cryptologs/cryptolog_135.pdf; Black also noted that NSA was cognizant that “the post-Cold War enemy changed their tactics, techniques and procedures (TTP’s) and the Intelligence Community had to adapt as well.” This lesson was not lost on the NSA leadership.


The top-down changes at NSA Minihan and Black believed were necessary to win the next war led to an internal struggle. Predictably, the stand-up of the IOTC met with significant internal NSA resistance. The move to active SIGINT and the stand-up of the IOTC activated NSA’s internal bureaucratic imperative to preserve existing missions and ways of operating. The IOTC was considered controversial because it was a newly forming mission area as well as a special organization within NSA, which made it susceptible to intra-organizational politics—where money (budgetary authority) and mission statements drive the bureaucracy’s direction. To overcome significant internal resistance and foment change, Black needed to outflank an entrenched bureaucracy that aligned against the cyberwarfare initiative. His initial solution was to stack the IOTC staff with personnel he knew would carry out the paradigm shift for NSA, whether or not he personally continued on in the organization. This move can be seen as a conscious effort by Black to empower a small group of talented individuals to operate outside of normal bureaucratic channels to foster bureaucratic change. The IOTC itself can also be considered a relatively small group of talented interagency individuals directly

---

776 At NSA, “a lot of folks just wanted to do the traditional SIGINT mission; this exotic IO stuff was a costly distraction from an already tough job and there was fear that IOTC tools in the hands of others would compromise NSA’s fragile endpoint operations” (Michael V. Hayden, Playing to the Edge: American Intelligence in the Age of Terror (New York: Penguin Press, 2016) Chapter 8).
778 One key NSA insider who did not try to kill IOTC, although he had a bureaucratic incentive to do so, was Denis Chiari, the head of NSA section G44 that was a precursor to NSA’s Tailored Access Operations (TAO). Chiari sympathized with Marshall as he experienced the same institutional intransigency years before with the TAO precursor organizations (William P. Marshall, interview by the author, Washington, DC, May 2015).
empowered to operate as a special organization within NSA to foster technological change.

These initial moves were strengthened, broadened and institutionalized by DIRNSA Hayden in the NSA 2001 transformation initiative which included the de facto firing of 60 Senior Executive Service members in a two-week period, clearing the way for a group of hand-selected individuals who would implement the new theory of victory. Hayden leveraged lessons learned from Minihan’s initial organizational change management efforts, and in concert with Bill Black, set out to accomplish integration by organizational design, not by integration processes, which NSA’s history of bureaucratic intransigence had shown to be ineffective. The changes included a realignment of organizational functions and integration of personnel from various silos of excellence. These moves were coupled with a refinement of the global network intelligence concept of operations derived from G group’s approach in the 1990s into an industrial-sized strategy for tailored access operations by “living on the net,” which extended Minihan’s original intellectual conceptualization for CNO. Hayden’s championing of the new SIGINT paradigm forcefully moved the organization away from reliance on analog point-to-point communications collection transmitted via air, microwave or satellite voice channels to digital exploitation methods focused on fiber optic, high-speed data and wireless communication environments. This approach was technologically supported by the continued pursuit of CNA and CNE tool development through the IOTC’s efforts, which were started under Minihan.
Furthermore, the creation of the Signals Intelligence Directorate as an operationally based organization, born from consolidated and realigned subelemental components, with mission responsibilities to “Get It (S3), Use It (S1) and Know It (S2),” had profound effects on the maturation of the CNO mission space. “The ‘Get It’ guys were consolidated (K sections and G sections etc.) under a recast mission vision, with descriptive functional and specific targeted objectives,” and soon came to be known for their expertise in Tailored Access Operations, among other skill sets and mission responsibilities. Some promising, mid-level intelligence officers involved in the New Enterprise Team review (‘responsible anarchists,” according to Hayden) were empowered. For example, Chris Inglis, who was identified as a future leader years before by LTG Minihan, was selected to lead another newly consolidated subelement, S2 (the “Know It” guys). Inglis furthered Hayden and Black’s efforts, and initiated an additional internal realignment designed to remove an organizational bias towards geographical and nation-state issues. His moves consciously sought to break down counterproductive stovepiping of information and human resources, which permitted a more flexible organizational response to collection and analysis in support of dynamic CNO activities.

NSA’s changes did not create a more decentralized organization per se. However, the transformation initiative did empower new leaders like Inglis to create and effectively execute innovations within their directorates without the need for ongoing organizational changes elsewhere in the agency, once the main organizational realignment was complete. To be successful, this innovative approach required “endpoint and midpoint

---

779 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
780 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
collection efforts that would be mutually reinforcing and interactive.”

The creation of TAO, the fastest growing part of NSA in the post-2001 time period, led to the creation of a variety of new career billets to ensure incorporation of key skills necessary to support the new theory of victory, which was predicated upon access to endpoints using sophisticated exploitation techniques matched against ever-evolving computer network hardware and software platforms.

As the case history in this chapter shows, NSA created the opportunity for STRTCOM to enter the CNA world. There were already ongoing organizational and personal affinities between the organizations, which only grew stronger over the time period. The new thinking, organizational and capability changes made by NSA influenced STRATCOM’s interest and approach to CNO within DoD, and predictably, it encountered internal bureaucratic dynamics similar to NSA’s recent experience as well. At first, the military Electronic Warfare constituencies within DoD took a negative view of STRATCOM’s interest in CNO as a newly emerging mission area. STRATCOM, despite the misgivings of the EW community, decided to expand its operational capabilities in CNO, and became a main beneficiary of IOTC tool development, including the Center’s efforts to develop capabilities to affect weapons systems and

---

781 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
782 According to Matthew Aid, these roles include military and civilian computer hackers, intelligence analysts, targeting specialists, computer hardware and software designers, and electrical engineers (Matthew M. Aid, “Inside the NSA’s Ultra-Secret China Hacking Group,” Foreign Policy, June 10, 2013, accessed August 29, 2016, http://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/).
783 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
784 William B. Black, Jr., interview by the author, Pasadena, MD, May 1, 2015.
attempts to integrate said capabilities with a service platform.\textsuperscript{785} In 2002, STRATCOM became responsible for the IOTC’s requirements development efforts and tool management responsibilities via the Network Attack Support Staff, which was domiciled at NSA.\textsuperscript{786} (See Appendix F for the full text of Hayden’s Director’s Message about the IOTC.) The natural organizational affinity and relationships between senior leaders in the two organizations set the stage for further cooperation and integration. This was driven by NSA’s ongoing successes with CNO, and SPACECOM’s lack of indigenous CNA forces needed to execute the CNO mission for which they were, up until 2003 notionally responsible.

Soon, as DoD’s desire to develop advanced CNO capabilities for STRATCOM and other service components grew stronger, the need for the services to organize, train and equip for cyberoperations was identified. New DoD career paths were necessary, and this requirement was highlighted as part of a series of comprehensive recommendations made in the 2003 Information Operations Roadmap, a document clearly influenced by ideas exchanged with NSA leadership. The Roadmap recommended that new DoD billets, such as IO planner and IO capability specialists (for CNO, EW or Psyop) be created. To ensure a progressive, formal career path, the study recommended that traditional types of rotational assignments be instituted for these new career billets to maintain or enhance skill proficiency that would guarantee advancement and continued

\textsuperscript{785} National Security Agency, “Information Operations Technology Center (IOTC) Concept of Operations (CONOP),” December 31, 1997 (Ft. Meade, MD: NSA). (Unclassified material extracted from classified document.)

career opportunities. Additionally, the need for focused analytic and intelligence support that could “effectively characterize targets and improve weaponeering was recommended.”

DoD’s new strategy, outlined in the Information Operations Roadmap, would more fully “leverage the Intelligence Community’s (read: NSA’s) capabilities, including its knowledge of the threat space and access into adversary systems” to rapidly improve its own CNA capability. The need for effective command and control of balkanized CNO entities throughout DoD led to the consolidation of efforts under a single four-star combatant commander, a change that was designed to streamline DoD CNA (and Psyop) organizational constructs as well as command and control. By the end of the 2003-2004 time period, a new distribution of power for CNO emerged within DoD, resulting in STRATCOM taking over command for DoD Title 10 CNO activities, although it is unclear from the case history to what extent this change was a result of an ideological struggle. What is clear is that this new distribution of power was a marriage of NSA’s CNE and CNA capabilities with STRATCOM’s authorities, combined under a four-star combatant commander. This collaboration occurred over time, and required

---

790 Department of Defense Historian, name withheld upon request, interview by the author, Maryland, May 22, 2015.
each to overcome internal bureaucratic resistance to the CNO mission change. Fortunately, this phenomenon did not extend to the organizations themselves partnering. NSA and STRATCOM had a close, ongoing organizational relationship, and worked together on IW capability development as early as 1996.

STRATCOM itself did not have indigenous CNA personnel but NSA and IOTC, the supplier of DoD’s CNO tools and the main source of the expertise in the US government, did. A deal was struck between GEN Cartwright and DIRNSA Hayden to dual-hat the Director of NSA as the leader for STRATCOM JFCC for Net Warfare which essentially was an expansion and rebranding of the IOTC, directly providing NSA’s resources to enhance DoD cyber combat power.\footnote{Michael V. Hayden, \textit{Playing to the Edge: American Intelligence in the Age of Terror} (New York: Penguin Press, 2016) Chapter 8.} The alignment of NSA with STRATCOM effectively advanced STRATCOM’S capabilities and NSA’s authorities, and more fully realized the new theory of victory advanced by Minihan, operationalized by Bill Black, institutionalized by Hayden and leveraged by Cartwright.

Technology for CNE and CNA continued to develop during this time period, and clearly preceded incremental doctrine refinements: The basic analysis is essentially the same for interagency and intraservice rivalry throughout this time period. At most, operational refinements that informed doctrinal developments flowed from advancements in CNE and CNA capability. Doctrinal development during this time period flowed directly from the existing technology development and human capital resident at NSA. The Information Operations Roadmap described the possibility that the Commander STRATCOM could “delegate operational control to his subordinate commands” to allow
for “unity of effort for [those] who have been responsible for exploiting a particular target in peacetime…to attack targets with high confidence of success when directed by Commander STRATCOM.”

A year later, STRATCOM made the decision to dual-hat the DIRNSA as the commander of JFCC-NW, which effectively empowered him to order a computer network attack (and secund his skilled NSA employees) as needed. This move, only possible as a result of the technology already created at NSA, resulted in a de facto doctrinal change that blended “the traditional relationship between Title 50 (espionage) and Title 10 (war making) authorities.”

The case history supports the hypothesis that CNO technological innovations during this time period were largely the continuation of long-term development projects conducted within the Intelligence Community with important civilian support but without significant civilian direction. The concept and actualization of the IO/IOTC came from within the IC. Senior civilian IC and DoD leaders embraced the concept and provided the top cover for the creation and maturation of the organization from 1997-2004 without any evidence of significant direction. The ER 97-1 exercise proved to be a catalyst for further internal and external PR support of the organization over the time period, although an argument can be made that even sufficient civilian support in terms of financial resourcing was lacking. At first the IOTC was wholly funded by NSA, most billets were


reimbursable and the organization was constantly in need of funding sources.\textsuperscript{795} Similarly, the stand-up of TAO as well as the creation of CIA’s information Operations Center were based on a long history that built on the back of antecedent organizations which engaged in developmental activities and operations involving computer and computer network access. While civilians were supportive of these activities, or at least made no patent efforts to stop them in the manner NSA’s early IW activities were stopped by Congress in the early ‘90s, there is no evidence to support a claim that civilians provided significant direction beyond the need for the USIC and the USG create better CNA tools and better overall CND posture. See Table 15 for a summary.

\textsuperscript{795} William P. Marshall, interview by the author, Washington, DC, May 2015; the former high ranking DoD IO official described “wire brushing” Marshall when he was forced to ask DoD for financial contributions to sustain the Center. Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
<table>
<thead>
<tr>
<th>Intraservice Rivalry Theory 1997-2004</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respected senior military officers formulated a strategy for innovation which possessed both intellectual and organizational components.</td>
<td>Yes</td>
<td>A variety of respected senior officers, including Minihan, Black, Marshall, Gosler and Gaffney, and Hayden formulated strategies for the innovation at NSA and CIA during this time period.</td>
</tr>
<tr>
<td>An ideological struggle manifested within a particular IC or service component revolving around “a new theory of victory,” which included an explanation of what the next war will look like and how leaders must fight it if it is to be won.</td>
<td>Yes</td>
<td>Internally, an ideological struggle continued at NSA throughout the first half of this time period.</td>
</tr>
<tr>
<td>A bureaucratic imperative to preserve existing missions and ways of operating attempted to crush the impulse to make technological innovations.</td>
<td>Yes</td>
<td>This dynamic is evident during the first part of the time period at NSA from employees who favored the traditional passive SIGINT approach, despite an apparent need to adapt.</td>
</tr>
<tr>
<td>A conscious effort was made by leadership to empower a small group of talented individuals to operate outside of normal bureaucratic channels to foster bureaucratic change.</td>
<td>Yes</td>
<td>NSA’s Inside and Outside review teams, as well as IOTC’s creation, provide evidence of this dynamic.</td>
</tr>
<tr>
<td>The innovation program was promoted as an evolutionary rather than a revolutionary system.</td>
<td>Yes</td>
<td>This dynamic is apparent at NSA and CIA, although the outcomes of the innovation were revolutionary.</td>
</tr>
<tr>
<td>Initiating the innovation and bringing it to the point where it provided a strategically useful option was accomplished when money was tight.</td>
<td>No</td>
<td>The innovation was already initiated during the previous time period. Although money was tight at NSA during a portion of the first half of this time period, significant post-9/11 funding allowed the innovation to grow to a strategically useful option by the end of the time period.</td>
</tr>
<tr>
<td>A more decentralized organization was created within the agency that was designed and empowered to create and effectively execute an innovation without the need for organizational changes elsewhere in the agency.</td>
<td>Yes</td>
<td>The creation of the IOTC and the early TAO organizational entities were responsible for creating the innovation; later on in the time period these organizations were centralized after the innovation matured.</td>
</tr>
<tr>
<td>New career paths were created from within the organization by senior leadership to ensure incorporation of key skills necessary to support the new theory of victory.</td>
<td>Yes</td>
<td>During the second half of the time period, new career paths were created at NSA, IOTC, TAO and DoD JFCC-NW.</td>
</tr>
<tr>
<td>A new distribution of power within the IC or service emerged as a result of an ideological struggle manifesting itself as a new senior leadership rank, billet, or command.</td>
<td>Yes</td>
<td>The delegation by the STRATCOM commander of authority to DIRNSA as head of JFCC-NW created a new power center.</td>
</tr>
<tr>
<td>Technology development preceded doctrine development.</td>
<td>Yes</td>
<td>Ongoing IW, CNE and CNA technology development and activities during this time period preceded doctrinal development and publication.</td>
</tr>
<tr>
<td>Technological innovations were largely the product of long-term development projects conducted within or at the direction of the military with important civilian support but without significant civilian direction.</td>
<td>Yes</td>
<td>Ongoing CNE and CNA activities during this time period were a result of IW and G44 and K 7 technical developments that occurred in the previous time period, and continued to draw on the 1980s IW experience.</td>
</tr>
</tbody>
</table>

Note. Gray cells identify common hypothesis elements that overlap across theories.
CHAPTER 6. 2005-2010

Introduction

Chapter 6 reveals that as of 2006 US CNO capabilities were able to “achieve critical operational effects,” the apparent result of cumulative NSA and IOTC efforts during the 1997-2004 time period. The command and control of a combined CNE/CNA capability was operationalized via the stand-up of JFCC-NW and the delegation of CNA authority from the Commander of STRATCOM to the DIRNSA. Several months later, DoD declared cyberspace a military domain of operations, and detailed specific doctrinal approaches for CNO in the National Military Strategy for Cyberspace Operations, including the importance of computer network attack – operational preparation of the environment. In 2007, DNI McConnell moved to consolidate information operations capabilities into a unified command housed at NSA’s Ft. Meade headquarters. The original plan for consolidation failed to materialize. In 2008, a computer systems penetration galvanized the need to recombine offensive and defensive capabilities at Ft. Meade, although final form of USCYBERCOMMAND did not meet the original design intent of DNI McConnell’s vision.

The second part of this Chapter examines the case history from 2005-2010 against the hypotheses of each of the main MMI theories. Stephen Rose’s theory of intraservice rivalry provides the most congruent explanation for CNO development during this time period.


In light of the recommendations of the Information Operations Roadmap and the agreement to transition the IOTC to JFCC-NW, a refinement that codified the changes to the previous Information Operations order last issued in December 1996 was needed. On August 14, 2006, DoD 3600.01 was issued by Secretary of Defense Gordon England.797 It reaffirmed several of the principles from the previous 3600 series order including the recognition of the core IO fields: EW, CNO, PSYOPS, MILDEC and OPSEC. CNO, with the embedded subset CNA and CNE, was implicitly recognized as operational and able to “achieve critical operational effects (or prevent the adversary from doing so).”798 The revised order explicitly highlighted the importance of intelligence. Intelligence support was required to “provide data about adversary information systems or networks consistent with the National Intelligence Priorities Framework”799 and mandated that

799 The National Intelligence Priorities Framework (NIPF) is the DNI’s guidance to the IC on the national intelligence priorities approved by the President. The NIPF consists of: Intelligence topics reviewed by the National Security Council Principals Committee and approved by the President; a process for prioritizing foreign countries and non-state actors that are relevant to the approved intelligence topics; and a priorities matrix that reflects consumers’ priorities for intelligence support and that ensures that long-term intelligence issues are addressed (Office of the Director of National Intelligence, “National Intelligence: A
“tactics, techniques, procedures and technologies be shared among the DoD components to fully facilitate synchronization and integration of IO.” CNE was defined for the first time as “enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks,” while CNA was defined as “operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves.”

NSA, through the DIRNSA, was specifically required to “support IO planning and operations with signals intelligence, technology and access. Additionally, DIRNSA would support proposed IO courses of action with the intelligence gain/loss assessments and potential targeting strategies as well as host and serve as executive secretary for the process to deconflict Department CNO activities with the IC.” The order did not address in specific detail which organization would be responsible to develop and execute CNA activities. At the time STRATCOM housed five Joint Functional Component Commands (JFCCs). The network warfare component, JFCC-Network Warfare (JFCC-NW), contained two subsidiary elements: the Joint Task Force-Global Network Operations (JTF-GNO) and the Joint Information Operations Warfare Center (JIOWC).

