Does It Matter How the U.S. Army Organizes To Deal with Cyber Threats?

A Monograph

by

MAJ Shane A. Roppoli
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2013-02

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
31-10-2013		February 2013 – December 2013

4. TITLE AND SUBTITLE
Does It Matter How the U.S. Army Organizes To Deal with Cyber Threats?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major Shane A. Roppoli (U.S. Army)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
School of Advanced Military Studies (SAMS)
250 Gibbon Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORGANIZATION REPORT

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
100 Stimson Avenue
Fort Leavenworth, KS 66027-1350

10. SPONSOR/MONITOR'S ACRONYM(S)
CGSC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A review of the open-source cyber security and organizational design literature suggests that the factors of complexity and rate of change combine to generate uncertainty within the cyber domain. This monograph examines four cyber attack case studies to identify and compare their environmental and contextual factors and to assess the relationship between uncertainty and organizational design. The cyber attack case studies demonstrate the importance of experts in enabling organizations to deal with ill-structured problems. They also suggest that no single organizational design is optimal for dealing with all threats in the cyber domain, because ill-structured problems require diverse expertise to identify and structure them. The hypothesis that complexity and rate of change increase uncertainty about cyber threats was confirmed. The findings suggest that future organizational designs must be able to gain access to experts to hedge against forecasted cyber threats.

15. SUBJECT TERMS
Cyber Threats, Organizational Design, Operational Art, National Security

16. SECURITY CLASSIFICATION OF: (U)			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Hank L. Arnold COL, U.S. Army
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	(U)		**19b. TELEPHONE NUMBER** *(include area code)*
(U)	(U)	(U)			913-758-3302

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MONOGRAPH APPROVAL

Name of Candidate: MAJ Shane A. Roppoli

Monograph Title: Does It Matter How the U.S. Army Organizes To Deal with Cyber Threats?

Approved by:

_____, Monograph Director
Michael D. Milhalka, Ph.D.

_____, Seminar Leader
Juan K. Ulloa, COL

_____, Director, School of Advanced Military Studies
Hank L. Arnold, COL

Accepted this 31st day of October 2013 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency.

ABSTRACT

DOES IT MATTER HOW THE U.S. ARMY ORGANIZES TO DEAL WITH CYBER THREATS? by MAJ Shane A. Roppoli, 42 pages.

A review of the open-source cyber security and organizational design literature suggests that the factors of complexity and rate of change combine to generate uncertainty within the cyber domain. This monograph examines four cyber attack case studies to identify and compare their environmental and contextual factors and to assess the relationship between uncertainty and organizational design. The cyber attack case studies demonstrate the importance of experts in enabling organizations to deal with ill-structured problems. They also suggest that no single organizational design is optimal for dealing with all threats in the cyber domain, because ill-structured problems require diverse expertise to identify and structure them. The hypothesis that complexity and rate of change increase uncertainty about cyber threats was confirmed. The findings suggest that future organizational designs must be able to gain access to experts to hedge against forecasted cyber threats.

TABLE OF CONTENTS

ACRONYMS

ARCYBER	Army Cyber Command
CBA	Capabilities-Based Assessment
CyberOps	Cyber Operations
CyberSA	Cyber Situational Awareness
CyberSpt	Cyber Support
DHS	Department of Homeland Security
DoD	Department of Defense
HSOC	Homeland Security Operations Center
SA	Situational Awareness
TRADOC	Training and Doctrine Command
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command

ILLUSTRATIONS

Page

TABLES

Page

"We are in the process of putting together our organization; we are working on an extensive strategy on cyber operations that will be released in the coming months, and it would include opportunities for the private sector."