---


802 Both JTF-GNO and JWIOC reportedly had direct responsibility for defense against cyberattack. “The JTF-GNO defends the DoD Global Information Grid, while the JIOWC assists combatant commands with
In December 2006 the National Military Strategy for Cyberspace Operations was published, and explicitly stated that “cyberspace” is ‘a domain of military operations’ and DoD will “execute the full range of military operations (ROMO) in and through cyberspace to defeat, dissuade, and deter threats against US interests…DoD will use network exploitation to gather intelligence and shape the cyberspace environment as necessary to provide integrated offensive and defensive options. DoD will leverage the authorities and capabilities of those agencies under the Director of National Intelligence, as appropriate. DoD may conduct cyberspace operations across national boundaries…DoD will partner with the Intelligence Community (IC), Department of


Cyberspace characteristics were detailed as: “created, maintained, owned and operated by public, private and government stakeholders and exists across the globe; changes as technology, architectures, processes and expertise co-evolve to produce new capabilities and operating constructs; is subject to the availability of the electromagnetic spectrum; allows high rates of operational maneuver that capitalizes on decision quality information at speeds that approach the speed of light; enables operations across the domains of air, land, maritime and space; transcends commonly defined organizational and geopolitical borders; formed by the interconnection of information and data transmission systems supporting critical infrastructure, devices that store, process and transmit data and the use of hardware and software applications; includes data, voice and video ‘at rest’ and ‘in motion’; readily accessible in varying degrees to other nations, organizations, partners, the private sector and our adversaries; and forms the foundation of the information environment” (Chairman of the Joint Chiefs of Staff, The National Military Strategy for Cyberspace Operations (Washington, DC: Department of Defense, December 2006), accessed August 30, 2016, http://www.space-library.com/0612dod_The%20National%20Military%20Strategy%20for%20Cyberspace%20Operations(U)_2+52pages.pdf).
Justice (DoJ), Department of Homeland Security (DHS), and other Federal departments and agencies to further DoD cyberspace operations.”

The document describes the emerging concept of cyberspace warfare and specifically discusses cyberspace as providing new opportunities for “Operationalizing Intelligence,” “not only as an enabler of military operations, but as an operation intrinsically comparable to traditional military actions. Intelligence Operations in and through the electromagnetic spectrum can provide DoD the asymmetric edge necessary for military operations and to overcome DoD challenges.” Furthermore, the document also describes a newer subsection of preliminary computer network attack capability, computer network attack (CNA) operational preparation of the environment (CNA-OPE). “CNA-OPE are operations conducted to gain and to confirm access to, and gather key information on the target network concerning the capabilities and configuration of targeted networks or systems and to facilitate target acquisition and target analysis in preparation for CNA and/or other offensive missions.”


After conferring with Robert Gates and accepting the role as the second DNI in 2007, McConnell wanted to consolidate the IW (IO) capabilities to maximize

---


effectiveness. Admiral Studeman recollected that once Admiral McConnell came in as DNI 2007 and surveyed the enterprise, “he did not understand why NSA and CIA were not operating on the same track for cyber—there was some coordination but it was not optimized.” McConnell related that he understood “the real power for IW (IO) is NSA, not STRATCOM, and sought to encourage the Secretary of Defense to create Cyber Command and dual-hat DIRNSA as the Commander.” He discussed this realignment in summer 2008 with General Keith Alexander (DIRNSA) and General Cartwright (now Vice Chairman of the Joint Chiefs of Staff and described by McConnell as having become “Mr. Information Warfare” for the Administration); the realignment included an organization consolidation of Defense Information Systems Agency, known as DISA (which was in the process of being relocated to the Army base portion of Ft. Meade), NSA and the newly developing Cyber Command under a four-star general officer billet and tasked the new commander to run the entire combined organization.

---

810 General Alexander assumed the role of DIRNSA on August 1, 2005.
811 In 2012, General Cartwright provided some insight regarding his thinking on cyber warfare during his time as vice chairman of the Joint Chiefs of Staff: “The tools available to a president or nation in between diplomacy and military power were not terribly effective…. We needed to be able to work at no strategic depth and very large strategic depth,” Cartwright said. “Speed-of-light weapons were well suited for those kinds of problems.” To Cartwright, cyber warfare exist(s) on three levels: tactical, strategic and operational (Sam LaGrone, “Retired General Cartwright on the History of Cyber Warfare,” October 18, 2012, excerpted from US Naval Institute Conference Report, USNI News, https://news.usni.org/2012/10/18/retired-general-cartwright-history-cyber-warfare).
Alexander, Cartwright and McConnell agreed to this approach and shook hands.\textsuperscript{814} General Chilton, the new Commander of STRATCOM, disagreed and was opposed to the creation of Cyber Command. The DISA commander was also against becoming a subordinated entity.\textsuperscript{815} Robert Gates, who looked favorably on the proposal for a combined CNE, CNA, CND organization, indicated that it was not politically feasible for him to order it now, after recently establishing AFRICOM, and thus decided to pursue a modified consolidation strategy.\textsuperscript{816}

**The Creation of US Cyber Command: 2009-2010**

The creation of US Cyber Command was at least thirteen years in the making, and was envisioned during Ken Minihan’s tenure as DIRNSA, who set a variety of preconditions for its successful creation. On June 23, 2009\textsuperscript{817} Secretary Robert Gates signed off on the Establishment of a unified U.S. Cyber Command subordinate to the U.S. Strategic Command, recommending to the president that the director of the National Security Agency be appointed as commander of the Cyber Command. According to Deputy Secretary of Defense William Lynn, “in 2008, the U.S. Department of Defense suffered a significant compromise of its classified military computer networks…by a foreign intelligence agency. Malicious code spread undetected on both classified and unclassified systems, establishing…a digital beachhead, from which data could be

\begin{itemize}
  \item \textsuperscript{814} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
  \item \textsuperscript{815} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
  \item \textsuperscript{816} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
  \item \textsuperscript{817} Admiral McConnell provided some additional comments on the creation of Cyber Command. In June 2009, SECDEF directed the stand-up of US Cyber Command, headed by a four-star, dual-hatted as the Director of NSA, not as a Unified Functional Combatant Command but as Sub-Unified Combatant Command subordinate to STRATCOM. GEN Alexander was the first to fill this position and was very effective in standing up the new command (Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015).
\end{itemize}
transferred to servers under foreign control.” Further, according to STRATCOM, this “malicious code, which would allow an adversary to download critical defense information, spread across the DoD’s classified and unclassified networks in 2008. As JTF-GNO synchronized efforts to disinfect and protect over 2.5 million computers in 3,500 DoD organizations spanning 99 countries, Defense Secretary Robert Gates endorsed the idea of a new sub-unified command under USSTRATCOM that would recombine offensive and defensive computer network operations.” The bureaucratic impetus for the creation of CYBERCOM was ascribed to the BUCKSHOT YANKEE remediation efforts during this time period. The new Cyber Command was required to achieve initial operating capability by October 2009 and full operating capability by October 2010. Gates directed the disestablishment of the Joint Task Force – Global


Network Operations (JTF-GNO) and Joint Functional Component Command – Network Warfare (JFCC-NW) prior to the new command reaching full capability.\textsuperscript{823}

Today USCYBERCOM is a sub-unified command subordinate to U.S. Strategic Command (USSTRATCOM). Service Elements include Army Forces Cyber Command (ARFORCYBER), 24th USAF, Fleet Cyber Command (FLTCYBERCOM), and Marine Forces Cyber Command (MARFORCYBER).\textsuperscript{824} These organizations effectively act as the COCOMs envisioned in the Information Operations Roadmap under the control of the Dual-Hatted DIRNSA via the STRATCOM delegation referenced earlier. Chris Inglis, who was deeply involved with the process as Deputy Director, offered the following perspective: “When NSA joined with Cyber Command, you now had a fusion of SIGINT, proactive information assurance and a Title 10 purpose. While the meld of authorities has still not been substantially reconciled to the true nature of cyberspace, NSA has worked hard to deliver a system that can be maximally responsive to whatever collaboration is deemed necessary and appropriate.”\textsuperscript{825} Staffing of the idea of a separate Unified Command, subordinate only to the Secretary of Defense, has continued and as of this writing, plans were being finalized for a Presidential decision and Congressional authorization to stand-up the new independent command.\textsuperscript{826}


\textsuperscript{825} James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.

\textsuperscript{826} Admiral John M. (Mike) McConnell, interview by the author, Washington, DC, December 7, 2015.
CNO MMI Analysis of 2005-2010

Civilian–Military Relations Theory 2005-2010

The assembled evidence does not provide any significant role being played by the international threat environment during this time period as a driver of the organizational innovation per se, beyond the foreign intelligence breech of DoD networks in 2008. More broadly, however, international pressure was mounting. By the end of the time period, up to 33 nation-states had developed or were in the process of adopting computer network operations for use in their military planning, either as standalone elements or in combination with traditional electronic warfare or information operations.\footnote{James A. Lewis and Katrina Timlin, Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization (New York: UNIDIR, 2011), accessed August 30, 2016, http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.} On a broad basis Posen’s theory of Civilian–Military relations predicts that the role of the external threat environment is a key factor in explaining the impetus for civilians to intervene in intelligence activities. There is no evidence that pressure was brought to bear by external civilian organizations to merge the capabilities necessary to create a CNO MMI: Essentially the technical and organizational work necessary to achieve a full exploitation and attack capability was already accomplished, merging two IC-developed technical approaches to espionage and cyberwarfare into an integrated capability, housed separately at both NSA and CIA, within SID and IOC respectively. All formative preconditions were already in place and developing internally within the IC. What remained was the need for a more refined capability, a fully usable sabotage or military

cyberwarfare capability to “achieve critical operational effects,” including “tailored handcrafted tools for [a] specific target…modified to meet our operational and legal requirements.” During this time period, it does not appear that civilians openly intervened to direct the development of specific CNO capabilities to address a threat. Furthermore, there is no evidence available of specific civilian intervention to spur additional CNO capability development to address concerns resulting from nation-state activities occurring in the broader international threat environment; however, this conclusion could change as more detailed unclassified information becomes available in the future.

Similarly, civilian leaders, including President Bush, Secretary of Defense Rumsfeld and Congressional intelligence oversight committees, explicitly and implicitly supported the self-directed marriage between NSA and STRATCOM, a post facto endorsement of internally generated IC and DoD activity, including the devolution of the CNA attack authority from GEN Cartwright to DIRNSA Hayden. This newly formalized alignment of Title 50 capabilities and Title 10 authorities can be seen as part of a natural evolutionary process necessary to create a prototypical US Cyber Command in 2005, a vision for a truly unified cyberwarfare capability that began during Minihan’s tenure as DIRNSA in 1996. Furthermore, evidence of civilian intervention related to the issuance of the National Military Strategy for Cyberspace Operations is also absent from the case history. The National Military Strategy essentially declared US CNO as fully operational,

---

and started to directly incorporate CNO into formalized military doctrine, while at the same time recognizing a new domain of warfare which required both CNE and CNA (as well as CND) to achieve its objectives.

During this time period the NSA/CSS Threat Operations Center (NTOC) was established as a joint Information Assurance and SIGINT initiative to assess and report on foreign threats against U.S. information systems, and by the 2007-2008 time frame, the Center had “almost a thousand folks in place.” NTOC was established at Bill Black’s insistence. The motivation for creating NTOC was summed up nicely by General Hayden: “If we were going to be throwing cyber rocks, we had better start protecting our glass house.” NTOC’s creation is clearly a response to the growing threat environment, and grounded in the understanding that US CNO would have to co-exist with and defend against foreign adversary activity as well. Contrary to Posen’s theory, the case history shows this was self-initiated, proactive managerial effort and not a result of civilian intervention.

Posen’s writings explicitly identify an alignment of external statesmen (civilian) with a maverick military officer as an operative mechanism in creation of a MMI. While the creation of Cyber Command in and of itself cannot be considered a MMI, an alignment of DNI McConnell, GEN Keith Alexander (DIRNSA) and GEN James Cartwright, Vice Chairman of the Joint Chiefs of Staff (“Mr. Information Warfare” for the Administration) facilitated the stand-up of the organization during this time period.

---

Either Alexander or Cartwright might fit the military maverick moniker under this set of facts; however, the technological developments, and delegation of CNA attack authority to DIRNSA, already existed well in advance of Cyber Command’s formal creation. Therefore, while on its face this alignment of facts is congruent with Posen’s theory, the temporal sequence is clearly not.

The role of the cyber threat environment did provide the impetus to formalize the creation of US Cyber Command toward the end of this time period, as malicious code attributed to a foreign intelligence agency,832 which would allow an adversary to download critical defense information, spread across the DoD’s classified and unclassified networks in 2008.833 The Pentagon operation to counter the attack, known as Operation BUCKSHOT YANKEE, characterized as a turning point in U.S. cyberdefense strategy, can be seen as a precipitating event to formalize a new sub-unified command in an attempt to integrate each element of CNO, although the case history indicates this initiative was only partially met its intended goal of merging NSA and DISA into a new entity called Cyber Command. Although this incident was the precipitating event for the creation of Cyber Command, serious discussions about the further consolidation and optimization of US capabilities for CNO were already underway inside the executive branch.

Prior to the intrusion, newly installed DNI McConnell was already encouraging SECDEF Gates to create Cyber Command and dual-hat DIRNSA as the Commander, due to his advanced understanding NSA’s CNO capabilities—something STRATCOM did not actually possess. The discussions between the leaders of the Intelligence Community and the Department of Defense were internal to the executive branch, and therefore it would be difficult to conclude pressure was brought to bear by an external civilian organization (causing an innovation to occur), although the significant cyber intrusion into DoD’s systems likely exerted congressional pressure on DoD and the IC to remediate the breach, assess damage and ascribe attribution as quickly as possible. Clearly, a push to formally consolidate various organizations into Cyber Command was made as a result of a failure to defend DoD’s classified networks adequately. However, the result of this consolidation cannot be construed as a new technological or organizational innovation.

A reasonable inference can be drawn that the decision to formally create Cyber Command resulted from this sufficiently stark incident to create a push to further integrate DoD’s computer network operations organizations, although the discussions were an internal executive branch activity and not congressionally instigated. The case history does show internal pushback or resistance occurred as a result of the discussions to fully integrate NSA and Defense Information Security Agency (DISA) into a new Cyber Command, principally from the commanders of STRATCOM and DISA. However, the initiative to create Cyber Command was essentially instigated to enhance

---

and integrate DoD computer network defenses, and cannot be considered a call for an expansion of intelligence areas of operations. The 2008 intrusion into DoD’s classified networks clearly resulted in a high degree of attention to this significant area of operational concern. The consolidation of these organizations was viewed as necessary to address deficiencies in computer network defenses that were operating in an enhanced threat landscape. NSA, through NTOC’s formidable capabilities and staffing levels, could likely help mitigate these types of intrusions in the future. Unfortunately, despite the fact that Secretary of Defense Gates notionally controlled the appointments of both the STRATCOM and DISA commanders, he apparently believed he possessed insufficient political capital to force the merger of NSA and DISA. There is a lack of evidence that civilians changed or modified budget requests to influence the merging of NSA and DISA or reallocated funds to force this merger, although overall DoD computer network defense spending increased, and has continued to increase since this incident. See Table 16 for a summary.
Table 16. Civilian–Military Relations Theory 2005-2010 MMI Hypotheses Analysis

<table>
<thead>
<tr>
<th>Civilian–Military Relations Theory 2005-2010</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>The push to innovate was a result of a previous military or intelligence failure.</td>
<td>No</td>
<td>In fact the opposite is true. There was no previous military or intelligence failure driving this innovation. There was an organizational realignment, but this cannot be considered a technical or organizational initiative that fostered the MMI.</td>
</tr>
<tr>
<td>A civilian intervention occurred as a result of a demonstration of an adversary’s technology, either through a test or combat use that was sufficiently stark and frightening to shake civilians’ faith in their own military or intelligence organizations’ ability to handle it.</td>
<td>Yes</td>
<td>A civilian intervention occurred as a result of the 2008 DoD intrusion, resulting in organizational alignment</td>
</tr>
<tr>
<td>Evidence indicating a heightened degree of attention was paid by senior civilian officials to a particular area of operational concern within the overall threat environment.</td>
<td>Yes</td>
<td>The vulnerability and exploitation of DoD systems was of significant concern.</td>
</tr>
<tr>
<td>Pressure was brought to bear by an external civilian organization(s) on the IC or DoD.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history related to the reorganization.</td>
</tr>
<tr>
<td>Civilians exerted control over appointment of senior officials who would carry out policies deemed necessary for innovation in this area of operations to address the perceived external threat.</td>
<td>Yes</td>
<td>Yes, although these individuals partially blocked the reorganization initiative.</td>
</tr>
<tr>
<td>Civilians changed or modified budget requests submitted by IC or DoD agency to reallocate resources in order to foster innovation to be applied against the threat they wanted addressed.</td>
<td>No</td>
<td>There is no direct evidence of this dynamic occurring, although CND spending has increased year over year due to the increased threat environment.</td>
</tr>
<tr>
<td>Internal pushback or resistance occurred after a civilian-led external intervention called for an expansion of intelligence areas of operations.</td>
<td>Yes</td>
<td>There was resistance to the organizational realignment, although enhanced CND was a goal at this time.</td>
</tr>
<tr>
<td>Evidence indicating that intelligence agencies adopted research and development or applied science policies favored by civilians as a result of their intervention.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history related to the reorganization.</td>
</tr>
<tr>
<td>Doctrine preceded technology.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
</tbody>
</table>
Interservice Rivalry Theory 2005-2010

The main tenet of interservice rivalry theory states that conflict is due to (financial) resources needed to execute a primary mission(s) are limited or perceived as being limited. There is no affirmative evidence that CNO activities at NSA or CIA were resource constrained during this time period, nor is there evidence that any significant friction between interagency CNO components existed on the basis of financial considerations resulting in limitations on the effectiveness of one IC element over the other. Overall, a segueing of IC and DoD interagency operational cooperation and merging of integrated capabilities were formalized in the National Military Strategy for Cyberspace Operations and appeared to be occurring, but not without some growing pains.

Bureaucratic concerns related to status/organizational prestige can be implied as a result of the proposed merger of NSA, JFCC-NW/JTF-GNO and DISA into a Unified Functional Combatant Command under a newly created four-star position. The proposal to consolidate organizational capabilities would have moved the CNA authority out of STRATCOM and downgraded DISA to a subordinate command within Cyber Command. Naturally, and as interagency rivalry theory predicts, both heads of DISA and STRATCOM resisted this change, which had the potential to impact their current and future mission relevance in CNO. Although core CNE, CNA and CND competencies and expertise actually resided at NSA, the proposed realignment would directly benefit General Alexander, providing him a promotion and a larger, independent unified combatant command to lead, with ascendancy for the operation domain, both in the IC
and DoD. On a broad basis, this can be seen as NSA’s attempt to maintain current mission areas and capture new areas of operations within the CNO space, without having the organization under some form of control from future STRATCOM commanders. Ultimately the bureaucratic deal to create Cyber Command partially failed as the organization remained a subordinate entity, regardless of the positive impact it was meant to create for integrated offensive and defensive national security purposes. There is no evidence that a formal mechanism was used during this time period to evaluate whether one service component’s technical approach was more effective than another; however, it was clear that DNI McConnell believed, based on his experience, observations and knowledge, the true power for IW/IO resided at NSA, where it had existed since the 1980s. The IC’s traditional operating experience, and ongoing successful execution of the CNO mission, made it less susceptible to external interference, and in fact the continued need for access and target intelligence was actively being incorporated into the cyberwarfare approaches required in National Military Strategy for Cyberspace Operations. There is some evidence that NSA, through the stand-up of the NTOC organization, together with its traditional Information Assurance activities, could be seen as impinging on or co-opting a portion of DISA’s mission space, which was focused on computer network and communications assurance (defense) activities. Clearly, in light of the BUCKSHOT YANKEE remediation efforts, and mindful of past incursions like MOONLIGHT MAZE, the fears of a growing foreign intelligence threat to DoD and IC computer systems were now realized, and could not be ignored. It now appears that the IC and DoD organizations came to the same conclusions regarding the threats they were
trying to address. For CNE activities, there is evidence that NSA and CIA continued to have different mission need requirements and operational doctrine preferences that substantially influenced or defined how the organization interacted with each other. Essentially, the approaches taken by the two organizations led DNI McConnell to conclude that “NSA and CIA were not operating on the same track for cyber—there was some coordination but it was not optimized,” something that continued to confound him, despite the creation of deconfliction mechanisms and a White House ruling.