U.S. Army Chief of Staff General Raymond Odierno[1]

INTRODUCTION

Policymakers and U.S. Army leaders share concerns that other nations and non-state actors expose U.S. cyber security vulnerabilities when they conduct cyber attacks. The growth of U.S. cyber security appropriations, within a fiscally constrained environment, demonstrates the high level of concern about cyber security.[2] In the 2014 defense budget, Congress committed $4.7 billion to cyber operations, up from $3.9 billion in 2013.[3] Given the directives of its most senior leader, the U.S. Army must consider how it can best organize to prepare for uncertain cyber threats while also informing policy so as to improve its ability to contribute to national cyber security efforts. This monograph applies organizational design theory to evaluate cyber attack case studies and identify the characteristics that enable organizations to efficiently and effectively gain, maintain, and exploit advantages in cyber space.

Does it matter how the U.S. Army organizes for cyber threats? To answer this question I first survey the current cyber security and organizational design literature to identify the environmental and contextual factors that influence organizational design. A review of the open-source cyber security and organizational design literature suggests that two factors—complexity and rate of change—combine to generate uncertainty within the cyber domain and therefore to influence organizational design. Further, the literature and empirical findings demonstrate the relationship between uncertainty, organizational design activity, and the number of ill-structured problems. Organizational design theory suggests that organizations derive their purpose from the

[1] Ellen Mitchell, "Odierno: Army Will Have Clearer Cyber Strategy in Coming Months," *Inside the Army*, May 24, 2013, http://insidedefense.com/index.php. (assessed 10 July 2013).

[2] Steven L. Hite, *Cyber Space: Time to Reassess, Reorganize, and Resource for Evolving Threats* (Carlisle, PA: Army War College, 2012).

[3] Ibid., 6-9.

problems that they intend to solve;[4] it also suggests that different organizational designs have different strengths and weaknesses with regard to their ability to exploit or mitigate the driving factor of uncertainty associated with the cyber domain. Further, organizational design research demonstrates that structured problems drive organizational design, whereas ill-structured problems[5] drive organizational design uncertainties.

Scholarly research demonstrates that both hierarchical (mechanistic) and heterarchical (organic) organizations are challenged by the pace of environmental change, which is why military theorists such as Bousquet,[6] Boyd,[7] and Clausewitz[8] assert that uncertainty requires adaptive systems to hedge against emerging contingencies. Research findings show that hierarchical and heterarchical structures efficiently and effectively solve structured problems, while ill-structured problems often require expert diversity, such as "skunk works"[9] organizational designs, to identify the structural problems and render solutions.[10] This would suggest that the idea that a single optimal organization can best mitigate risk is a fallacy.[11] The cyber domain creates a level of uncertainty that requires organizations to have access to expert diversity outside the selected organizational structure. Meanwhile, the U.S. Army continues to

[4] Mary Jo Hatch, *Organization Theory: Modern, Symbolic and Postmodern Perspectives* (New York: Oxford University Press, 2012).

[5] Herbert A. Simon, "The Structure of Ill-Structured Problems," *Artificial Intelligence* 4, no. 3 (1974): 181-201.

[6] Antoine J. Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, Vol. 1. New York: Columbia University Press, 2009.

[7] John R. Boyd, "Organic design for command and control," in Boyd, *A Discourse on Winning and Losing* (1987).

[8] Carl Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1974), 170-74.

[9] Michael L. Tushman and C. A. O'Reilly III, "Building Ambidextrous Organizations: Forming Your Own 'Skunk Works,' " *Health Forum Journal*, 42, no. 2 (1999), 20.

[10] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2010).

[11] Eric-Hans Kramer, *Organizing Doubt: Grounded Theory, Army Units and Dealing with Dynamic Complexity* (Copenhagen, Denmark: Copenhagen Business School Press DK, 2007).

deal with the uncertainty of the cyber domain by expanding its current cyber structure and forming new hierarchal cyber structures to respond to emerging problems.[12]

Thesis

There is no optimal way to organize to gain a competitive advantage against cyber threats. Cyber problems are both structured and ill-structured. Hierarchical structures best solve structured problems, while organic structures best provide access to the expert diversity needed to solve ill-structured cyber problems.