Interservice rivalry theory indicates that technology typically precedes doctrine, and this appears to hold true for this portion of the case history. The tool creation capabilities were now institutionalized as a result of the efforts of the IOTC, and propagated throughout the empowered IC and DoD elements according to the interviews conducted. An indirect acknowledgement of this can be seen in the language of DoD Directive O-3600.1, Information Operations, issued in 2006. What was needed was doctrinally driven integration across DoD. The Directive mandated that “tactics techniques, procedures and technologies be shared among the DoD components to fully facilitate synchronization and integration of IO.” The language defining CNE and CNA was also slightly refined to explicitly incorporate the need for integrated intelligence collection for computer network operations. CNE was defined for the first time as “enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks,” while CNA was defined as

---

“operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves.”

This shows an incremental doctrinal evolution, incorporating the recommendations from the Information Operations Roadmap in 2003, but does not represent anything new in terms of doctrine driving technology: The military was now simply thinking through the applied uses and implications of the technological innovations developed over time. All technological elements and technical approaches (TTPs) for CNE and CNA were already in place. What had apparently changed was DoD’s confidence in its ability to operate a newly declared fifth domain of armed combat, and now chose to formalize in its strategy and doctrine for integrated offensive and defensive purposes “to defeat, dissuade, and deter threats against US interests…and may conduct cyberspace operations across national boundaries.”

A new set of terminology, delineated in the Military Cyberspace Operations doctrine, helped organize the blended approach of CNE and CNA necessary to achieve success in cyberwarfare: the concept of computer network attack (CNA) operational preparation of the environment (CNA-OPE). “CNA-OPE operations were necessary to gain and to confirm access to, and gather key information on the target network concerning the capabilities and configuration of, targeted networks or systems and to facilitate target acquisition and target analysis in preparation for CNA and/or other

---


offensive missions.” The technological innovations for CNO continued as part of a long-term development effort generated by NSA (as well as CIA’s CITO and IOC) and were continuations of the global access and tailored access called for in the NSA 2001 Transition strategy. These efforts continued to be seen as valuable and were supported by civilian and military leadership alike during this time period according to the interviews conducted, and prospered without the need for significant civilian direction. See Table 17 for a summary.

<table>
<thead>
<tr>
<th>Interservice Rivalry Theory 2005-2010</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources for the service’s primary mission(s) are limited or perceived as being limited.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>Rivalry-based behavior between IC or DoD organizations was driven by concern for current or future mission relevance.</td>
<td>Yes</td>
<td>There is some evidence rivalry drove DISA to try to remain independent of CYBERCOM. Similarly, STRATCOM clearly wanted JFCC-NW/CYBERCOM to remain a subsistent command.</td>
</tr>
<tr>
<td>IC or DoD organizations sought to maintain their current mission and attempted to capture a share of the new mission area.</td>
<td>Yes</td>
<td>NSA exhibited this behavior during the organizational realignment but this was not an adversarial process.</td>
</tr>
<tr>
<td>IC or DoD organizations came to different conclusions or perceptions regarding the threats they were trying to address, which resulted in different mission need requirements and operational doctrine preferences that substantially influenced or defined how the organization interacted with other services.</td>
<td>No</td>
<td>There is no evidence of this dynamic in the case history.</td>
</tr>
<tr>
<td>The Intelligence Community leveraged its traditional operating experience and allowed it to expand into a new mission domain, making it less susceptible to external interference.</td>
<td>Yes</td>
<td>There is some evidence of this dynamic in the case history. The creation of CYBERCOM can be seen as a merging of IC and DoD traditional mission spaces into a cyberwarfare capability.</td>
</tr>
<tr>
<td>Co-option of one IC or DoD organization’s traditional mission space by another organization occurred.</td>
<td>No</td>
<td>There is some evidence that an unsuccessful attempt was made between NSA and DISA.</td>
</tr>
<tr>
<td>An evaluation mechanism utilized by senior civilian leadership during an interservice competition led to the selection of a winner based on the perceived effectiveness of one IC organization’s approach to innovation over another’s.</td>
<td>No</td>
<td>No, however, there is some evidence that the DNI believed NSA’s approach was best.</td>
</tr>
<tr>
<td>Technology development preceded doctrine development.</td>
<td>Yes</td>
<td>Ongoing IW, CNE and CNA technology development and activities during this time period preceded doctrinal development and publication.</td>
</tr>
<tr>
<td>Technological innovations were largely the product of long-term development projects conducted within or at the direction of the military with important civilian support but without significant civilian direction.</td>
<td>Yes</td>
<td>Ongoing CNE and CNA activities during this time period were a result of IW, G44, K 7, IOTC and TAO technical developments that occurred in the previous time period, and continued to draw on the 1980s IW experience.</td>
</tr>
</tbody>
</table>

Note. Gray cells identify common hypothesis elements that overlap across theories.
Intraservice Rivalry Theory 2005-2010

The case history shows the presence of several strong senior intelligence officers within the Intelligence Community who formulated a strategy to create an integrated CNO organization combining NSA, JFCC-NW and DISA (CND) capabilities, an approach that possessed both intellectual and organizational components. The proposed combination of these three organizations was viewed as the final organizational step necessary to combine and maximize the effectiveness of military cyberwarfare capabilities, an organizational realignment melding Title 50 and Title 10 authorities necessary to implement a new theory of victory on the battlefield—the fusion of SIGINT, proactive information assurance applied to a Title 10 purpose. Despite an agreement between DNI McConnell, General Cartwright and General Alexander to merge these organizations, and a measure of support from Secretary of Defense Bob Gates, the creation of a unified functional combatant command subordinate only to the Secretary of Defense partially failed due to successful bureaucratic maneuvering by the commanders of STRATCOM and DISA, who were determined to protect their command authority and mission space, which ultimately led to a suboptimal compromise not fully in synch with the true nature of cyberspace operations.

It is difficult to portray the interagency conflict that developed around the merging of NSA, JFCC-NW/JTF-GNO and DISA as an ideological struggle evolving around “a new theory of victory,” the future of warfare and how it must be fought if the US was to win because this issue was essentially settled at this time, after a new military domain of operations was declared in 2006 following many years of CNE and CNA
development. The failure to incorporate DISA’s computer network defense capabilities into CYBERCOM, according to the interviews conducted, was less about an ideological struggle and more closely aligned with bureaucratic politics. Similarly, creating CYBERCOM as a unified command under a four-star General not beholden to STRATCOM seems to be more in alignment with traditional power politics in the military than the future of warfare. In this case, the STRATCOM commander’s refusal to allow CYBERCOM to become a co-equal independent entity despite the clear national security benefits and desires of the DNI and the Secretary of Defense is clearly congruent with the expectations of intraservice rivalry theory. This episode displays a bureaucratic imperative to preserve existing missions and ways of operating and forestall any attempts to make organizational innovations at his bureaucratic expense.

The agreement between DNI McConnell, GEN Cartwright and GEN Alexander cannot be characterized as a small group of talented individuals empowered by leadership to operate outside of normal bureaucratic channels to foster bureaucratic change: These were a mixture of elite civilian and military leaders operating at the highest levels of the executive branch, although because their agreement did not include the STRATCOM and DISA Commander, it can be seen as going, at least initially, around normal channels. The outcomes of their efforts, which created a different version of an existing subunified command, was still beholden to STRATCOM leadership despite the elevation of the leadership billet to a four-star rank, and did not create a new distribution of power within the IC. Correspondingly, the creation of CYBERCOM, which was a combination of organizations, cannot truly be considered as a more decentralized entity designed to
effectively create an innovation without the need for changes elsewhere in its parent organization.

After its inception, Cyber Command created a variety of new career paths within the organization to ensure incorporation of key skills necessary to support cyberwarfare capabilities. These roles are aligned with traditional military billets and organizational nomenclature, although by many accounts it still must detrimentally rely on NSA technical capabilities. The positions are typical of traditional military organizations, focused on manpower, intelligence, operations, logistics, plans and policy, C4IT, Exercises and Training, capabilities and resource integration as well as developing advanced capabilities and technologies. As part of the continuing organizational development, CYBERCOM has established Cyber Mission Teams and National Cyber Mission Teams, and has integrated the armed service components for cyber that were under development since the mid-1990s. Service Elements include Army Forces Cyber Command (ARFORCYBER), 24th USAF, Fleet Cyber Command (FLTCYBERCOM), and Marine Forces Cyber Command (MARFORCYBER). These organizations effectively act as the COCOMs for the overall organization. This force structure alignment and formality of operations is beginning to create a new distribution of power for cyberwarfare activities in the US.

The analysis for whether technology development preceded doctrine for intraservice rivalry theory is essentially the same as provided for interservice rivalry. Technology clearly preceded doctrine, and in fact facilitated the creation of

---

CYBERCOM: Typically the military will create a new command once the technological basis for a new area of operations is mature, and then create tactical use doctrine, plans, and train and equip the force thereafter. CYBERCOM has followed this pattern, although it must be noted that the organization has a plans and polices component to continually refine the doctrine under which it is operating, as well as an advanced capabilities and technologies directorate focused on continual development of CNO tools for its use in cyberspace operations. The struggle, which continues today, is how to fully align and meld organizational capabilities and structure with the demands of the chaotic and dangerous cyberspace operating environment, which requires iterative organizational innovations.

CYBERCOM’s creation can be viewed as a long-term revolutionary plan realized through the incremental, evolutionary efforts of intelligence officers Studeman, Minihan, Black, Hayden, McConnell and “scores of others”\(^\text{842}\) over a ten- to twenty-year period of time. The changes instituted during McConnell’s time as DIRNSA, advancing Global Network Intelligence, combined with Minihan’s theory of access, access, access, set the stage for the creation of a variety of innovative NSA-based organizations including TAO, IOTC, SID, IAD, NTOC, JFCC-NW and eventually CYBERCOM. Most of the efforts were conducted within or at the direction of the Intelligence Community with important civilian support but without significant civilian direction. The work, in the eyes of many involved over time, is still not complete today.

The CNO MMI provides the US Government a strategically useful option. As documented in this study, over the years a variety of technically and bureaucratically challenging efforts needed to be surmounted. On a general level, it is true that the substantive, foundational work necessary to achieve full operational capacity for CNO was accomplished when NSA’s budgets were declining. However, for this time period it cannot be said that CNO was made into a strategically useful option when money was tight. During the 2005-2010 time frame, due in part to the onset of the Afghanistan and Iraq wars, overall military and intelligence spending increased substantially, which likely provided additional resources to further CNO capability developments and capacity growth. See Table 18 for a summary.
### Table 18. Intraservice Rivalry Theory 2005-2010 MMI Hypotheses Analysis

<table>
<thead>
<tr>
<th>Intraservice Rivalry Theory 2005-2010</th>
<th>Presence or Absence of Theory Tenets</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respected senior military officers formulated a strategy for innovation which possessed both intellectual and organizational components.</td>
<td>Yes</td>
<td>DNI McConnell, drawing upon the previous work of DIRNSA’s Minihan and Hayden as well as Deputy Director Bill Black, formulated a strategy for innovation that possessed both intellectual and organizational components.</td>
</tr>
<tr>
<td>An ideological struggle manifested within a particular IC or service component revolving around “a new theory of victory,” which included an explanation of what the next war will look like and how leaders must fight it if it is to be won.</td>
<td>No</td>
<td>There is no evidence that an ideological struggle occurred over a new theory of victory per se.</td>
</tr>
<tr>
<td>A bureaucratic imperative to preserve existing missions and ways of operating attempted to crush the impulse to make technological innovations.</td>
<td>Yes</td>
<td>Yes, however, the imperative was over organizational innovation, not technological innovation during this time period.</td>
</tr>
<tr>
<td>A conscious effort was made by leadership to empower a small group of talented individuals to operate outside of normal bureaucratic channels to foster bureaucratic change.</td>
<td>Yes</td>
<td>An agreement for organizational realignment was reached among DNI, Vice Chairman of Joint Chiefs and DIRNSA Alexander, operating outside of normal bureaucratic channels.</td>
</tr>
<tr>
<td>The innovation program was promoted as an evolutionary rather than a revolutionary system.</td>
<td>Yes</td>
<td>The organizational realignment was seen as an evolutionary process started two decades before, although in its totality, it is revolutionary.</td>
</tr>
<tr>
<td>Initiating the innovation and bringing it to the point where it provided a strategically useful option was accomplished when money was tight.</td>
<td>No</td>
<td>There is no evidence in the case history that money was tight at this time.</td>
</tr>
<tr>
<td>A more decentralized organization was created within the agency that was designed and empowered to created and effectively execute an innovation without the need for organizational changes elsewhere in the agency.</td>
<td>No</td>
<td>The final steps taken for organizational realignment were to centralize capabilities.</td>
</tr>
<tr>
<td>New career paths were created from within the organization by senior leadership to ensure incorporation of key skills necessary to support the new theory of victory.</td>
<td>No</td>
<td>Career paths were already established during the previous time period.</td>
</tr>
<tr>
<td>A new distribution of power within the IC or service emerged as a result of an ideological struggle manifesting itself as a new senior leadership rank, billet, or command.</td>
<td>—</td>
<td>Clarity on this dynamic is unclear from the evidence assembled for the case. At this point in time, it is likely too soon to tell.</td>
</tr>
</tbody>
</table>
Technology development preceded doctrine development.

| Yes | Ongoing IW, CNE and CNA technology development and activities during this time period preceded doctrinal development and publication. |

Technological innovations were largely the product of long-term development projects conducted within or at the direction of the military with important civilian support but without significant civilian direction.

| Yes | Ongoing CNE and CNA activities during this time period were a result of IW, G44, K 7, IOTC and TAO technical developments that occurred in the previous time period, and continued to draw on the 1980s IW experience. |

Note. Gray cells identify common hypothesis elements that overlap across theories.
CHAPTER 7. HOW MAJOR MILITARY INNOVATIONS OCCUR

Although Rosen’s theory sufficiently explains why CNO developed as a MMI, it lacks any explanation of how technological innovations occur. This creates a situation where his model, while important, provides incomplete information as to how to bring a MMI to fruition. To provide further insights as to how the CNO MMI occurred, this chapter identifies evidence from the case history that directly correlates with specific hypothesis elements of the Christensen disruptive innovation model. While features of managerially driven innovation commensurate with Christensen’s model can be found in each of the four time periods examined in this study, the substantive and fundamental organizational changes necessary to create a CNO MMI occurred during the 1996/7-2004 time and will be the focus of the analysis in this section. As a result of this analysis, it is clear that Clayton Christensen’s model for creating and managing disruptive innovation provides strong explanatory power as to how computer network operations emerged as a MMI. The creation of small spin-off organizations in the case histories to foster innovation is clearly an important approach worthy of replication.

Christensen described the need for managers to change organizational structures and strip out counterproductive legacy processes to foster disruptive innovation. These wholesale changes are necessary when a current organizational structure and an existing organizational culture perpetuate a type of institutional value system that is likely to have
a deleterious effect on accomplishing a new mission.\textsuperscript{843} Ken Minihan, and later Michael Hayden, instituted these exact types of changes at NSA during this time period through a series of organizational and systems component reconfigurations and integrations which had a cumulative, transformational effect.\textsuperscript{844} DIRNSAs Minihan and Hayden acted as visionary champions for two key foundational changes at NSA designed to transform NSA CNA and CNE technological development into a MMI. Minihan, Hayden (and Bill Black’s) efforts resulted in the creation of the IOTC and wholesale changes to the totality of NSA’s activities as a result of the NSA Transition 2001 change management plan. NSA, through the efforts of the IOTC, was able to create a new category of special weapons for cyberwarfare use by the US Government during its lifetime. The NSA Transition 2001 led to a massive increase TAO’s organizational capacity to conduct CNE and set the preconditions for the reintegration of CNA and CNE efforts into one set of capabilities and personnel at NSA as the IOTC’s charter came to an end.\textsuperscript{845}


\textsuperscript{844} Inglis noted that the organizational and cultural transformation that was started by General Minihan continued and matured with General Hayden and concluded during General Alexander’s tenure “took forever” due to institutional intransigence, including a pre-existing “warlord culture” amongst the major Group leaders in A, B, G etc. He observed that “culture eats strategy for breakfast.” Meaningful, lasting change was only completed by the end of Alexander’s time at NSA, the longest tenure of a DIRNSA in NSA history. Between Hayden and Alexander, 14 years of continuous leadership finally accomplished the changes being sought (James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015).

\textsuperscript{845} The IOTC was directed to categorize CNA tools into three categories: Category III CNA weapons: capabilities not allocated to COCOMs therefore requiring Secretary or Presidential approval to employ (Department of Defense, \textit{Information Operations Roadmap} (Washington, DC, October 30, 2003), accessed August 30, 2016, https://www.nsarchive.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf). Author’s note: Therefore, Category III CNA weapons would have release authority similar to nuclear weapons. General Hayden also observed that “From their inception, cyber weapons have been viewed as ‘special weapons,’ not unlike nuclear devices of an earlier time” (Michael V. Hayden, \textit{Playing to the Edge: American Intelligence in the Age of Terror} (New York: Penguin Press, 2016) Chapter 8; Michael V. Hayden, “IOTC Mission Accomplished,” Director’s Message: DIReqram-345, posted September 28, 2004).
DIRNSA Minihan, together with his adviser and Special Assistant for Information Warfare Bill Black, recognized the need to change the existing organizational structures and the predominant culture within NSA to create the capabilities necessary to achieve their vision for IW/CNO. To ensure NSA would create capabilities for a new method of warfare, Minihan needed to overcome an entrenched culture of bureaucratic intransigence that was accustomed to waiting out any top-down attempts at institutional change until a current DIRNSA was reassigned. The culture at NSA included a “lying in wait” style of bureaucratic retribution that at times gained primacy over mission accomplishment. This was driven by an overarching “warlord culture” amongst the institutionally powerful major Group leaders in the Operational (SIGINT) Directorate, each of whom controlled significant numbers of personnel and budgetary authorities, and predictably sought beneficial outcomes for their areas of operational concern that resulted in inherent parochialism. Minihan actively attempted to integrate information assurance, mission support and operational equities, and create processes for information sharing that would ensure important intelligence or operational information would not be missed, and increase decision-making speed. He sought to inculcate a new mission-oriented value system amongst the parochial and often adversarial warlord culture. Minihan also disestablished A Group, the largest constituent element within the Directorate of Operations, to repurpose money and personnel toward IW/IO/CNO efforts, which was accompanied by a compelling narrative meant to sway embedded interests toward the importance of adopting the new active SIGINT paradigm. These initiatives were highly

846 Often derisively referred to as “this Director.”
847 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
significant steps toward the maturation of the CNO MMI. Other changes Minihan implemented during his tenure can be viewed as modest modifications of existing NSA internal organizational alignments and processes, and did not always meet their intended goals. However, the totality of the changes, both major and relatively minor in nature, created a significant cumulative impact well beyond his service as DIRNSA.

Despite DIRNSA Minihan’s efforts to more fully integrate the efforts of the Directorate of Technology and the Directorate of Operations through process improvement and a new mission-oriented value system during his three-year tenure, LTG Hayden inherited two main NSA elements which were still locked into current processes and value systems. This organizational misalignment left these directorates unable to accomplish essential mission-oriented intraorganizational cooperation, resulting in organizational gaps with operational effects.\textsuperscript{848} Shortly after assessing the strengths and weaknesses of his new organization, Hayden initiated a series of internal reviews that culminated in significant organizational changes which were necessary to mature the Active SIGINT and Global Network Intelligence/Digital Network Intelligence paradigm shifts championed by DIRSA Minihan (some of which, like Global Network Intelligence, were quietly fostered earlier by DIRSA McConnell). The reviews also identified additional deficiencies that ran the gamut from governance, culture, mission strategy, resource management, communication with IC and DoD partners as well as business planning.\textsuperscript{849}

\textsuperscript{848} James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.  
Hayden’s NSA Transition was specifically meant to recast the agency “organizationally, intellectually and…technologically, to exploit in an unprecedented way the explosion in global communications.”850 In order to complete the transition to a new paradigm at NSA, DIRNSA Hayden recognized that process modifications were necessary but not sufficient to achieve the overall organizational changes required to fulfill a new theory of victory. Hayden explicitly knew that purposeful organizational change was needed to realize a MMI based on CNO activities: “We didn’t want stability, we wanted disruption.”851 Hayden and Black disestablished the Directorate of Operations and the Directorate of Technology and created the Signals Intelligence Directorate (SID) by regrouping the relevant suborganizational elements into a new, separate operations-based organization852 with the responsibilities to “Get It (S3), Use It (S1) and Know It (S2).”853 “The ‘Get It’ guys were consolidated (K sections and G sections etc.) under a recast mission vision854 to live on the network,855 as part of a strategy to establish “tailored access to specialized communications when needed”856 and “deploy technology to meet operational requirements in non-networked environments,”857 which required the

852 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
853 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
854 James C. (Chris) Inglis, interview by the author, Annapolis, MD, November 30, 2015.
adoption of a “no target impossible to penetrate mentality.”

858 The creation of S3 can be seen as a heavy-weight team (organization) created from disparate intra- or extra-organizational departments, with a new organizational boundary drawn around it. The newly created S3 developed new processes and value systems necessary to achieve the CNO MMI objectives laid out in NSA Transitions 2001. The disruptive innovation that began during the early 1980s was finally achieved as a result of these wholesale organizational changes. DIRNSA Hayden’s vision for a transformed NSA required constant championing to ensure the changes were successfully engrained within the NSA culture. These efforts led to the continual expansion and refinement of CNO MMI developmental activities.

§

The creation, spin-off and reabsorption of the IOTC were key factors in the creation of CNO as a MMI, and the IOTC stands as a paradigm of disruptive innovation management. The IOTC was a quasi-independent NSA-based organization designed to carry out key pioneering work in developing CNA requirements, tool distribution to the interagency, and was responsible for the nation’s broadest and most sophisticated program of CNA technology development.859 The establishment of the IOTC can be viewed as a separate, special purpose, somewhat autonomous interagency organization, designed to provide the technological drivers necessary to expand and refine both CNE and CNA capabilities. The start-up of the IOTC was accomplished as a result of

---

Minihan’s efforts at championing its formation, and initial financial sustainment despite significant interagency and intra-agency resistance. The launch of the IOTC could not have been accomplished without the efforts of Bill Black and Bill Marshall, and a small group of other NSA managers, with high-level cooperation from the Director, Central Intelligence and the Secretary of Defense.

The creation of the IOTC is in direct agreement with Christensen’s model, which highlights the importance of separating out an independent organization from the parent entity to create a disruptive innovation. The spin-off of a smaller, more agile entity with a specific mission focus, in this case the creation of advanced cyber exploration and cyber attack solutions, allowed for shedding cumbersome and sometimes self-defeating processes and values from the parent organization, and replacing them with newly developed ones that were designed to be of service to the entirety of the new mission area. The IC recognized that the “information operations approach is so different that it will not fit into the older military paradigms…[we] must organize and attack the problem differently.” Areas where processes and value systems from the parent organizations needed to be overcome were special access program compartmentation and the creation of “jointness,” or interoperable capabilities that were not necessarily service or agency specific, as part of the national repository for CNE and CNA tools that was a core element of the IOTC mission. John Hamre’s willingness to “grant read-ins on special

---

programs related to the IOTC mission space…to avoid balkanization of capabilities or replication of efforts facilitated the success of the IOTC, and stands out as a significant process and value system change. DIRNSA’s Minihan, Hayden, Deputy Director Black and the former high-ranking DoD IO official continued to perform interagency reviews for sensitive capabilities and activities to remove CNA/CNE redundancies through the IOTC mechanism. These efforts also present a significant process and value change from normal bureaucratic functioning, coupled with high-level, direct leadership involvement in ensuring mission success.

The entirety of the IOTC CONOP agreement created an intricate set of processes based around a value system of “true interagency cooperation designed to integrate intelligence, technology, operational concepts, and potential solutions to legal and policy issues.” A variety of other collaborative processes that were antithetic to normal bureaucratic parochialism were put in place to ensure mission successes were set up to enhance interoperability, collaboration and deconfliction. For example, personnel were assigned by their parent organizations for a specified period of time as fully integrated members of the IOTC. The Joint Staff coordinated operational interfaces between

864 Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015.
IOTC and the Unified Commands,\textsuperscript{867} while CIA provided support for analysis, technology development, community coordination, and provided its expertise in conducting clandestine overseas operations. CIA also provided expertise for technology development for operations through existing partnerships with NSA for the benefit of the IOTC mission.\textsuperscript{868} DIA analysts and action officers were assigned to the Analysis and Assessments Group (AAG) and the Community Coordination Group (CCG) in direct support of the IOTC mission and provided all-source intelligence collection to the Advanced Technology Office (ATO), as appropriate.\textsuperscript{869} The CCG’s role was to coordinate IOTC technology development efforts “in satisfaction of validated CNA, exploitation, and related requirements”\textsuperscript{870} and provide the “DoD/IC Steering Group appropriate information and recommendations to facilitate Steering Group decisions and guidance.”\textsuperscript{871} These types of purposeful changes to create a new type of organizational structure are directly correlated with creating the CNO MMI.

The sunsetting of the IOTC provides additional support for the observations in the Innovator’s Dilemma and the efficacy of Christensen’s model for disruptive innovation

\textsuperscript{867} National Security Agency, “Information Operations Technology Center (IOTC) Concept of Operations (CONOP),” December 31, 1997 (Ft. Meade, MD: NSA). (Unclassified material extracted from classified document.)

\textsuperscript{868} National Security Agency, “Information Operations Technology Center (IOTC) Concept of Operations (CONOP),” December 31, 1997 (Ft. Meade, MD: NSA). (Unclassified material extracted from classified document.)

\textsuperscript{869} National Security Agency, “Information Operations Technology Center (IOTC) Concept of Operations (CONOP),” December 31, 1997 (Ft. Meade, MD: NSA). (Unclassified material extracted from classified document.)

\textsuperscript{870} By 2002, the sustaining elements of IOTC’s traditional DOD-style operations, namely the requirements development efforts and tool management functions established in the CONOP, were transitioned to STRATCOM’s Network Attack Support Staff, also domiciled at NSA (Michael V. Hayden, “IOTC Mission Accomplished,” Director’s Message: DIRgram-345, posted September 28, 2004).

\textsuperscript{871} National Security Agency, “Information Operations Technology Center (IOTC) Concept of Operations (CONOP),” December 31, 1997 (Ft. Meade, MD: NSA). (Unclassified material extracted from classified document.)
management, with one significant modification. Christensen did not stipulate whether the small spin-off organization would continue to be a quasi-independent entity once a disruptive innovation was created, or if the organelle would be reabsorbed into its parent. NSA opted for reincorporation, and after seven years was able merge the two interrelated CNE and CNA development efforts which were substantially driven by NSA-developed technology and personnel since the early to mid-1980s. General Hayden directed that IOTC’s analysis and CNA technology development mission, and closely related NSA computer network exploitation development efforts, be combined and incorporated into an integrated effort at NSA to maximize the dual use potential of the staff’s efforts in September 2004. Hayden’s message to the NSA community elegantly described the changes ahead: “Virtually all of the IOTC’s analysts and technicians have been NSA experts on rotational assignment. However, the IOTC’s formal separation from NSA divided a workforce with exceptional dual-use potential across two organizations, one dedicated to computer network exploitation (CNE) and the other to CNA. Bringing this workforce together will eliminate artificial boundaries and enable a larger cadre to contribute across the entire mission space. The IOTC and its mission are not going away. They’re coming home.” See Table 19 for a summary.

Table 19. Model for Creating and Managing Disruptive Innovation

<table>
<thead>
<tr>
<th>Theory Tenets</th>
<th>Presence or Absence</th>
</tr>
</thead>
<tbody>
<tr>
<td>The organization was locked into its current processes and values. Innovation was only accomplished as a result of the presence of a champion (visionary) leader with sufficient power and prestige within the organization to overcome great resistance to change, including elements of internal processes and values.</td>
<td>Yes</td>
</tr>
<tr>
<td>Innovation occurred when leadership separated out an independent organization.</td>
<td>Yes</td>
</tr>
<tr>
<td>The new organization was autonomous.</td>
<td>Semi-Autonomous</td>
</tr>
<tr>
<td>The autonomous organization developed new processes and values required to solve a new problem.</td>
<td>Yes</td>
</tr>
<tr>
<td>Innovation was a result of creating a “heavy-weight team” to achieve an innovation objective.</td>
<td>Yes</td>
</tr>
<tr>
<td>A heavy-weight team was created from disparate intra- or extra-organizational departments.</td>
<td>Yes</td>
</tr>
<tr>
<td>A new organizational boundary was drawn around the group.</td>
<td>Yes</td>
</tr>
<tr>
<td>Innovation is a result of a purposeful change to an organizational structure.</td>
<td>Yes</td>
</tr>
<tr>
<td>The purposeful change to organizational structure is directly correlated with creating innovation.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
CHAPTER 8. CONCLUSIONS AND IMPLICATIONS

Introduction

Rosen’s intraservice rivalry theory provides the best overall explanation for the development of CNO as a major military innovation. This is evident through an examination of the main areas of disagreement between the three theories and an analysis of the hypotheses statements against the case evidence. In this chapter I will briefly review the findings of the case history analysis in light of the traditional MMI theories. In an effort to extend the explanatory power of traditional MMI theories, the case history was also analyzed through the perspective of Christensen’s model of disruptive innovation management. My findings indicate the innovation management techniques executed during the main period of MMI activity substantially match major elements of Christensen’s model. Next, I examine an element of Terry Pierce’s model for disruptive military innovation to provide an enhanced explanation of how CNO developed as a MMI. Finally, based on the findings from the case study and theory analysis, I provide generalized suggestions for policy makers that may more fully inform future innovation management efforts. I will then suggest possible future areas of research for MMIs to advance the scholarly literature.

In this study I have proven that CNO is a major military innovation under two distinct analytical frameworks. In Chapter 1 I show that CNO is a MMI in accordance
with Andrew Krepinevich’s framework. The detailed CNO case history provided in the preceding chapters is also in close alignment with Rosen’s definition of a MMI. It is clear that CNO development led to organizational changes in NSA (and by extension Cybercom) and CIA, caused substantial modifications to traditional approaches in intelligence collection and resulted in technical competencies to perform full-spectrum computer network operations, which includes destructive attacks. The growth and maturation of CNO as a MMI can also be viewed as the application of new technologies into a system that combined innovative operational concepts and organizational adaptation in a way that is beginning to fundamentally alter the character and conduct of nation-state conflict.

This dissertation is the first time the IC has been studied as a possible creator of a MMI. Not only is the role of the US Intelligence Community central to the creation and use of CNO methodologies, this is in fact the first time a weapons capability was created by the Intelligence Community. This capability evolved over a 30-year period of research and operational development. Today the IC continues to be the seat of expertise and capability for CNO in the US government. As such, the findings of this study represent a potentially new development in the traditional pathways that lead to the creation of the tools of warfare. This study is also important for the broader innovation theory literature, as the same drivers for innovation, and entrenched organizational pathologies, appear to be operant in both intelligence and military organizations. Future MMIs, regardless of organizational origin, can be tested against the theory confirming and theory informing outcomes from this study to understand if they developed in substantially the same way.
Finally, this study has provided the first presentation of the origins and efforts of the IOTC in the open source. The seven-year history of interagency CNO tool development, including this special organization’s efforts, for example, in support of TAO,\textsuperscript{874} intelligence-driven targeting methodologies, independent verification and validation as well as policy development, is likely a key case in and of itself for how to mature a disruptive innovation. I believe the collaborative innovation approach undertaken through the IOTC to mature CNO provides a key lesson for future IC and DoD MMI development, one that is possible to replicate. NSA and the IOTC’s unparalleled importance to CNA as a MMI cannot be underestimated. As an outgrowth of the IOTC study, it was determined that NSA engaged in computer exploitation as early as 1986, which is newly available information and historically important. A basket of operations, technology and research organizations evolved and merged over time to create Tailored Access Operations, which was established in 1995 as the K 7 organization, significantly benefitting from IOTC’s creation and development (see Appendix A).

**What Theory Best Explains Why Computer Network Operations Emerged as a Major Military Innovation?**

Stephen Rosen’s intraservice rivalry model of military innovation provides the most compelling, theory-congruent explanation of why computer network operations

\textsuperscript{874} For example, see: National Security Agency, “Memorandum of Understanding Between National Security Agency/Signal Intelligence Directorate/Data Acquisition/Tailored Access Operations/Remote Operations Center and Information Operations Technology Center for Tool Transfer,” 24 September 2001 (Ft. Meade, MD: NSA). The document is related to the withdrawal and transfer of the MOUNTEBANK tool for development and possible use in computer network exploitation activities.
emerged as a major military innovation, although elements of civilian–military relations and interservice rivalry were found to be operant factors to lesser degrees.

The case history clearly shows that CNO developed along parameters described by Rosen in *Winning the Next War: Innovation and the Modern Military*. The CNO MMI resulted from the development of a predoctrinal new theory of victory by a series of senior leaders who were able to successfully explain and demonstrate, over time, what the next war would look like and how it must be fought if it was to be won. This new theory of victory was coupled with the adaptation, exploitation and use of emerging information and communication technologies to create a MMI. The technological development and scaling of efforts necessary to transform nascent CNO capabilities into a MMI was a slow internal process, effectively stretching across a generation. The MMI was achieved as result of a very specific alignment of senior leaders and their talented support officers who, in several instances, eventually succeeded their mentors in leadership roles, and each of whom worked in intelligence organizations—most prominently the ONI, AIA, NSA and CIA. The initiatives undertaken by these leaders and their support staff resulted in significant organizational, process and mission-based changes that led to a major achievement with global impacts. Civilian involvement (intervention) was shown to be effective to the extent that it was used to support the self-initiated goals of intelligence officials. Technological development preceded doctrinal development in each time period studied as predicted by Rosen’s theory.

More specifically, at NSA, the rapid peacetime advances in transmitting data across digitally based information and communications technologies necessitated the
development of Global Network Intelligence collection and Tailored Access capabilities, which ignited a variety of internal and external bureaucratic struggles. Partisan interagency intransigence was only overcome through the efforts of visionary leaders, aligned with likeminded advocates and interagency allies, coupled with sufficient resources to ensure that the vision of a new integrated technical approach for espionage, sabotage and warfighting became a reality. A paradigm shift to Active SIGINT, a phrase that encapsulated activities that were a combined outgrowth of Information Warfare and Global Network Intelligence collection, were coupled with the IOTC’s advanced CNO tool development, intelligence analysis and targeting activities, and resulted in a new way of war. The weaponization of CNO capabilities, shared through a national repository, substantively changed the ways NSA, CIA and DoD organizational components related to each other and how they configured themselves to fight America’s enemies. During any one of the time periods studied, CNO innovation developments which might appear to be sustaining and incremental in nature are actually disruptive and revolutionary in their totality, and represent an archetypal change for warfare. The coupling of evolving technology, developments in exploitation and attack capabilities with incremental doctrinal changes were shepherded over time by a series of internal champions at NSA who possessed sufficient organizational prestige and the strategic vision necessary to create a MMI, ultimately leading to the establishment of CYBERCOM.

Similarly, modern CNO capabilities at CIA started as a twelve-person branch in the Directorate of Intelligence in the pre-1995 time period, also in response to rapid technological changes, shaped by a mid-level officer’s experience with IW special
technical operations activities during the 1980s. As a result of this officer’s thoughtful leadership and a white paper, CIA came to understand that adaptations to ICT changes would significantly advance their traditional mission space activities, but required an organizational reconfiguration to maximize their intelligence collection and clandestine activity opportunities. CIA, through the direct efforts of Glenn Gaffney and technologist Jim Gosler, with support from Director George Tenet, leveraged the Agency’s inherent strength in HUMINT operational methods and innovative technology development. These HUMINT capabilities were merged with a technical operations approach that created a revolution in collection and special activities for the Agency. After proving this evolving concept of operations over a period of five years in collaboration with DS&T, the Clandestine Information Technology Office became a formal arm of the Directorate of Operations/National Clandestine Service. The newly evolved entity, known as the Information Operations Center, was subsequently empowered to conduct full-spectrum cyber operations.\textsuperscript{875} After fifteen years of development, growth and success in the DO, IOC has now been transformed into an entirely new, separate and distinct Directorate known as DDI.\textsuperscript{876}

In \textit{Winning the Next War}, Rosen systematically refuted Posen’s list of significant, requisite drivers needed for innovation, including previous defeat in wartime, a heightened threat environment, civilian intervention (in alignment with a military


maverick) as a key element that generated innovation and integration, as well as the primacy of doctrine as the progenitor of technological innovation. While elements of Posen’s theory of Civilian–Military relations were present in the case history, the core tenets of his theory were not found to be causative, necessary or sufficient to explain the development of CNO as a MMI. The overall role of the external threat environment as a driver for innovation does not sufficiently explain the long-term, internal technological analysis and development efforts that resulted in CNO capabilities, and arguably the totality of the advancements in this capability occurred independent of any major war, let alone a recent military defeat. Posen posited that doctrine drives technology changes, and this is clearly not how CNO developed as detailed in the case history and subsequent analysis in Chapters 3-6. Finally, there is limited evidence that civilian intervention was a key factor driving integration and innovation in CNO. In 1996 Ken Minihan was named DIRNSA, a move that was clearly an executive branch civilian intervention, however, at best this move can only be seen as a contributing factor to innovation and integration at NSA: Many of the foundational and Information Warfare and computer network exploitation innovations were already well underway. Minihan undoubtedly set the table for status quo change at NSA by championing a new paradigm for warfare and establishing the IOTC mechanism, but the actual key organizational realignments and many of the additional technological innovations and integrations were accomplished under the direction of DIRNSA Hayden, Deputy Director Bill Black and IOTC Director Bill Marshall, whose roles and decisions cannot be substantively attributed to civilian intervention.
Sapolsky, Armacost and Cote’s works focus on the dynamics of interservice rivalry to explain the creation of MMIs. Once again, while elements of this analytic frame were present in the case history, the core tenets of their theories were not found to be causative, necessary or sufficient to explain the development of CNO as a MMI. Elements of Interservice rivalry between NSA and CIA were present during the 1996-2002 time period, however, the entirety of the case history shows more cooperative than competitive interactions between the USN, NSA, CIA and Title 10 DoD organizations. The conflict over end-point targets related to data at rest versus data in motion, and CIA’s fears that DIRNSA Minihan was trying to pre-emptively claim the totality of the cyber operational arena for NSA were real, and the resultant maneuvering by each organization to maintain control over traditional mission space and organizational relevance clearly occurred. Still, whatever tension existed between NSA and CIA during the 1996-2002 time frame—admittedly an important innovation period—did not interfere with their operational collaboration nor the innovative joint activities executed through the IOTC. Similarly, Interservice rivalry theory states that organizations seek to maintain their budget authority and end-strength, and thus maintain control over their traditional missions to ensure their ongoing relevance, as well as resource allocations they believe “accrue to their unique strategic approach to war fighting.”