Research Question

The central research question of this monograph is stated in the title: does it matter how the U.S. Army organizes to deal with cyber threats? More specific questions guiding the analysis and application of the selected case studies are:

1. What potential relationships are exposed by comparing cyber attack types, organizational types, level of complexity, and rate of change?

2. Do complexity and rate of change generate the organizational competitive advantage that organizational design theory posits?

3. How did the different types of organizations respond to ill-structured cyber problems?

Scope of the Study

The monograph relies on open-source reporting regarding the four selected cyber attack case studies and regarding cyber security in general. The major research threads that support the logic of this monograph derive from organizational theory, design theory, and systems thinking. Hatch's organizational theory establishes a common organizational design understanding and frameworks to determine the effects of high and low rates of change and complexity on

[12] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin, 2006).

organizational designs. A two-by-two scenario-planning model is included to assess the interaction between levels of uncertainty and impacts on organizational design.

What Is Outside the Scope of This Study

To maintain the focus of the monograph, it is necessary to limit its scope. This study does not address in detail the relationship between organizational design and deterrence of cyber attacks, nor does it cover the relationship between the Department of Homeland Security and the Department of Defense with regard to private organizations or informal security agreements between the various organizations.

Organization of the Study

This monograph is organized into three sections. The first section, the literature review, examines prior research, theories, and frameworks supporting the theory presented in this study. The second section describes the theoretical and research approach employed in the study. The final section presents the analysis, followed by conclusions and recommendations for further study.

LITERATURE REVIEW

This literature review is organized into five parts. The first part provides an overview of the cyber domain. The second part reviews the cyber security literature to identify the general problems and threats in the area of cyber security. The third part draws on both cyber threat literature and organizational design literature to identify the possible driving factors behind the relationship between cyber threats and organizational design. The fourth part reviews the literature associated with how the U.S. Army organizes to deal with cyber threats. Finally, the last section of this chapter summarizes the literature review and establishes a common understanding regarding the methodology to be pursued in the monograph.

The Cyber Domain

The cyber domain is created by the interaction of connected nodes and the non-physical relationships generated by interactions. The U.S. Joint Forces Command document "Joint Operating Environment 2010" conceptualizes the cyber domain into three layers: the physical layer, the logical layer, and the social layer.[13] The physical layer consists of geographic and physical network components; the logical layer consists of the technical connections that create the network of nodes; and the social layer consists of the human and cognitive aspects of the cyber domain.[14] The layers of the cyber domain facilitate communications between the nodes and generate competition between organizations to solve both structured and ill-structured cyber problems.[15] The Army further conceptualizes the cyber domain into separate and overlapping cyber backbones (i.e., systems providing physical networks). The Army envisions the cyber domain as consisting of U.S. military networks, allied networks, global networks (which both

[13] U.S. Joint Forces Command, "Joint Operating Environment" (February 18, 2010): 63.

[14] The United States Army's Cyber Space Operations Concept Capability Plan: 2016-2028," TRADOC Pamphlet 525-7-8.

[15] Herbert A. Simon, "The Structure of Ill-Structured Problems," *Artificial Intelligence* 4, no. 3 (1974): 181-201.

U.S. military and allied networks partially leverage), and closed foreign networks that do not leverage global networks.

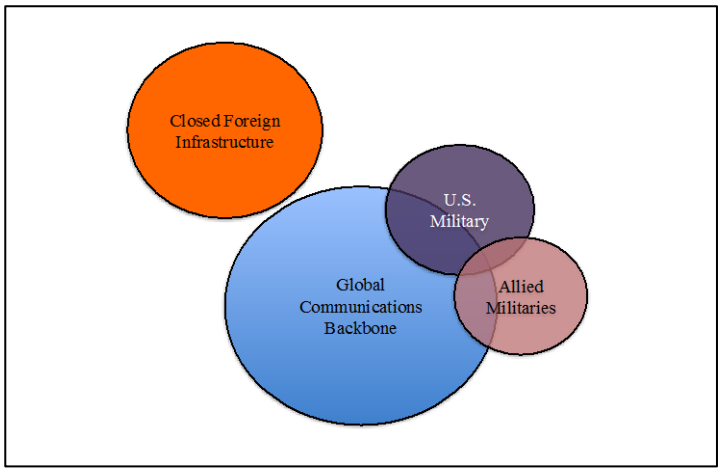

Figure 1: Cyber Domain Model

Source: TRADOC, Cyber Space Operations Concept Capability Plan. (2010), 11.

The General Problem of Cyber Security

The general problem of cyber security is the uncertainty generated by the cyber environment, which in turn impacts the problem-solving agent of organizational design.[16] A survey of the cyber security literature forecasts a rising amount of cyber attacks, which will correspond with a rise in the amount of cyber security requirements. Meanwhile, U.S. private industries are contributing fewer resources to their cyber security while also placing increasing expectations on the U.S. government to provide for a common cyber defense.[17] These trends will likely drive the U.S. Army toward organizational design efforts to ensure that it is prepared to satisfy both expeditionary and domestic cyber security requirements. Specifically, the cyber security literature and U.S. Army doctrine agree that the Army must be prepared to give cyber

[16] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What To Do about It* (New York: Harper Collins, 2010).

[17] Mark D. Young, "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power," *Journal of National Security Law and Policy* 4 (2010): 173.

security support to national organizations.[18] Cyber security uncertainty created the impetus that drove the Department of Defense (DoD) to form the U.S. Cyber Command (USCYBERCOM) and assign it the mission of gaining, maintaining, and exploiting advantages within the cyber domain.

Security experts, scholars, and practitioners disagree about the role of the military in providing cyber security. There are two primary schools of thought, one focused on cyber attack complexity and the other on organizational complexity. Those adhering to the first thread view cyber security as becoming so complex that access to experts are crucial.[19] Military theorist Antoine Bousquet argues in *The Scientific Way of War* that the evolution of technology generates corresponding organizational design innovations.[20] Further, Bousquet asserts that the military must operate as a complex adaptive system in order to achieve a position of relative advantage over competing complex systems.[21] For instance, the air domain emerged during World War I, creating a problem that the U.S. Army solved by developing the Army Air Corps. Scholars suggest that the cyber domain has evolved from an intangible competitive environment of information flows toward that of a tangible competitive environment where code can lead to physical destruction. The transition of cyber warfare from a virtual domain to the physical domain offers potential adversaries an opportunity to gain competitive advantages using cyber space. Therefore, organizing to deter adversaries and secure national cyber space interests within expected constraints requires an understanding of cyber security problem structures.

Cyber attacks have spurred U.S. government responses in the form of policy development and appropriations to create and support organizations tasked with providing national cyber security. John Healey of the Cyber Conflict Studies Association asserts that cyber conflicts are

---

[18] TRADOC, *Cyber Space Operations Concept Capability Plan*.

[19] Edmund H. Durfee, "Distributed Problem Solving and Planning," in *Multi-agent Systems and Applications* (Berlin: Springer, 2006), 118-49.

[20] Bousquet, *The Scientific Way of Warfare*, 25-30.

[21] Ibid., 54-60.

best understood as issues of international security, not information security.[22] Healey demonstrates the development of cyber security by discussing case histories of actual cyber attacks and the policy issues they generated. Healey refers to prior cyber incidents as "wakeup calls"[23] the lessons of which are at risk of being lost—and then rediscovered by the next group of policymakers when a catastrophic event forces them to deal with a similar security threat.