However, there is insufficient evidence in the case history to conclude that this competitive situation led to a bureaucratic fight over resource allocation or budgetary dollars. Actual funding requests

---

never seemed to be at issue, nor is there any evidence that a zero-sum game for CNO funding between NSA and CIA occurred, based on a review of the existing literature and the interviews conducted for this study. Funding issues for CNO were a DoD concern and, driven by the tyranny of their Programming, Planning, Budget and Execution (PPBE) process which did not account for funding CNO activities through a supplemental mechanism, affected their ability and willingness to make substantial contributions to the IOTC joint enterprise.

The case history does not support the interagency rivalry theory principle that competing technological initiatives generate more rapid innovation. NSA always possessed the broader core SIGINT capacities, technological capabilities and industrial strength collection approaches, a system CIA was ill equipped to compete against directly to achieve any measure of true ascendency. Moreover, it was the interagency cooperation between NSA and CIA channeled through the IOTC mechanism that led to the maturation of CNE and CNA technologies, intelligence-driven targeting and indirectly informs modern approaches to cyber kill chain and CNA-OPE activities today. The joint NSA/CIA efforts at IOTC enjoyed the tacit and explicit support of the DCIA. Moreover, the case history does not contain any information that competing technological initiatives resulting in more rapid innovation were pursued in a competitive manner by any organization separate from their IOTC collaboration in order to gain mission area ascendency. Counterfactually, it was only after President Bush signed off on a compromise allowing both agencies to collect data at rest in accordance with their SIGINT and HUMINT authorities, ending a bureaucratic controversy over targets, that
CNO was fully transformed.\textsuperscript{878} This decision, coupled with the continued use of the Trilateral MOA deconfliction mechanism,\textsuperscript{879} helped suppress bureaucratic infighting. The decision also likely provided a requisite level of operational certainty for each organization, thus allowing them to develop additional capabilities and conduct more comprehensive efforts over time under their respective authorities.

**Implications for Future Innovation Efforts**

The dynamics Rosen, Christensen and Pierce described in their models, combined with information uncovered during the case history research, may assist policy makers and innovation leaders in the DoD and IC in their long-range research, development and capability planning.

The CNO MMI was achieved through a mixture of approaches Christensen identified as successful managerial methods to foster disruptive innovation. The case history showed NSA was able to achieve success by separating out a new spin-off organization, the IOTC, staffed with “heavy-weight” teams of experts from internal and external organizations with new organizational boundaries that cross-cut existing technical and managerial approaches. This organization was effectively stripped of counterproductive legacy approaches and encouraged to develop new processes and values required to solve a new problem. As with Rosen’s theory, the role of a champion with sufficient prestige to overcome resistance to change directly factored into the


\textsuperscript{879} A Trilateral MOA was created between DoD, DOJ and the IC related to CNE/CNA activities focused on the deconfliction of various activities (Department of Defense, former high-ranking Department of Defense official responsible for IO at OSD, name withheld at individual’s request, interview by the author, McLean, VA, October 2015).
disruptive innovation success. NSA later reabsorbed the personnel from this organization into two key CNO elements within SID, and transitioned additional capabilities to a newly created JFCC-NW, a STRATCOM organizational component, but one that was effectively commanded by Director, NSA. The model of IOTC offers a strong path forward for the Third Offset where coupling an emerging disruptive technology with a focused mission-specific goal can be brought to fruition for broad interagency application. It appears that the IOTC concept has not been replicated to create disruptive offensive military innovations since its sunsetting in 2004.

Current US efforts at disruptive military technology development are manifesting, at least publicly, as the Third Offset Strategy, which is built upon an evolving list of existing or emerging technologies applied to forward-looking operational areas of concern. Topical areas currently identified in the Third Offset Strategy include developing Advanced Computing/Cyber capabilities, Electromagnetic and RF dominance, C4I disaggregation, autonomous capabilities and advanced weapons systems, including Directed Energy and Hypersonic technologies. Today, US government directives and implementing instructions to develop new capabilities are

---

880 C4I (command, control, communications, computers and intelligence) disaggregation leverages the concept of satellite disaggregation, which refers to a space architecture concept that distributes capabilities across a variety of platforms to minimize vulnerability from anti-satellite attack capabilities that could theoretically be fielded by US adversaries. Applied to C4I, a disaggregated approach would protect these types of platforms as well through an adaptive network approach (Mike Gruss, “Disaggregation Giving Way to Broader Space Protection Strategy,” Spacenews.com, April 26, 2015, accessed October 12, 2016, http://spacenews.com/disaggregation-giving-way-to-broader-space-protection-strategy/).

highly prescriptive,\textsuperscript{882} programmatic, acquisition focused, inherently risk adverse and are unfortunately designed to support sustaining innovations. It is unclear whether the recent round of identified technologies for the Third Offset Strategy can or will result in disruptive or sustaining innovations. Based on the case history and theoretical perspectives outlined in this dissertation, applying typical processes and procedures within existing organizations charged with developing these technologies will most likely be sustaining in nature, absent the development of a currently undisclosed technical approach that evolves from current U.S. research activities. The following sections provide generalizable observations as to why and how the CNO MMI was realized, which may be applicable to the Third Offset Strategy.

The main element necessary to achieve large-scale disruptive innovation was a predoctrinal theory of victory generated by an influential champion as predicted by Stephen Rosen. This champion combined emerging technologies with elements drawn from previous military tactics to build expanded dual-use capabilities for intelligence collection and computer system attack. This technical approach ensured widespread applicability to vast categories of targets due to the ubiquity of interconnected information processing systems. Successions of senior Intelligence Community leaders were key drivers of innovation, and were provided with significant top cover from various executive branch civilian leaders over time. Substantive organizational

\textsuperscript{882} Policy makers should be mindful of Martin Van Creveld’s studies of military innovation. The origins of tanks, jet engine, radar, helicopter as well as nuclear weapons were not a result of a doctrinal requirements laid down by the military. Simply put, military demand was not the source of new military technologies in the 20\textsuperscript{th} century (Martin Van Creveld, \textit{Technology and War: From 2000 B.C. to the Present} (New York: Free Press, 1989)).
realignments were coupled with the creation of new career paths commensurate with key technical skills needed to successfully execute a new theory of victory. While resources were helpful—and indeed as heightened external threats arose post-9/11, funding levels increased—the significant, foundational technological innovations for CNO actually occurred when resources were internally scarce. An inference can be drawn from the case history that the next “new theory of victory” will likely be linked with an emerging technology or basket of technologies that is currently under development in academic and commercial incubators. A robust predoctrinal theory or concept of victory may also leverage a combination of smaller systems (or a “systems of systems” engineering approach) brought to bear in a novel or repurposed, recombinant manner.

The development of CNO as a MMI has implications for disruptive innovation management. Based on the lessons learned from the case history, novel or emerging technologies that might reasonably fulfill a new theory of victory should be approached, broadly speaking, as a two-step process. The initial evaluation of a novel or emerging technology should not impose requirements at the onset of an investigatory phase so that the fullest possible range of applications can be creatively explored and perhaps incubated, including exploring any potential military utility. Once a technology has sufficiently matured, then it can be evaluated for a specific military application and fed into a more deliberate application-specific maturation process. This process, especially when dealing with advanced science or technologies, clearly should have an empowered champion with significant intellectual capacity and a variety of hard and soft skills.
Those hoping to operationalize a new theory of victory should seriously consider LTG Minihan’s philosophy toward fostering innovation for IW capabilities: “If it doesn’t satisfy a requirement, it’s a good idea.” AIA under Minihan, in his role of champion, established a type of freeform think tank or incubator far from the oversight of Washington, DC, which “opened up a lot of new frontiers” in information operations (computer network attack/Information Warfare). This innovation unit was composed of redirected EW practitioners, who essentially developed their approaches from a bottom-up, hands-on perspective—in other words, these new tools of warfare were not generated by DARPA, a Service component or even a national research laboratory. True innovation does not typically conform to rigid acquisition parameters, but is instead an iterative trial-and-error process by the end-users themselves. A possible path forward for future disruptive innovation generation should include the use of technology harvesting strategies by experienced hands-on operators not bound by DoD 5000R type requirements, coupled only to reasonably focused mission-based criteria. Normal chain of command communication pathways may interfere with the ability of these operators to highlight their findings to senior leaders. A method to conceptually outline and demonstrate the efficacy of new approaches directly to senior leaders should be put in place to overcome instances where middle managers may not recognize the utility of a disruptive initiative and fail to advance it accordingly. Furthermore, any early developmental activities should directly involve feedback from end-use operators early

884 Unfortunately, typical research, development, test and evaluation efforts are linear Programming, Planning, Budget and Execution (PPBE)-driven acquisition-centric approaches based on fixed military or intelligence requirements. These are outsourced by contract to systems integrators, who have to meet cost, scope and schedule requirements.
on in the technology maturation process. Once these findings are communicated, and in some cases displayed as prototypes or models, the technology maturation can be fed into a more deliberate process inside a spin-off organizational entity like the IOTC. At the onset of this second-stage process, managers who are adapting an emerging technology to fulfill their new theory of victory should account for a reasonable estimate of future mission needs and possible use cases for these technologies; conduct dynamic assessments of intelligence collection regarding adversary technological development plans, doctrinal developments and geopolitical intentions; provide an adversarial vulnerability analysis; and look for technological adoption by adversaries as the indigenous new theory of victory is being operationalized. Finally, to enhance this approach, managers should incorporate contributions from intelligence entities throughout the disruptive innovation lifecycle including iterative adversarial vulnerability analyses to ensure technological efficacy.

For their part, senior leaders and line managers who are placed in charge of developing disruptive innovations in an incubator or IOTC-like entity must have deep facility across a variety of parameters to be successful champions. This includes possessing technical competence sufficient to understand complex technology systems, capable of direct formulation of adaptive doctrinal development, to ensure the full utilization of the technology and be empowered to shape organizational realignments—three key factors that, when combined, create disruptive innovation. These leaders should be politically skilled enough to overcome internal resistance based on status quo thinking. These leaders should also be empowered with sufficient organizational authority at the
onset of a project to sideline individuals—or even, in extreme cases, organizational elements—who present parochial impediments. This type of flexibility, however, is more often found in small business owners than large government organizations. Organizations that are charged with developing a new theory of victory must have requisite core competencies with sufficient numbers of technically capable personnel already in place, with an alignment of dedicated leadership and mid-level officers with clear promotional pathways. These types of leaders, personnel and organizations have the best opportunity to successfully manage innovative concepts and make them strategically useful. This combination of leaders, middle managers and core technical personnel should be placed in charge of projects from basic concept through at least a prototypical demonstration in an operational high-fidelity environment, what the US government typically describes as Technology Readiness Levels 1-7.

While the combination of Rosen and Christensen’s work can more fully inform future approaches for technology development and innovation management, an additional element is needed to provide the fullest explanation possible for how disruptive military innovation occurred in the CNO case, and how it might occur again. Terry Pierce recognized that disruptive military innovation results from the combination and integration of technological and doctrinal changes which result in new linkages between existing constituent components, which are then applied in a new, more powerful way.\(^{885}\) Pierce, drawing on the work of Henderson and Clark, explained that technological innovation is derived from a deep understanding of components that are integrated and

linked together into a coherent whole through a process of systems development and systems integration. Once this type of systems integration is well characterized and understood, disruptive military innovations can occur through the reconfiguration of established doctrinal approaches to create something new.\textsuperscript{886}

\textit{The Relationship Between Technology and Doctrine}

As discussed during the literature review, the relationship between technology and doctrine is part of a long-standing doctrinal debate, most notably between Barry Posen and Stephen Rosen. For each time period studied, the findings of the case history clearly indicate that technology and capability existed prior to the formalization in doctrine. Table 20 highlights the relatively small, incremental component changes in doctrine over time. As described in the case history, JSSG activities provided key elements for a proof of concept operational capability (and what would later become CNE and CNA\textsubscript{1})—namely breaking into an information network and disrupting or denying communications on that network;\textsuperscript{887} however, these capabilities are not specified or mentioned in the C3CM doctrine. Functions that would be critical to the JSSG’s activities under the C3CM doctrine, such as targeting, maneuver and intelligence support, were not carried over explicitly as elements of the Information Warfare doctrine, which made its debut in 1992. Instead, a computer network attack component was added to the IW doctrine—although arguably targeting, maneuver and intelligence support would be an inherent part of this activity. Furthermore, the explicit use of the term computer

\textsuperscript{886} Rebecca M. Henderson and Kim B. Clark, “Architectural Innovation: The Reconfiguration of Existing Product Technologies and the Failure of Established Firms,” \textit{Administrative Science Quarterly} (1990): 9-30. Pierce called this construct an architectural innovation, which was disruptive by its nature.

network attack clearly was codifying the capabilities created during the 1980s under the JSSG. The other main components of the classified 1992 IW doctrine (renamed Information Operations (IO) in 1996) stayed the same over a fifteen-year period.

The term IO entered into use in late 1996, and now contained a discrete component known as computer network operations, which was both a nomenclature change and substantive acknowledgement of capabilities development. The umbrella term IO was subdivided into subcomponent parts named CNE, CNA and CND, also modest doctrinal modifications. Interestingly, this revised document finally acknowledged a role for computer network exploitation in the overall doctrinal approach, a mechanism that was already in use for a decade. Once again, the change in doctrine was codifying the capabilities already created. By 1998 (once the IOTC was up and running and NSA was granted the authority to develop computer network attack tools), CNO, a subset of overall Information Operations doctrine, was then further refined as CNE, CNA₁ and CNA₂ (and CND). This further explanation of what CNO entailed patently acknowledges that physical destruction could result from digital means, which implies the capability already existed, and was at least proven to work through testing. In 2006 an acknowledged role for intelligence support, and the operationalization of intelligence necessary to be directly integrated with CNA₁ and CNA₂, reemerged in military cyber operations doctrine. This doctrinal change inherently reintroduced the role of targeting for CNO, a term not used since the 1980s, but which had never truly gone away in practice. Furthermore, the acknowledgement of the CNA-OPE requirement was a modest doctrinal refinement that described an activity that was essential for successful CNA.
concept of operations for CNA-OPE overtly described in the 2006 doctrine is a dual-use, mature, converged interoperable network exploitation and attack capability supported by iterative intelligence collection. As shown in the case history, this capability was already explicitly acknowledged in the Information Operations Roadmap, released in 2003. Once again, the change in doctrine was codifying the capabilities already created, typically by several years’ time.
Table 20. Doctrine Development Over Time

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Network Attack_1</td>
<td></td>
<td></td>
<td>Computer Network Attack_1</td>
<td>Compu...</td>
<td>Computer Network Attack_2</td>
<td></td>
</tr>
<tr>
<td>Computer Network Attack_2</td>
<td></td>
<td></td>
<td>Computer Network Attack_2</td>
<td>Compu...</td>
<td>Computer Network Attack_3</td>
<td></td>
</tr>
<tr>
<td>Computer Network Defense</td>
<td></td>
<td></td>
<td>Computer Network Defense</td>
<td>Compu...</td>
<td></td>
<td>Computer Network Attack, Operational Preparation of the Environment</td>
</tr>
<tr>
<td>target</td>
<td>Deception</td>
<td>Destruction</td>
<td>Destruction</td>
<td>Deception</td>
<td>Deception</td>
<td>Deception</td>
</tr>
<tr>
<td>Deception</td>
<td>Deception</td>
<td>Deception</td>
<td>Deception</td>
<td>Deception</td>
<td>Deception</td>
<td>Deception</td>
</tr>
<tr>
<td>Electronic Warfare</td>
<td>Electronic Warfare</td>
<td>Electronic Warfare</td>
<td>Electronic Warfare</td>
<td>Electronic Warfare</td>
<td>Electronic Warfare</td>
<td>Electronic Warfare</td>
</tr>
<tr>
<td>Intelligence Support</td>
<td></td>
<td></td>
<td>Intelligence Support</td>
<td>Operationalizing</td>
<td>Intelligence Support</td>
<td>Operationalizing</td>
</tr>
</tbody>
</table>

Note. Gold Boxes Indicate unique or new elements to the evolution of the doctrine over time.

Future Research Agenda

This dissertation points to several fruitful areas of future research on the theory of major military innovations, the role of the Intelligence Community in MMIs, and furthering our understanding of the development of computer network operations.
Armed unmanned aerial systems (UAS) are a prominent example of an emergent MMI in the 21st century that was developed, at least in part, by the Intelligence Community. UAS came into being as a result of a series of technology changes, systems development, an operational innovation and organizational adaptations and is a precursor to the robotics revolution in warfare. UAS also caused organizational adaptations in both the Intelligence Community and the Department of Defense patterned after the MMI definition used in this dissertation. It must be noted that this new instrument of power is still in the process of being incorporated and refined in an iterative cycle similar to CNO. My preliminary research indicates the developmental models will have some similarities to the dynamics revealed in the CNO case study. I believe a comparison of these two IC-driven MMIs will provide further insights for bringing disruptive innovation to fruition more rapidly in the future.

Based on the findings in this study, a variety of future research should be conducted to more fully understand the developmental history of computer network operations. First, does the US CNO development model hold for our allied partners? Do the same development dynamics for CNO hold true in other large nations, as well as smaller ones who are choosing to emulate and adopt this new type of weapons system? If so, what can we learn from a comparative analysis between the US and other nation-states?