Richard Clarke, former Special Advisor to President George W. Bush on cyber security, suggests striking similarities between the struggles to determine the uses of nuclear weapons of the 1950s and those over the use of cyber war today.[24] Clarke argues that, in both cases, new weapons require experts and that there massive destructive potential has led to the formation of new military organizations.[25] The devastating potential and likely proliferation of cyber threats to proliferate will increase the uncertainty associated with the cyber domain while also increasing national cyber security requirements exponentially.

Numerous security scholars argue that incomplete security partnerships significantly hinder national cyber security efforts.[26] Joel Brenner and Mark Frazzetto argue in *America the Vulnerable"* that 9/11 exposed fundamental flaws within the U.S. intelligence community and that a "Cyber 9/11" threatens to expose a broader fundamental flaw between U.S. public and private responsibilities for national cyber security.[27] Although U.S. policymakers created laws to enforce public and private responsibilities for securing cyber space, critical security gaps remain. The authors explain these gaps using the "tragedy of the commons" theory, which asserts that users will continue to use common resources until they exhaust them versus paying the cost of

[22] Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association, 2013).
[23] Ibid., 45-50.
[24] Clarke and Knake, "Cyber War."
[25] Ibid., 35-39.
[26] Abraham M. Denmark et al., "Contested Commons" (2011).
[27] Joel Brenner and Mark Frazzetto, *America the Vulnerable* (New York: Penguin, 2011).

managing their use to prevent exhausting the resource; the tragedy stems from the preventable depletion of common resources.[28]

Other scholars offer other research that lends support to the argument that incomplete security partnerships hinder U.S. cyber security efforts. James P. Farwell, in "Industry's Vital Role in National Cyber Security," argues that U.S. cyber security legislation used privacy issues and incentives to spur the free market to develop its own cyber security requirements for industry, but made this a higher priority than enabling the DoD to collaborate with the private sector to improve national cyber security.[29] However, Farwell points out that only 25% of industries have given feedback to national cyber security agencies or participated in national cyber awareness activities.[30] He adds that industry requests for expertise to maintain effective cyber security grew by 55% over a two-year period.[31] Although the relationship between private industry cyber security and national cyber assets is a matter of policy, the U.S. Army must maintain its awareness about the factors that drive cyber problems, so that it can use organizational design to hedge its readiness to deal with emerging cyber problems.

Organizing to deal with cyber threats requires threat environment awareness to effectively generate the capabilities and policies necessary to synchronize national and international security efforts. Terrence Kelly and Jeffrey Hunker argue that the continuously transforming world requires the international community to establish cyber security agreements to deter and prevent the escalation of cyber warfare.[32] The authors argue that the distributed nature of cyber space and the globalized economy make cyber space just as valuable as the straits that create strategic geopolitical positions around the world; they predict that cyber attacks will

---

[28] Ibid., 26-31.

[29] James P. Farwell, "Industry's Vital Role in National Cyber Security," *Strategic Studies* 10 (2012), 10-41.

[30] Ibid., 15-17.

[31] Ibid., 26-29.

[32] Terrence K. Kelly and Jeffrey Hunker, "Cyber Policy: Institutional Struggle in a Transformed World." *Information Society Journal of Law and Policy* 8, (2012): 211-439.

terrorize and paralyze national economies in the future.[33] Meanwhile, scholars James Farwell and Rafal Rohozinski argue in "The New Reality of Cyber War" that republican governments cannot legislate cyber security policy as fast as cyber threats can shift their methods of attack.[34] Beside the physical mobilization required to attack waterways and airways, the cyber domain enables adversaries to conduct attacks while enjoying anonymity, adding additional uncertainty to cyber security design efforts.

The Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency[35] advocated a broad framework for cyber security. It also encouraged the collaboration and cooperation between the DoD and the Department of Homeland Security (DHS) to improve national cyber security. The Office of the President of the United States released its “Comprehensive National Cyber Security Initiative” to extend the federal government’s role in providing cyber security for critical infrastructure.[36] Surprisingly, a review of the National Security Strategy, the National Defense Strategy, and the National Military Strategy offers few objectives for U.S. military cyber forces. However, the DoD’s “Strategy for Operating in Cyber Space” provides guidance regarding building a pool of talented civilians and military personnel to enable the DoD to achieve its objectives in cyber space.[37] U.S. Strategic Command (USSTRATCOM) organized the U.S. Cyber Command and tasked it with the responsibility of organizing the DoD’s cyber capacity and developing ways to deal with cyber threats.

---

[33] Ibid., 250-52.

[34] James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* 54, no. 4 (2012), 107-20.

[35] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyber Space for the 44th Presidency* (Washington, D.C.: Center for Strategic and International Studies, 2008).

[36] Young, “National Cyber Doctrine,” 173.

[37] Gregory C. Wilshusen and David A. Powner, *Cyber Security: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats* (Washington, DC: Government Accountability Office, 2009), No. Gao-10-230t.

The General Structure of Cyber Threat Problems

The general structure of cyber threat problems seems to parallel general organizational problems. Mary Jo Hatch describes complexity by referring to the number and diversity of elements within the associated environment.[38] Her definition suggests that the rate of change refers to how rapidly associated elements change within the environment of an organization. Hatch describes environmental uncertainty as the interaction between varying amounts of complexity and change in the environment. Her model of organizational problems will be used to specifically examine the cyber problems presented later in this study. I will examine the literature on organizational design theory to identify the relationship between different organizational designs and problem structures.

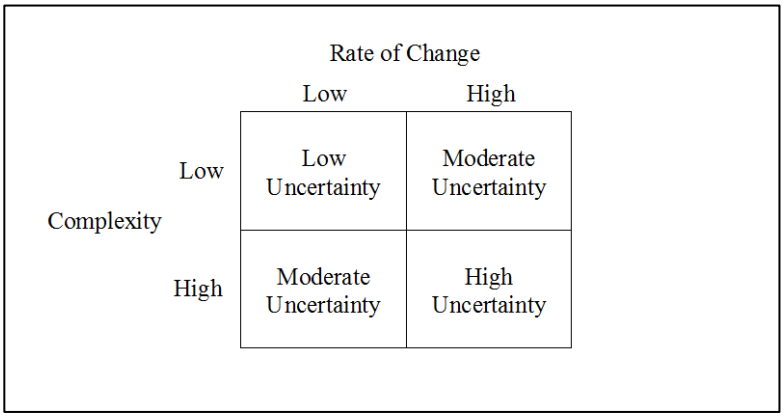

Figure 2: Organizational Design Environment

Source: Hatch, Organization Theory. (2012), 79.

Organizational design theory asserts that hierarchical (mechanistic) and heterarchical (organic) organizations bound the ends of organizational design options.[39] Hierarchical

[38] Mary Jo Hatch, *Organization Theory: Modern, Symbolic and Postmodern Perspectives* (New York: Oxford University Press, 2012).

[39] Ibid. Hierarchies are described in terms of command and control, top-down authority structure, centralized coordination, and vertical communication. Heterarchies are described in terms of a horizontal network; they are becoming an increasingly influential organizing principle of regional and global

organizations have mechanistic characteristics that focus on obtaining certainty in order to earn a competitive advantage through efficiency, while heterarchical organizations contain organic characteristics that enable their agility and competitive advantage within uncertain environments. Although numerous organizational design possibilities exist between these two extremes, organizational design theory proposes that organizations form in order to solve problems, and establishing certainty within the environment is one of the problems that organizations must consider when constructing their organizational structure. From a business perspective, Bar-Yam argues that hierarchies are designed to provide order and efficiency for large-scale operations but that, as environments become more complex, new organizational designs become competitively necessary.[40] Organizational design theory asserts that rapidly changing environments require organizations to innovate in order to survive.

Research findings demonstrate the importance of experts to organizations and their ability to anticipate and respond quickly to environmental change. Zaltman, Duncan, and Holbek determined that, in more certain environments, mechanistic organizations outperformed organic organizations because efficiency is favored in these environments.[41] Meanwhile, in less certain environments, organic organizations outperformed mechanistic organizations because speed and agility are more valued. The researchers concluded that organic organizational designs enable innovation and organizational change while mechanistic organizations enable resource conservation and stability. The presence of uncertainty thus influences organizational designs toward identifying sources of agility to hedge against uncertainty.

---

governance.

[40] Yaneer Bar-Yam, *Making Things Work: Solving Complex Problems in a Complex World* (Boston: Massachusetts Knowledge Press, 2004), 13-85.

[41] Gerald Zaltman, Robert Duncan, and Jonny Holbek, Innovations and Organizations (New York: Wiley, 1973).

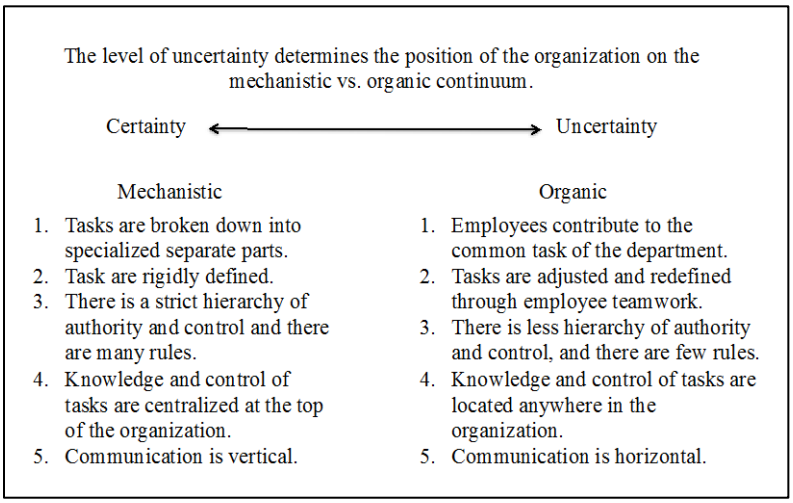

Figure 3: Organizations and Uncertainty

Source: Zaltman et al., Innovations and Organizations. (1973), 131.

Expanding upon the findings of Zaltman et al., social scientists developed a model to illustrate four types of goal-oriented organizations.[42] The mechanistic type is characterized by vertical coordination and high task specialization, and is recommended for organizations with narrow product lines and those that do not plan to diversify into complex forms of business.[43] The organic type is characterized by multitasking and lateral coordination and by the presence of facilitative leadership; it is recommended for startup organizations with innovative products or entities that are active in several venues.[44] The matrix type is characterized as project-oriented teams with members from several different divisions; this approach is recommended for stable organizations attempting to reinvent the way in which they operate and to discover new ideas and strategies.[45] Finally, the M-form type encompasses multiple agencies that organize by purpose,

[42] Jennifer L. Miller, "Conducting Business in a Fast-Paced World: The Importance of Change Management," *Student Pulse* 2, no. 10 (2010), 1-31.
[43] Ibid., 2.
[44] Ibid., 2-3.
[45] Ibid., 3.

and is recommended for organizations containing diverse groups or agencies that must cooperate to accomplish a broad purpose.[46]

Mechanistic Specialization	Organic Multitasking
Matrix Project teams	M-Form Type of Output

Figure 4: Organizational Types

Source: Miller, *Conducting Business in a Fast-Paced World*. (2010), 13.