A fascinating study to conduct would provide a network/link analysis of key individuals and organizations involved in previous MMI creation to see what patterns emerge. The CNO case itself would be a prime candidate. The study showed a very
particular intersection of senior leaders, comparatively more junior officers and dedicated civilians that contributed to the rise of computer network operations. Admiral Studeman commented that innovation is usually generated by “a small core of interconnected people pushing other people, programs and ideas around to achieve a transformational goal. Typically, personalities will emerge around a situation or a topic—these are extreme teams of the best, most talented people with a specifically defined mission. There is usually a collective spiraling up of an idea, opportunities to develop the idea present themselves operationally and soon you’d have a doctrine.” This comment is intriguing. A longitudinal study tracking the interrelationships between these key individuals, the organizations they served in and their contributions to MMI or even sustaining innovation creation should prove to be instructive for future research and development efforts aimed at disruptive innovation.

Next, I suggest a deep dive be made into the organizational history and activities of the Joint Strategic Studies Group, which appears to have been the progenitor of Information Warfare and Computer Network attack in the USIC. The origins of this organization, its full scope of activities, how it intertwines with the later stages of the Cold War, nuclear weapons issues and the activities of the Reagan Administration will surely result in a fascinating, untold piece of history with implications for how the US might address future perils it can be expected to face. Similarly, the history of the IW “M” program, which was cancelled by Congressional action, is likely to fill an important historical gap in early IW capability development. For example, an analysis examining

888 Admiral William O. Studeman, interview by the author, Severna Park, MD, August 2015.
whether the program cancellation had a significant opportunity cost in development of CNA capabilities, or if ongoing GNI activities became a suitable surrogate, would be highly useful. Did the GNI programs allow NSA to overcome the loss of the IW program’s capability and substantively contribute to the success of CNA development? Conclusions as to whether this was accomplished with an analogous or dissimilar technical approach would be valuable for analysis of Type II innovation strategies described by Rosen in *Winning the Next War*.

Furthermore, the entirety of TAO’s organizational development in light of the theories and models presented in this study would likely provide significant management lessons to create future innovation organizations. The technological capabilities and structural developments of computer exploitation efforts by NSA G Group and its successor organizations warrant significant study. A paper based on this innovative time period should provide insights into a variety of important topics such as key technical skill sets necessary to launch the activities, how they changed over time, and the challenges faced by leaders focused on the early adoption of disruptive technology. Other key factors for innovation managers would detail why and how the programs continued to be funded in the face of significant bureaucratic intransigence and the ostracizing of proponents. (See Appendix A.)

Similarly, the developmental history of CITO, which resulted in a revolution in collection for the CIA Directorate of Operations, will likely prove to be a valuable bureaucratic and innovation theory case study as well. The historical origins, initial vision, stand-up and maturation of NTOC is also an important study to conduct in light of
the evolving cyber threatscapes and NSA’s future mission approaches as adversaries continue to emulate and adopt the CNO MMI paradigm.

Final Thoughts

I want to acknowledge the significant constraints that continuing classification of source materials and interviews/oral histories will have on future open source research and publication in this area. Fuller narratives related to the creation and activities of CYBERCOM and the contributing factors related to the establishment of CIA’s DDI are currently unavailable in any significant detail. While academically unfortunate, it is clearly necessary. This delimitation, which applies to the entirety of this study as well, should not deter USG researchers and academics alike from attempting further analysis within this subject area.
APPENDIX A. THE K 7 ORGANIZATION

As depicted below, and in light of recently declassified information NSA released for this study, it is now apparent that the USG began to engage in computer exploitation as early as 1986 under unit designator G8, after a computer exploitation feasibility study performed in P04. The exploitation of packet switching networks began in 1989 under unit P571, and later transitioned to targeting PBX technology as early as 1990, and merged with G08’s computer exploitation efforts in 1991. Similarly, efforts to collect SIGINT against Central Office Switches were performed jointly between P571 and CIA in 1989. Both G08 and P571 merged to form G44 in 1992, which eventually segued into what eventually became K 7 in 1995.\textsuperscript{889} Internally, NSA recognizes 1995 and the establishment of K 7 as the beginning of the TAO organization.\textsuperscript{890}


Figure A1. Establishment of K7.
Figure A2. Establishment of K 7 – Original.
Welcome to our telling of the "K7 Story – The First 12 Years" by some of those, both past and present, who worked in K7 and its predecessor organizations. If you were given a K7 overview today (December, 1998), you would find that K7 is working a dozen or so technology areas, and those areas are highlighted in the various K7 home pages. Each technology area has its own story to tell about how K7 got involved in working that technology. In some cases, various organizations were working parts of what is now worked in K7, and mergers over the years got us to where we are today. In other technology areas, they grew from our realization that given a new technology (e.g., ATM, Computer Telephony Integration) we had to be involved.

The "birth" of K7 is captured in an organization flow chart. Keep in mind the following as you read the reflections of our first 12 years:

1. The P04 feasibility study resulted in the creation of G08 in 1986. G08 was initially focused on computer exploitation. G08 is the organization which started, and evolved from G08 to G44 to K15 to K7. This computer exploitation activity merged with K14 who was doing related computer network activities, expanded over the years, and evolved to what is a major part of K13 today. Those who collectively tell the K7 "computer" story are:

2. K7's work in the technology area of packet switching networks has its roots in B Group (1985) when B Group was the office doing intelligence reporting on the Korea's, People's Republic of China, and Southeast Asian target countries. The packet switching network (PSN) effort came from B03 to P571 to G08 to G44 to K15 to become K732. Those who collectively tell the K7 "PSN" story are:

3. P571, as noted, began as an effort focused on the exploitation of packet switching networks, but a P571 PBX effort started in 1990 realizing the potential value of exploiting these customer premise voice systems. The P571 PBX effort moved to G08 (along with packet switches), and evolved to become an effort under G442, K152 and now K72. Those who collectively tell the K7 "PBX" story are:

4. K7's work in the technology area of central office switches began in 1989 in P571. It was SIGINT focused, and at that time we partnered with CIA. The effort was terminated temporarily in 1991, rejuvenated in 1993 when it was merged with an ASD/CJ1 effort, and it eventually evolved into what is now K74. Those who collectively tell the K7 "Central Office Switch" story are:

5. Lastly, we tell the story of K7 support to Information Operations (IO, formerly called Information Warfare) as it is currently performed in K75. Those who collectively tell the K7 "Support to Information Operations" story are:

We hope through these reflections that you get at least a sense of our history, and (if you are now assigned to ACNE Enterprise/K7) of the groundwork that has been laid for you to now "carry the torch" in your area of expertise.

(U) Anticipating Cyberspace Security:

William M. Nolte

(U) Cybersecurity—the safety of the electronic medium of computer networks—is now one of the principal issues in American national security planning and operations. The Department of Defense established the U.S. Cyber Command in 2009, and the Congressional Cybersecurity Caucus and various communities have conducted extensive hearings on the subject with officials across a wide range of agencies and departments. Executive branch papers on everything from a national cyber strategy to “educating the cyber workforce” are now common, as are complementary efforts from think tanks, universities, and the corporate sector. The President has a cybersecurity coordinator within his executive office.

(U) The reasons for this level of attention are not hard to determine. Information and information technologies are now central to how Americans—along with the rest of the world—conduct their lives. In some countries, more people have access to cell phones than have access to clean water. In the developed nations, the average citizen has access to more computing power in his or her smart phone than supported the Apollo program or the earliest space shuttle launches. Perhaps most importantly, attacks on information systems that form part of the world’s cyberspace are no longer the province simply of individual hackers out to prove they can “beat the system”; nation states now attack information systems within or belonging to other nations or private corporations.

(U) This essay reflects a first effort to examine how one major American intelligence agency, the National Security Agency, encountered the early emanations of cyberspace and attempted to define that space and how it would (or would not) fit within NSAs structures, missions, and authorities. The essay is based on approximately ten cubic feet of NSA documents largely compiled between 1993 and 1995. The historian for U.S. Cyber Command holds these documents and commissioned this review to assist in the development of a command history.

(U) These documents show an agency becoming alert that “something new was out there” in its operational environment, something that may or may not align with traditional understandings of information warfare and electronic warfare. The documents demonstrate an early perception, if not a full understanding, that this new phenomenon had potential implications both for NSA’s “offensive” (signals intelligence) and “defensive” (then known as communications security or COMSEC, more recently as information assurance or IA) missions. Finally, these sources reveal that whatever the nature of the new phenomenon, possible responses to it may not fit easily within either mission or within the legislation and regulations

(U) Defining Domains

(U) The development of information technology and systems has been as rapid as it has been pervasive. In 1965, Intel Corporation founder Gordon Moore wrote his landmark prediction in four pages that the appearance of powerful integrated circuits would be incorporated into the average workplace, home, and school. As Moore put it at the time, he believed it would be possible for people to wear wristwatches that contained integrated circuitry if the display problem were solved. This application and many others he suggested were resolved within a short period. (In 1965, however, Moore could not have foreseen that wristwatches would become a mark of a generational divide, with younger generations checking the time—and getting a mass of other information—from their smart phones or tablets.) If anything, the pace of change in information systems has exceeded what became known as Moore's Law and seems unlikely to slow over the next ten or twenty years.

(U) In light of these developments, the security implications of what became known as cyberspace and the integration of those implications into American national security have proven complex. When does an attack on an American system merit consideration as a crime? Or as an act of war? What are the responsibilities of various government agencies to protect...
CRYPTOLOGIC QUARTERLY

American systems against attack from other nations, groups, or even individuals? Which systems are to be protected? Defense and other governmental systems? Those of regulated public utilities? Of the private sector generally? As of late 2011, these questions remain under intense study, with no final answers available. Given the fluid state of the cyber environment, it may in fact be unreasonable to think in terms of "final" answers.

(U) What are the responsibilities of government agencies to protect American IT systems against attack from other nations, groups, or even individuals? Which systems are to be protected?

(U) Nevertheless, significant steps have been taken to define the national security issues created by cyberspace. A few have been noted above. Perhaps no action has been of greater conceptual significance than defining cyberspace as a national security domain for a large and influential audience, which then-Deputy Secretary of Defense William Lynn did in a 2010 article in Foreign Affairs. No doubt the definition had floated about the Pentagon and other locations before then, but whatever its provenance, it is a powerful step in aligning strategies and tools against a revolutionary change in the national security environment.

(U) The 20th century offers precedent for new security domains. In 1900 ground warfare and naval warfare were the only known national security domains (though the term national security domain comes later). After the invention of the airplane, nations needed to define an emerging air dimension, a process accelerated by the First World War. Nuclear weapons (and almost immediately the ballistic missile delivery systems) and space launchers also created the need for definition of new domains and responses to them.

(U) The first reality about new domains is that they are not self-defining. Different nations, with different histories, structures, and strategic needs will establish unique understandings of a new domain and responses to it. Britain established the Royal Air Force in 1918 but has revisited the role of the RAF and its relationship with the British Army and the Royal Navy, especially the latter, ever since. The United States did not establish an independent Air Force until 1947, and even then that decision left the Army, Navy, and Marines with their own "air forces." In the 1950s, the American services each launched ballistic missile development programs, as that domain (or subdomain) was under discussion. The Air Force assumed that because missiles flew they came under its purview, while the Army attempted to define the intercontinental ballistic missile (ICBM) as an extension of its historic artillery function. The Navy, having experienced what it perceived to be a critical threat to its mission (and its future) in the debate over nuclear weapons a decade earlier, did not want to be left out, and began the Polaris missile program. The Soviet Union, to cite a different response, dealt with the emerging ICBM field by creating a separate, long-range rocket service.

(U) With 20th-century precedents in mind, it should not surprise us that defining the national security implications of the cyber environment and instrumental responses to it takes time. Cyberspace is in some ways more complex and pervasive in its implications than any of the previous domains. The outer space domain proved relatively easy to deal with: once the international community determined that national air space did not extend indefinitely, a treaty prohibiting warfare in space was in place by 1967.
(U) No one should anticipate similar speed on a treaty governing and defining the cyber domain, though an international regime based on existing law, treaties, and regional agreements will appear, probably piece by piece.

(U) At the national level, arrangements and authorities designing the cyber domain will almost certainly follow, also piece by piece. This slowness may prove frustrating to members of the public confronting identity theft, to legislators wanting to appease the fears and frustrations of the public, and to policy makers charged with defining a "cyber structure." Some may describe this pace negatively as "muddling through," but sometimes muddling through is the only option. The United States is said to have established its Cold War national security structure in 1947 with passage of the National Security Act. A more accurate statement would be that the United States began to define its Cold War national security structure in 1947 but completed the process only in 1986 with passage of the Goldwater-Nichols Act—less than five years before the collapse of the Cold War adversary. In that sense perhaps, the United States muddled through the Cold War more effectively than efficiently. The effectiveness of the Cold War American national security apparatus proved more important as a metric than its relative inefficiency. In other words, a generally effective but often inefficient structure achieved its primary strategic goals.

(U) Defining the New Reality

In June 1994 NSA Director McConnell issued a memorandum for the National SIGINT Committee proposing to "Define "Information Systems Intelligence" and Designate "INFOSINT" as a Component of SIGINT." Even within that memorandum, the "definition" of INFOSINT is tentative, reflecting the fluidity of the phenomenon that NSA (and others) were attempting to identify and categorize. Before and after the June 1994 memorandum, the committee vigorously debated the characteristics of the new domain—what it was and what it

NSA and other organizations are currently exploring a variety of computer-based telecommunications and information processing systems for foreign intelligence purposes. As the targets, techniques, and methods vary widely, so do the definitions and related terminology which describe these activities. [emphasis added.]
The 1994 N511 Memorandum is an important mark of the work and thought NSA officials had expended on what would ultimately become cyberspace. That other organizations would not in the end accept—or would the environment support—the INFO/SINT definition or NSA's view of it as a component of SIGINT should not negate its importance in demonstrating one agency's understanding at a specific point in time.

The U.S. Cyber Command records on which this article is based reflect some of the history preceding the N511 INFO/SINT memorandum. Much of this documentation sheds light on efforts to understand what becomes the cybersecurity issue and its relationship to previously defined activities, including but not limited to NSA's signals intelligence and communications security missions. Within DOD, the growing importance of computers and computer-based information and systems was affecting known categories such as information warfare and electronic warfare. Did cybersecurity fit within one or more of these fields? Did it alter them while still being contained by them? Or was it something new?

Such questions had been raised before the June 1994 memorandum. In December 1992 the assistant secretary of defense for command, control, communications, and intelligence (ASC2I) published an IW directive (DOD T53060.1) that led NSA to create an IW working group. While attempting to operate within the IW framework, the group reported by spring 1993 that the "degree to which government and society rely on automated information systems, and the consequences of unauthorized access, corruption, or destruction of government, business, and personal databases is in itself a mandate for policy on information warfare." In a relatively short time it would become apparent that this very precise assessment of the changes driven by the world's reliance on automated information systems would take the discussion beyond the bounds of what had been known as information warfare. The N511 INFO/SINT memorandum reflects that change.

The brief proposes several choices for the future of COMPUINT. The first two, clearly straw men, are that either NSA should do all COMPUINT. The clearly preferred third option is "an integrated/integrated" COMPUINT: modeled on efforts in other projects, with the apportionment of effort on an individual case determined by the circumstances of the case. Apparent throughout the discussion of this period is an almost experimental approach to naming the new phenomenon. Not only do terms like COMPUINT come and go, they sometimes come again. The degree to which these shifts in terminology reflect growing understanding of the new environments, or the need to reach consensus among a range of agencies and other stakeholders, is a subject for further study. Suffice it to say that technical and bureaucratic factors commonly influence terminology changes, but these factors apparently did not disrupt the efforts to define cybersecurity. Only when the description in the COMPUINT brief of the emerging environment touches on how to operationalize reactions to the environment, and where to place operational control over all or part of it, does terminology become critical. For example, the term "information warfare" clearly implies actions appropriate to wagingfight components of the Defense Department but not to intelligence components, especially of NSA.
(U) The Authorities Issue

(TS) In July 1993 the NSA Information Warfare Working Group published a report in response to a DOD directive (TS3600.1) on information warfare. NSAs specific concern was that the directive implied that SIGINT and information security (INFOSEC) "fell" under the IW umbrella. NSA believed that this assigniment of responsibility did not accurately reflect the equities involved in balancing SIGINT needs versus INFOSEC needs or the trade-off analysis that must be made in determining whether to exploit or destroy an intelligence source. Distinguishing between information and electronic warfare had long been an issue: Military advantage might be gained by destroying an adversary's communications capabilities or systems, but at the cost of intelligence derived from the interception of those capabilities.

(SSS) In attempting to clarify the distinction between NSAs mission areas and at least some aspects of information warfare, the NSA working group prepared an overview of the authorities under which the Director of NSA (DIRNSA) and the Agency needed to operate, noting first the absence of a "unified legislative enactment or single, complete statement" codifying NSAs missions. Its authorities derived instead from a series of laws, executive orders, and regulations, beginning with the Truman memorandum creating the Agency in 1952. The documents that followed the 1952 memorandum define signals intelligence and DIRNSAs control of SIGINT activities, and define authority over both communications and information security.

(SSS) When the authorizing documents refer to DIRNSA and NIS involvement with information or electronic warfare, however, words such as "control" tend to be replaced by "support" or "assist." Directive TS3600.1 requires that intelligence elements (such as NSA) "assist" IW and EW operators in developing effective capabilities in those fields. In return, the EW and IW operators were required to keep DIRNSA informed of technology developments associated with their fields. The statements of authorities, in short, confirm NSAs association with IW and EW but provide no authority for NSA to operate in either field.

(SSS) Information warfare clearly implies actions appropriate to warfighting components of the Defense Department but not to intelligence components, especially NSA.

(0) Much of this division of missions would have seemed fully unexceptional to officials dealing with these issues at this time. NSA, like other intelligence agencies, operated, then as now, under the provisions of U.S. law (largely Title 50 of the U.S. Code) applying to intelligence, while DOD overall operates under provisions (Title 10) that provide the authority to make war or conduct military operations. The NSA working group concluded that Directive TS3600.1 tended to blur that distinction, "bumping" INFOSEC under the IW umbrella, and further noted that such a definition "any government entity with a personal computer" could be seen as practicing rudimentary defensive IW.

(0) As of July 1993 NSA appeared to be defending what it saw as a traditional clarity separating its missions from the IW concepts outlined in Directive TS3600.1. NSA had not traditionally conducted IW operations and was initially reluctant even to appear to seek to widen its authorities. At the same time, however, the IW working group seems to have realized at least at some level that the directive is merely a reflection of a changing environment in which the nation, not just DOD, relied increasingly on auto
CRYPTOLOGIC QUARTERLY

nated information systems. "Clearly," the group concludes, "information warfare extends beyond DOD and requires a serious, coordinated effort to develop broad national policy." In the years that followed, of course, the requirement for national response and national policy would spread far beyond IW to a national reliance on information systems that could not have been envisioned in 1993. NSA would develop its own strategies for dealing with Title 10/Title 50 and related issues with the Agency not always on the side of traditional arrangements and understandings. In retrospect, NSA officials, along with everyone else

(U) Beyond NSA:
A Broader Discussion

The NSA was not alone in assessing the developments taking place in the information environment and the implications for national security issues, including but not limited to information warfare. The National Security Council (NSC), the CIA, and Congress were also defining cyberspace and its impacts. NSA had early on suggested that the cyber domain could be considered a fourth component of SIGINT, but almost immediately, the reality that the new field possessed both offensive and defensive manifestations came into the discussion. This reality did not diminish NSA's potential role in the new field. In fact, it identified potential roles for both of NSA's mission components.

(TS) The NSA working group concluded that ... under [the Directive TS600.1] definition, "any government entity with a personal computer" could be seen as practicing rudimentary defensive information warfare.

(TS) The NSA working group concluded that ... under [the Directive TS600.1] definition, "any government entity with a personal computer" could be seen as practicing rudimentary defensive information warfare.

Concurrent with and drawing significantly from the July 1993 Working Group report, NSA briefed the deputy secretary of defense on IW and what NSA continued to call COMPUINT in a rapidly changing information environment. The briefing is, as one would expect, informational and not intended to be excessively provocative. Nevertheless, in its recommendations NSA noted the need to establish "rules for offensice IW in peace/crisis periods, specifically intelligence collection and covert action, and in wartime situations, intelligence collection and military action." This relatively bland statement conceals a developing controversy over authorities in a redefined IW environment that would eventually lead a principal

By 1994, if not earlier, the process of defining cyberspace had produced more detailed—and more institutionally sensitive—discussions of the roles and responsibilities that would be assigned to agencies of interest. In 1994 the National Security Council staff had begun work on a Presidential Review Directive on information warfare. Within a few months, the proposed PRO had been split in two—one dealing with offensive or "Information Based" operations, the other with defensive issues under the heading "National Information Assurance Strategy." The NSC intended to link the two at the end of the drafting/review process."
(U/FOUO) The Congress was also expressing interest in the division of effort on IW and related issues, with Senator Robert Byrd submitting a question for the record regarding the integration of intelligence from the various intelligence "streams." Congressional interest in the discussions, from various sources and in a range of formats, continued over the next two years.

(TS) Much of the interest—and even controversy—suggested in actions coming from organizations outside NSA, appears to reflect three unsettled questions. What was the nature of the issue (i.e., offensive or defensive) under analysis? To what degree could that issue be dealt with in existing doctrinal and organizational structures? And to what degree could it not be encompassed within existing arrangements, which agencies had or should have responsibility for which portions of the new environment?

(U) Toward an Operational Capability

(TS) As the discussions over the definition of COMPUINT or a transformed IW intensified, NSA began to move toward operational capability. By early 1996 NSA had begun to conceive of an "IW center" of some size and scope, even if it could not determine if its mission would be offensive, defensive, or both. Plans for a staff of some 300 employees from a range of NSA components, the military, had been produced. The clear intent was a national center, housed at and directed by NSA. None of the documents in these NSA records says so explicitly, but it is a reasonable assumption that the individuals working this problem understood that some measure of operational activity could not await the resolution of the authorities issue.

(TS/TSI) By May of 1996 NSA was prepared to request approval from Congress to reprogram funds to create the new center, beginning with nearly...
cials drafted a memorandum for Director Minihan's signature. The draft proposed that Director Minihan advise the DCI only that the request "may generate interest on the Hill regarding the broader aspects of operationalizing IW in the community." In reality, both this draft and the LAO summary of congressional sentiment represented significantly optimistic assessments of the situation "on the Hill." In May 1996, several less optimistic, internal NSA emails appeared.

Described concerns emanating from NSCI that went far beyond the naming of the new center. The HPSCI situation under the subject "the good, the bad, and the ugly." The only "good," an assurance from HPSCI staff member Caryn (almost certainly Caryn Wagner) that she did not intend to block progress; the bad was that HPSCI would not move on the reprogramming action. Her reasons, as described by the very blunt assessment that NSA had "not yet delivered the appropriate people and understructure to support the center."

(TS) The email raises a significant and important disagreement. The view from HPSCI was that NSA had not received concurrence on the reprogramming and the consequent green light on the center from the DCI. It notes that "despite Bill [William B. Lawless] implication and assurances that the DCI is partnering with us on this one, the committee (i.e., Caryn and [Ken [NHT]]) does not feel we've delivered on this one."

(TS) These concerns notwithstanding, NSA moved toward operationalizing what for some time would be called the Information Warfare Operations Center. Space formerly occupied by the National SIGINT Operations Center was identified, as were the personnel billets and other resources needed to bring the center into being. The Agency expressed hope for a center stand-up late in calendar 1996, though it acknowledged that this was optimistic.

(TS) It is impossible to assess, from the documents in this collection alone, all the factors leading to NSA's strategy at this time. The uncertainties on charter and coordination raised by HPSCI staffers and others on the Hill were shared, in some or all particulars, by officials within DOD and the Community Management staff. In his 10 February 1996 comments on the charter for the newly created position of special assistant for IW, NSA Assistant General Counsel Kevin Powers had advised of the limits of NSA's role in IW. He proposed altering the language to eliminate any sense that NSA had a role in conducting information warfare and to make clear that its role was limited to providing "support to information warfare."

By December 1996 the Defense Science Board (DSB), made up of civilian advisors to DOD, had entered the discussion with a report on defensive IW that strongly endorsed a leading role for NSA. Offensive IW likely was beyond the DSB's charter, but the absence of any reference to it in the report could have hurt NSA's case for an IW center. IW clearly was the focal point of a serious disagreement regarding the future of NSA's proposed center. At times, it should be noted, NSA suggested the possibility that its center should be "aimed at offensive IW" only.

(TS) Documents in these files from the second half of 1996 suggest increased activities in "extended IW" from components beyond NSA. Though not altogether opposed to NSA's views and efforts, these documents strongly suggest that as more people in Washington became focused on extended IW, NSA's leadership in defining and responding to it became diluted if not openly challenged. By the summer of 1996 Admiral Dennis Blair (then associate director of Central Intelligence for Military Support) suggested a case-by-case division of effort on offensive IW operations, along with creation of a center jointly operated by the IC and DOD. The Community Management Staff preferred a DCI center. The differences in these views notwithstanding, both challenged NSA's preference to direct the new center.
(S) Discussion intensified in the ensuing months. By August 1996 NSA was dealing with a congressionally directed action from Senator Ted Stevens, chair of the Senate Appropriations Committee, that raised significant questions about NSAs new center. Drafts prepared for Director Minihan attempted to deal with the most contentious issues related to the center, that is, offensive IW and NSAs role in such operations, by proposing a phased development of what was by then named the Information Warfare Technology Center. (The same Information Warfare Center of Excellence still shows up occasionally, but the former term Information Warfare Operations Center disappeared.) By September 1996 a draft charter for the IWTC explicitly declared it would “not conduct offensive operations, i.e., the IWTC will not be a trigger puller.”

(S) By March 1997 NSA had achieved agreement from the deputy secretary of defense and the acting DICI for creation of the again-renamed Information Operations Technology Center (IOTC). NSA had raised for DOD consideration its own “doubts” about its role in IW. In response to this concern, the secretary had provided NSA “with additional authority to conduct CNA [Computer Network Attack] and related functions.” After what must have been a bruising struggle, this represented a clear achievement for the Agency. This outcome notwithstanding, Robert E. Drake of NSA reported at that time on friction between NSA and Pentagon officials, specifically within the office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASCDCI). Drake reported allegations from Capt. Greg Blackburn of ASCDCI that NSA had “fuzzed” some issues involving the IOTC in testimony before HPSCI and SCINT. Support to Counter-Intelligence (SSCI). Reflecting the way small matters sometimes take on larger dimensions, Drake noted that some ASCDCI staff were unhappy that NSA had requested their presence and support in testimony before Congress without confirming their availability in advance. As Drake concluded, “nerves are a little raw in the community,” presumably regarding IW and the IOTC.

(U) In the end, and under its IOTC name, the new center stood up in 1997, shortly after the documents under review here closed. William Black retired before the stand-up, though he would return to NSA some years later as the Agency’s deputy director.

(S) The reality that the new field possessed both offensive and defensive manifestations identified potential roles for both of NSA’s mission components.

(U) Assessment and Next Steps

(U) The NSA documents at Cyber Command are important records. They clearly represent a compilation in a redacted office of materials from many sources. The office is almost certainly that of the Special Assistant for Information Warfare. Despite what appear to be significant gaps—for example, either nothing happened of great consequence through much of 1994 or those records are simply not here—the records provide the basis for understanding how a major intelligence agency dealt with an important, unfolding development in its operational environment.

(U) Nothing in these files reflects the operational or analytical work done to come to grips with the new reality of what would be known as cyberspace. The discussion over the authorities to conduct offensive or defensive IW in the new environment did reflect a developed capability to operate in those realms. But
these documents reveal nothing about the efforts to discover what was possible in, for example, computer network exploitation or computer network attack, terms later applied to major aspects of cyber domain operations. This gap reflects the view that the records examined here rely on the information coming from research and analysis on cyberspace and were created or retained by staff primarily concerned with policy or senior staff issues, not operational or analytic issues.

(UNCLASSIFIED) The requirement for national response and national policy would spread far beyond information warfare to a national reliance on information systems that could not have been envisioned in 1993.

(UNCLASSIFIED) Another characteristic of the records is that they were largely created by NSA. Some copies of documents produced by other entities, legislative or executive, appear as attachments or are summarized by NSA officials. These are useful but provide only a partial look at how forces external to NSA were viewing the new environment and NSA efforts to deal with it. NSA, for example, advanced the idea of considering COMPOINTER as a fourth element of SIGINT but quickly abandoned it. Was this change of direction the result of evidence and experience gathered within NSA, pointing to the importance of both defensive and offensive components that would encompass more than the signals intelligence mission? Or was the shift the result ofcountering views from the Congress, DOD, or another intelligence agency?

(UNCLASSIFIED) Another area largely unaddressed is that of resources. The 1990s were, after all, a period of genuine austerity in the U.S. intelligence community; a decade of cuts that produced an overall reduction in resources of 30 percent or so. Was some of the reluctance to accept or support NSA's new center, by whatever name, a result of the austerity with which the community had to deal? Even such efforts as reprogramming funds from within the Consolidated Cryptologic Program involved loss of resources to projects that may have had interested and potential constituencies outside NSA. How did the military services feel about the possibly increased role of NSA in areas such as information warfare, in which NSA had not traditionally been engaged? Did they see NSA's efforts as competitive rather than complementary or cooperative?

In summary, these documents are limited in breadth and provide only a partial chronology of NSA's efforts to come to grips with a rapidly changing environment. They record some of NSA's efforts to assess the implications of that environment for its missions, its structure, and its relationships with other parts of the national security establishment. That said, the documents are an important part of what needs to be a broader story of the effort to define the still-emerging cyber domain.

(U) Notes


2. (U) For this purpose, I am excluding diplomacy, though it clearly belongs as a national security domain in a slightly broader definition of national security.

3. (U) It is also, as others have noted, the most "man-made" of the domains, having little connection with any physical or at least geographic dimension.

4. (U) The nuclear domain and space domain cases offer interesting comparisons, beyond the scope here, on how domains get defined and regulated. Unlike the space domain, the nuclear domain was not regulated internationally until the 1968 Nuclear Test Ban Treaty of 1963, al-
most twenty years after its development and first use.

5. (U//FOUO) Thomas J. Lyghtt to F. [redacted] Berghoff
COMPUINT File, Cyber Command Documents.

6. (U//FOUO) Information Warfare Working Group
Directive Sub-Committee Report, 12 July 1993, drawer
1, Cyber Command Documents.

7. (U//FOUO) The slides for this briefing are outdated,
but a rough summary (1 March 1993) reads:

That is the background for Director
McConnell's 2 March testimony, with no refer-
ce to the committee or committees in question.
The legislative affairs office or the NSA Executive
Sovereignty should be able to provide that information.

The information in question involved
sometimes intense disagreements over the division
of efforts regarding U.S. responses to a new and fluid
information environment. The lack of reference to
COMPUINT as a fourth "sub-component" of St-
GINT suggests that NSA had begun to move past
that early position.

8. (U) See note 3.

9. (U//FOUO) Memorandum from the Record,
1 March 1995.

10. (U//FOUO) NSARC Document, NSARC-020-
25, 22 February 1995, drawer 2, Cyber Files, IW Feb-
Chenow 1995.

11. (U//FOUO) NSARC Document, NSARC-020-
25, 22 February 1995, drawer 2, Cyber Files, IW Feb-
Chenow 1995.

12. (U//FOUO) DRAFT DOD, December 1994, with
cover note from Executive Director
for Intelligence Community Affairs, 18 January 1995.

[U] William M. Noise is a research professor at the School of Public Policy, University of Maryland,
and director of the university's Program in Intelligence Research and Education. He retired from
federal service in March 2006, as chancellor of the National Intelligence University system. During his
career at NSA, he served as an analyst, member of the history staff, and in executive jobs including
commandant of the National Cryptologic School. His community assignments included two tours
as the National Intelligence Council.
APPENDIX C. GLOBAL NETWORK INFRASTRUCTURE (GNI)

APPENDIX D. SAMPLE INFORMATION OPERATIONS TECHNOLOGY CENTER (IOTC) MEMORANDUM OF UNDERSTANDING (MOU)

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE NATIONAL SECURITY AGENCY/SIGNALS INTELLIGENCE
DIRECTORATE/DATA ACQUISITION/TAILORED ACCESS
OPERATIONS/REMOTE OPERATIONS CENTER
AND
INFORMATION OPERATIONS TECHNOLOGY CENTER,
FOR
TOOL TRANSFER
24 September 2001

1.0 (U) REFERENCES:

1.1 (U) NSA Staff Processing Form and attendant Tool Request Worksheet, 5324-020-01, Chief, Remote Operations Center, 30 August 2001, subject: Request for IOTC Tool – APPROVAL.


1.3 (U) IOTC Concept of Operations, dated 29 January 1998.

1.4 (U) DCI/DOD MOA ('The IOTC Charter'), dated 3 March 97.

1.5 (U) Title 10 U.S.C. § 167.

1.6 (U) Joint Pub 3-13, Joint Doctrine for Information Operations, dated 09 October 98.

2.0 (S/P) SUBJECT: Memorandum of Understanding (MOU) between NSA's Remote Operations Center (ROC) and the Information Operations Technology Center (IOTC) for transfer of the MOUNTEBANK tool for evaluation and possible use in Computer Network Exploitation activities.

3.0 (S/P) PURPOSE: To delineate respective responsibilities of IOTC and ROC and assign tasks concerning the tool transfer. Activities under this MOU will be conducted in accordance with the MOU, CICP, and CICP policy and guidance, and applicable U.S. law (see references 1.3 through 1.6).
4.0 (U) BACKGROUND:

4.1 (SECRET) In accordance with Reference 1.1, it is anticipated that the NSA Remote Operations Center will in short time be authorized by Director, NSA, as a recipient of IOTC tools for NSA;

4.2 (U) References 1.3 and 1.4 authorize IOTC to develop, in conjunction with Department of Defense and Intelligence Community elements, compile and maintain IO and related techniques as a Toolbox for IO customers;

4.3 (SECRET) Tools consigned to the IOTC Toolbox may be used for various Computer Network Operations (CNO) functions such as attack, exploitation, and defense, or to provide CNO enabling functions such as providing access. A single tool may be used for more than one function. Authorized tool recipients must obtain proper authority for any intended tool use.

5.0 (U) SPECIFIC ROLES AND RESPONSIBILITIES:

5.1 (U/FOFO) The NSA ROC, within security classification guidelines, will:

5.1.1 (SECRET) Withdraw the MOUTEBANK tool from the Toolbox for development and possible use in Computer Network Exploitation activities;

5.1.2 (U/FOFO) At a minimum, adhere to IOTC tool-specific security classification guidelines or conditions as provided in the tool fact sheets or transfer documents;

5.1.3 (SECRET) Be responsible for development, evaluation, training on, and maintaining the requested tool for ROC use; an exception would be if ROC specifically requests technical assistance from the IOTC and if IOTC has resources available at the time of the request;

5.1.4 (SECRET) Provide written feedback to the IOTC within 30 days on any modifications made to the tool and feedback on the effectiveness of the tool;

5.1.5 (SECRET) Protect tool from loss, compromise or misuse and immediately notify IOTC in the event of loss, compromise or misuse. Initial notification may be made via secure telephone. Full details should be provided via message 90 days from the time of incident;

5.1.6 (U/FOFO) Tool requested and drawn by the ROC will be retained by the ROC indefinitely.

5.2 (U) IOTC, within security classification guidelines, will:
5.2.1 (S/NIP) After coordination with USSPACECOM (JTF-CNO), transfer the tool to the ROC in an authorized and mutually agreed upon manner;

5.2.2 (U) Provide support to tool development, evaluation, training, and maintenance if requested by the ROC and contingent upon existing IOTC resource commitments;

5.2.3 (U) Provide or recommend technical safeguards if requested by the ROC and contingent upon existing IOTC resource commitments;

5.2.4 (U) Protect tools from loss, compromise or misuse and provide the ROC notification in the event of loss, compromise or misuse during transfer;

5.2.5 (U) Provide notification of significant/functional updates to the tool.

6.0 (U) IMPLEMENTATION PLANS AND REVIEWS:

6.1 (U) The documentation accompanying the tool applies only to the version of the tool transferred. Any modifications or changes to the tool will require an update to the documentation and will be reviewed jointly for potential resubmission into the Toolbox;

6.2 (U) This MOU shall become effective upon signing and remain in effect for as long as the tool, in its current or modified form, remains in the possession of the ROC, or until terminated by both parties;

6.3 (U) The parties, on agreement, may make modifications or amendments to this MOU at any time.

7.0 (U) POINTS OF CONTACT:

7.1 (U) For the IOTC: USNR, DSN 544-2364 (STU-III), commercial (301)-688-2374 (STU-III), secure 963-2364.

7.2 (U) For the ROC: Remote Operations Center, commercial (301)-688-6771, secure 961-1461.

Dated: 9/27/01

SECRET/COMM/NOFORN/XTI
This appendix contains the full text of the National Security Agency’s declassified “Memorandum of Understanding Between the National Security Agency/Information Assurance Directorate (NSA/IAD) and the Information Operations Technology Center Regarding the Sharing of Computer Network Operations Capabilities,” January 31, 2003 (Ft. Meade, MD: NSA).
(U) MEMORANDUM OF UNDERSTANDING
BETWEEN
THE NATIONAL SECURITY AGENCY/
INFORMATION ASSURANCE DIRECTORATE
AND
THE INFORMATION OPERATIONS TECHNOLOGY CENTER
REGARDING THE SHARING OF COMPUTER NETWORK
OPERATIONS CAPABILITIES

I. (U/FOUO) Purpose: This Memorandum of Understanding (MOU) is intended to strengthen the partnership between the National Security Agency (NSA)/Information Assurance Directorate (IAD) and the Information Operations Technology Center (IOTC). This document is an agreement between the NSA/IAD and the IOTC on the sharing of Computer Network Operations (CNO) related technologies, tools, techniques, and procedures in support of the IOTC’s CNO missions and the IAD’s Information Assurance (IA) and Operations Security (OPSEC) missions. Both NSA/IAD and IOTC elements may use this MOU to exchange CNO related tools, techniques, and related tool technologies in accordance with the requirements of Annex A. Additional Annexes may be written at any time if a situation arises that is not included in this MOU.

II. (U) Background:

A. (U/FOUO) The IOTC was established as a joint activity of the Department of Defense (DoD) and the Intelligence Community (IC). The Director, NSA (DIRNSA), is tasked to host and serve as the IOTC’s Executive Agent (see Annex C, Reference 1.). DIRNSA delegated his IOTC authorities to the Director of the IOTC to execute the following responsibilities (see Annex C, Reference 5.):

1. (S/NF) Develop, in cooperation with Military Service and IC elements, computer network attack (CNA), computer network exploitation (CNE), and related techniques based on computer
technology vulnerabilities and compile and maintain those techniques as a toolbox from which customer organizations may draw;

2. (SH/NF) Conduct analysis of foreign information infrastructure systems for CNA technology development;

3. (SH/NF) Develop analytic modeling and simulation techniques to characterize vulnerabilities of information systems and the effectiveness of developed CNA techniques; and,

4. (U/FOUO) Provide threat analysis and/or techniques, as appropriate. The IOTC, in executing its responsibilities, also provides a community forum for sharing CNO technology; conducts analysis supporting technical gain/loss resolution; renders technical assistance in the development, review, coordination and deconfliction of CNO plans and operations; and provides other assistance as directed.

B. (U) Information Assurance (IA) is one of the two core missions of the United States Cryptologic System (USCS). IA encompasses the disciplines and activities needed to ensure the availability, integrity, authentication, confidentiality, and non-repudiation (i.e., the five IA pillars) of national security information and information systems. IA also includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. The DIRNSA is the National Manager for the Committee on National Security Systems (CNSS) and administers these responsibilities through the NSA Information Assurance Directorate (IAD). The IAD acts as the cryptologic enterprise manager providing IA advice and assistance regarding national security information and information systems to the U.S. Government departments and agencies; in addition, the IAD fulfills the DIRNSA's National Manager role for the CNSS. The IAD accomplishes its mission objectives through the provision of IA services, products and solutions, and by conducting Defensive Information Operations (DIO) to achieve IA for national security systems.

C. (SH/NF) The NSA/IAD and the IOTC will leverage their respective capabilities and knowledge to more efficiently and effectively execute their respective missions. As described in Annex A, selected tools and techniques developed within NSA/IAD will be provided to the IOTC for inclusion into the IOTC Toolbox. Likewise, the IOTC, in accordance with tool release instructions and equity evaluations, transfers identified tools to NSA/IAD from the IOTC Toolbox. The IOTC Toolbox that contains tools and related techniques in support of CNO has been documented and described in Annex C. (Reference 3). The IOTC relationships with customer organizations, the roles of participating organizations, and the functional elements and processes performed by the IOTC (see Annex C, Reference 4) are also documented.
D. (U/PF) In accordance with Annex C, Reference 6, the IOTC recognizes designated offices within the NSA/IAD as authorized recipients of IOTC Toolbox tools. Annex C, Reference 4, describes the procedures for authorized tool recipients to access and draw tools from the IOTC Toolbox.

III. (U) Responsibilities:

A. (U) The NSA/IAD will provide to the IOTC (through appropriate dissemination vehicles and within the terms of this MOU and applicable security guidelines):

1. (U/PF) Selected technologies related to CNO tools and techniques. NSA/IAD will ensure that the IOTC receives all available documentation for each provided tool and technique, within applicable security guidelines; and

2. (U/PF) Selected NSA/IAD designed, developed, and implemented CNO tools and techniques approved for release.

B. (U) The IOTC will provide to NSA/IAD (within the terms of this MOU and applicable security guidelines):

1. (U/PF) Selected technologies related to CNO tools and techniques as identified and requested by authorized entities within the NSA/IAD. IOTC will ensure that NSA/IAD receives information on all tools and techniques within the Toolbox and make available all documentation for each provided tool and technique, within applicable security guidelines;

2. (U/PF) CNO tools, techniques, and technologies, in accordance with the procedures outlined in Annex C, Reference 4, that could be converted for use in NSA/IAD operations; and,

3. (U/PF) Analysis supporting technical gain/loss and offensive/defensive equities of specified tools and techniques as related to NSA/IAD initiatives in the event of DOD or IC planning or employment of IOTC CNO tools and techniques.

IV. (U) Points of Contact:

A. (U/PF) The NSA/IAD Information Assurance Policy Branch (I411) Point of Contact may be reached on 969-7894s.

B. (U/PF) The IOTC Point of Contact is the Chief, Policy Division, 963-2179.
V. (U) Review/Termination:

A. (U) Any revision or extension to this MOU will be by mutual written consent of both parties, and published as an addendum to this MOU.

B. (U) This agreement shall be effective on signature of both parties and shall be reviewed annually. Either party to the other may terminate this MOU unilaterally on written notice.
(U) ANNEX A

(U//FOUO) PROVISION OF NSA/IAD COMPUTER NETWORK OPERATIONS TOOLS OR TECHNIQUES TO THE IOTC

PROVISION OF IOTC COMPUTER NETWORK OPERATIONS TOOLS OR TECHNIQUES TO NSA/IAD

(U//FOUO) The IOTC Toolbox contains Computer Network Operations (CNO) tools and techniques. This Annex describes procedures for the consignment or transfer of tools to the IOTC Toolbox.

I. (U//FOUO) NSA/IAD Computer Network Operations tools and techniques consigned into the IOTC Toolbox. IOTC and NSA/IAD responsibilities:

A. (U) The NSA/IAD will provide (through appropriate dissemination vehicles and within the terms of this MOU and applicable security guidelines):

1. (U//FOUO) Tools and techniques and existing supporting documentation to the IOTC, with no obligation to provide any additional documentation, development, or information support in the future, unless otherwise agreed upon.

2. (U) As much of the following, as available, on the transfer and consignment of tools and techniques:

   a. (U) Written security guidance on the handling, storage, and dissemination of consigned technologies and supporting information to the IOTC;

   b. (U//FOUO) Documented status information on tool readiness and maturity, status of testing, and an estimated time for transfer for NSA/IAD tools consigned to the IOTC but not physically resident;

   c. (U) Technical guidance for consigned technologies, based on use or testing, and in a manner consistent with operational and other security guidelines;

   d. (U) A maintained up-to-date list of knowledgeable points of contacts (POCs) for each technology consigned to the IOTC Toolbox; and
B. (U) The IOTC, as recipient, will (through appropriate dissemination vehicles and within the terms of this MOU and applicable security guidelines):

1. (U) Store, share, and discuss consigned technologies and supporting information, in accordance with written security guidelines and other document restrictions;

2. (U) Notify the NSA/IAD POCs ascribed to a consigned technology of any use of the technology, as required;

3. (U) Inform the NSA/IAD of any loss or compromise of consigned technologies that may jeopardize use of consigned technologies;

4. (U) Forward technical feedback for consigned technologies based on use or testing in a manner consistent with operational and other security guidelines;

5. (U) Coordinate, and if possible, deconflict the technologies covered in this agreement with other IOTC maintained or developed technologies;

6. (U) Document and maintain a record of all use of consigned technologies. Use for deconfliction with NSA/IAD as necessary;

7. (U) Broker technology requests, use, and support between NSA/IAD and authorized recipients, and facilitate tool request conflict notification (i.e., equity concerns), as required; and

8. (U) Accept the tools and existing supporting documentation, and negotiate on a per tool basis the feedback to be provided to the NSA/IAD concerning the tools, as a result of further development, testing, training, or use, or transfer to an authorized recipient.

II. (U) Transfer of IOTC Tools to NSA/IAD. IOTC and NSA/IAD Responsibilities.

A. (U) NSA/IAD will:

1. (U) Adhere to IOTC tool-specific security classification guidelines or conditions as provided in documentation;
2. (U) Be responsible for any NSA/IAD-unique development, evaluation, training, and maintenance of requested tools, and return developed tools to the IOTC Toolbox, unless specifically stated that the tool(s) will be retained.

3. (U) Provide timely, written feedback to the IOTC on any modifications made to a tool and feedback on the effectiveness of the tool based on use or testing.

4. (U) Provide timely notification to the IOTC in the event there is a change to the intended purpose of the use of a tool beyond stated purpose in initial request for tool transfer.

5. (U) Protect the tool from loss, compromise, or misuse and immediately notify IOTC in the event of loss, compromise, or misuse; and

6. (U) Ensure any operational use of the transferred tools is in accordance with NSA/IAD-established planning and approval processes, to include legal and policy reviews.

B. (U) The IOTC will:

1. (U) Provide timely, written notification to the NSA/IAD on any modifications made to a tool previously transferred to the NSA/IAD and the effectiveness of those modifications;

2. (U) Protect tool from loss, compromise, or misuse and immediately provide the NSA/IAD notification in the event of loss or compromise. Initial notification may be made via secure telephone. Full details should be provided via written correspondence 30 days from the time of incident;

3. (U) Ensure documentation accompanying the tool applies only to the version of the tool transferred. Any modifications or changes to the tool will require an update to the documentation and will be reviewed jointly for potential resubmission into the Toolbox;

4. (U) Provide equity notification to NSA/IAD in the event another authorized user requests an IOTC tool previously delivered to NSA/IAD and that is still in their possession at the time of request; and,

5. (U) Keep NSA/IAD informed on any changes in POCs for transferred tools.
(U) ANNEX B

(U) DEFINITIONS

1. (U) Authorized Recipient: A specific party or organization that has been formally designated by an authorizing official to receive a tool (i.e., complete tool information) from the IOTC Toolbox, usually for a particular purpose.

2. (U) Authorizing Official: Department of Defense (DoD) and Intelligence Community (IC) officials who have been delegated authority to designate “Authorized Recipients” within their organization.

3. (U) Computer Network Attack (CNA): Operations to manipulate, disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.


5. (U) Computer Network Exploitation (CNE): Intelligence collection and enabling operations to gather data from target or adversary automated information systems (AIS) and networks.

6. (U) Computer Network Operations (CNO): In consonance with DCID 7/3, this term encompasses and will be used to refer collectively to all of its components; viz., Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND).

7. (U) Consigned: The process of incorporating tools, techniques, and supporting information into the toolbox.

8. (U) Consignor: An organizational element that submits tools to be included in the IOTC Toolbox. An equities stakeholder.
9. **Equities**: Used in this document to describe the resource investment, organizational value, or other special interests that a consignor has at stake in a particular tool or technique. For intelligence organizations, this often includes protection of sensitive sources and methods employed to develop the tool or enable access for its use. Loss of an equity can result in loss of target access, critical intelligence collection, and/or future inability to re-use the tool or technique affected. For DoD organizations, this includes maintaining military capabilities and the effectiveness of military plans and operations. Loss of an equity can result in rendering a military capability ineffective or jeopardizing planned or ongoing military operations. Equities of consignors are protected through classification procedures, special security restrictions, and any special release instructions agreed upon and documented in a Memorandum of Agreement between the consignor and the IOTC before the tool is included in the Toolbox.

10. **Information Operations**: Actions taken to affect adversary information and information systems while defending one's own information and information systems.

11. **Technology**: For purposes of this document, information about a vulnerability, a technique, or a piece of hardware to be used against a certain interest or item.

12. **Tools and techniques**: For purposes of this document, "tools and techniques" are referred to simply as *tools*. This includes tools and techniques that underlie an operational capability. A tool may be hardware or software that is designed, developed, or modified for CNA or CNE. For the DoD, tools generally require weaponization prior to operational employment.

13. **Transfer**: The process involving the release, to an authorized recipient, of all pertinent tool software, hardware, techniques and/or technical information relating to a specific capability; sufficient to build upon or operationalize the tool for use.
(U) ANNEX C

(U) REFERENCES

1. (U/FOUO) MOA between DOD and the IC Regarding the Information Operations Technology Center, dated 4 March 1997.

2. (U) MOU between NSA and IOTC for Support of the IOTC, dated 25 Nov 97.


4. (U) IOTC Concept of Operations, dated 31 Dec 97 and Addendum to IOTC CONOPS, dated 1 Nov 01.

5. (U/FOUO) Delegation of Authority, from DIRNSA to Director IOTC, dated 7 Jul 97.


APPENDIX F. HAYDEN’S DIRECTOR’S MESSAGE “IOTC MISSION ACCOMPLISHED”

This appendix contains the full text of Michael V. Hayden’s declassified “IOTC Mission Accomplished” Director’s Message: DIRgram-345, posted September 28, 2004.
(U) Director's Message: DIRgram-345: "IOTC Mission Accomplished"

Distribution: ENTIRE ENTERPRISE

POC: Michael V. Hayden

SECRET/REL TO USA, AUS, CAN, GBR, NZL

Posted on: September 28, 2004 [time unknown]

(U) Director's Message: DIRgram-345: "IOTC Mission Accomplished"

Distribution: ENTIRE ENTERPRISE

POC: Michael V. Hayden

SECRET/REL To USA, AUS, CAN, GBR, NZL

Today, the Information Operations Technology Center (IOTC) closes, and its people, facilities, and technology development mission move to NSA. I want to provide you some background on this milestone event and discuss why recent policy changes make it a good move now.

The IOTC was established as a joint DoD/IC activity to develop computer network attack (CNA) techniques and maintain them in a toolbox from which customer organizations could draw. The Center opened at Fort Meade in August 1997, with DIRNSA serving as its Executive Agent. Over the past 7 years, the IOTC carried out key pioneering work in developing CNA requirements, distributing tools, and conducting the Nation's broadest and most sophisticated program of CNA technology development.

DoD's Unified Command Plan for 2002 clarified policy and organization for the DoD CNA mission. Under the new framework, the IOTC's requirements development efforts and tool management functions become STRATCOM responsibilities, to be carried out by the Network Attack Support Staff, located here at NSA. The Center's analysis and CNA technology development mission, closely related to NSA's computer network exploitation development effort, is being incorporated into an integrated effort within NSA.

Virtually all of the IOTC's analysts and technicians have been NSA experts on rotational assignment. However, the IOTC's formal separation from NSA divided a workforce with exceptional dual-use potential across two organizations, one dedicated exclusively to computer network exploitation (CNE) and the other to CNA. Bringing this workforce together will eliminate artificial boundaries and enable a larger cadre to contribute across the entire mission space. The IOTC and its mission are not going away. They're coming home.

MARTIAL V. HAYDEN

(U)-DIRgram-345: "IOTC Mission Accomplished" - Agency All Mass Mailers

Lieutenant General, USAF
Director

DRV FM: NSA/CSSM 123-2
Dated: 24 Feb 98
DECL ON: X1

DEVELOPED FROM: NSA/CSSM 1-52, DATED: 20130930, DECLASSIFY ON: 20380930
SECRET/SI/REL TO USA, AUS, CAN, GBR, NZ

https://cws.web.nsa.ic.gov/mass-mailers/view_msg.cfm?messageid=8884&mailerid=1
11/9/2015
BIBLIOGRAPHY


Black, William B., Jr., interview by the author, Pasadena, MD, May 1, 2015.


Chairman of the Joint Chiefs of Staff. “Memorandum of Policy (MOP) 185, Command, Control, and Communications Countermeasures.” December 20, 1983.


Crowe, William F. “Cybersecurity Kill Chain.” Presentation at the ISACA Jacksonville Chapter Meeting, August 13, 2015.


Department of Defense Former DoD Official, interview by the author, McLean, Virginia, October 2015.

Department of Defense Former DoD Official, email correspondence with the author, Washington, DC, December 2015.

Department of Defense Historian, interview by the author, Maryland, May 22, 2015.


Gosler, James R., interview by the author, Tysons Corner, Virginia, August 2015.


Hurst, Elizabeth A. *Shaping the Battlefield with Command and Control Warfare*. Ft. Leavenworth, Kansas: Army Command and General Staff College, 1996.


Inglis, James C. (Chris), interview by the author, Annapolis, Maryland, November 30, 2015.


Kollars, Nina A. “By the Seat of Their Pants: Military Technological Adaptation in War.” PhD diss., The Ohio State University, 2012.


Studeman, William O., interview by the author, Severna Park, MD, August 2015.


United States Congress, House Permanent Select Committee on Intelligence. “IC21: The Intelligence Community in the 21st Century: Clandestine Service Executive


BIOGRAPHY

Craig J. Wiener is a graduate of Peter Stuyvesant High School in New York City, and holds a dual degree in history and politics (American History and National Security Policy) with Latin honors from New York University. He received a Master of Science degree in Biodefense with a concentration in Homeland Security from the George Mason University Graduate School of Public and International Affairs. After finishing his Doctor of Philosophy in Biodefense at George Mason University in 2016, Dr. Wiener will continue on in his current position as Senior Technical Analyst for the United States Department of Energy in Washington, DC.

In 2015 and 2016, Mr. Wiener was named a Pat Roberts USG scholar as he finalized his dissertation. In 2014, he was named the Intelligence and National Security Alliance (INSA) Sidney D. Drell Academic Award winner for significant contributions to the national security community. Mr. Wiener was named a 2013 Nuclear Scholar by The Center for Strategic & International Studies (CSIS), an internationally renowned think tank based in Washington, DC.

During his doctoral candidacy, from 2012-2015, Mr. Wiener was a special advisor to the Director of the Air Force Research Lab – Rome NY Information Directorate for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), Information Exploitation and Operations, Computer Network Defense, technical countermeasures and other future state applications of Lab Core Technical Competencies.

In addition to his professional activities, for the last five years Mr. Wiener has worked as a Graduate Teaching Assistant and Lecturer for Security and Intelligence matters at George Mason University Graduate School of Public Policy for General Michael V. Hayden while he completed his doctoral dissertation. His duties include staffing the General, managing and advising 25-30 Master’s and Ph.D. students per semester. Mr. Wiener provides research supervision and writing guidance to students in areas of counterterrorism, counterproliferation, cybersecurity, international security, failed or failing states, intelligence collection methods, counterintelligence and foreign intelligence services. He has lectured on a variety of topics at the GMU Graduate School of Public and International Affairs, the GMU School of Law for the National Security Program, the Defense Intelligence Agency and Los Alamos National Laboratory.

Mr. Wiener has previously served as Principal Consultant (Senior Advisor) for Strategic Planning and Analysis for the National Nuclear Security Administration’s (NNSA) Deputy Administrator for Defense Programs, Office of Program Integration (NA-14), where he provided program implementation planning and efficacy analysis to execute the Nuclear Weapons Council’s 3+2 Strategy. Mr. Wiener also supported aspects
of the Office of Research Development Test and Evaluation’s (NA-11) Advanced Simulation and Computing (ASC) Program concerning disruptive technology, as well as Advanced Radiography and Sub-Critical Experiment technologies. Prior to this assignment, Mr. Wiener was an Executive Policy Advisor for the Office of the Associate Administrator/Chief, Defense Nuclear Security at NNSA. Mr. Wiener developed strategic and operational policies, procedures and guidance for significant or “hot topic” issues for DNS physical and cybersecurity responsibilities throughout the US Nuclear Security Enterprise. His experience in the previous decade includes positions as a Senior WMD and Biodefense Analyst and Critical Environments Division Manager/Consulting Design Engineer for private sector firms supporting advanced science and technology and national security endeavors.