How To Organize To Deal with Cyber Threats

The traditional strength of a mechanistic organization[47] is to leverage its hierarchical structure to generate mass and thereby gain a position of advantage over an adversary. While this strategy worked for the Army in the past, in the development of the Army Air Corps between WWI and WWII, there is no guarantee that this strategy will work in the increasingly complex cyber domain. Today the DoD is preparing to deal with cyber threats by employing its traditional approach of generating mass; however, the complexity associated with the cyber domain is driving the use of capabilities-based assessments to generate resources for uncertain cyber operations.[48]

Military institutions are often mechanistic and struggle to reorganize into adaptive systems that can match the complexity of the environment and their institution's information framework when dealing with uncertainty. Winton and Mets argue in *The Challenge of Change*

[46] Ibid., 3.

[47] Robert Axelrod and Michael D. Cohen, *Harnessing Complexity: Organizational Implications of a Scientific Frontier* (New York: Free Press, 2001).

[48] Wilshusen, Gregory, C. *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities*. No. GAO-11-75. Washington, D.C: Government Accounting Office, 2011.

that the U.S. Army historically changes only in the face of a dramatic event that requires the organization to recognize its position of disadvantage, and even then it often takes an act of Congress to force institutional change.[49] Further, strategy and organizational theorists Mintzberg[50] and Kahneman[51] offer insights into why organizations tend to avoid change in favor of process and routine. Their findings demonstrate that organizations resist change by continuously searching for more certainty, which explains why the Army continues to form hierarchical organizations in response to emergent problems.

Rapidly changing environments challenge mechanistic organizational structures. Brafman and Beckstrom argue that large organizations employ equilibrium approaches to gain the benefits of adaptive behavior.[52] Specifically, hierarchical organizational designs detect change requirements slowly, and therefore they would only slowly institute the necessary changes to compete effectively within the cyber domain.[53] To offset this deficiency a generation of doctrinal clarity has developed to enable commanders to plan and employ effective cyber operations within their assigned areas of responsibilities, especially because doctrine offers the Army the most economical way to gain, maintain, and exploit cyber advantages.[54] However, the Army must also be prepared to provide cyber security support to private networks, and therefore Army cyber organizations must be prepared to collaborate effectively with the DHS, adding another layer of

---

[49] Harold R.Winton and David R. Mets, eds., *The Challenge of Change: Military Institutions and New Realities, 1918-1941* (Lincoln: University of Nebraska Press, 2000).

[50] Henry Mintzberg, "The Structuring of Organizations: A Synthesis of the Research," *University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship* (1979).

[51] Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (1974): 1124-31.

[52] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin, 2006).

[53] C. Argyris and D. A. Schön, *Organizational learning II*. (Reading, MA: Addison-Wesley, 1996). These authors found that organizational structures encompass the relationships of authority and communication, both formal and informal, that exist with an organization, as well as the rules, procedures, routines, norms, and other practices that guide and constrain the behavior of organizational participants.

[54] U.S. Army, *Draft FM 3-38, Cyber Electromagnetic Operations* (Washington, DC: Department of the Army, 2013).

organizational complexity.[55] Organizational theory and empirical studies offer organizational design approaches to deal with rapidly changing environments and emerging requirements.

How the U.S. Army Organizes To Deal with Cyber Threats

Emergent theory asserts that organizations have to match change in ways that allow their organization to achieve a better degree of fit within its changing environment.[56] The Army's ability to adapt its organizational designs to the demands of tactical, operational, and strategic changes has grown during the last 10 years of counterinsurgency warfare.[57] Structured problems enable organizations to optimize resource allocation and training decisions to increase certainty, but ill-structured problems seem to do the opposite. Therefore, is not surprising that the Army is expending resources on organizing and training cyber force structures. However, to the extent that its structures are trained to deal with structured cyber problems whereas the problems that it is most likely to encounter are ill-structured, this discrepancy lends credence to the argument for the value of experts who can solve both types of problems.

Organizational theorists suggest that organizational design encourages the interaction of agents to generate solutions to problems. General Keith Alexander described the U.S. Cyber Command's initial organizing principles in "Building a New Command in Cyber Space"[58] as identifying problems and using capability-based assessments (CBA) to develop training regimes in order to rapidly develop the human resource dimension of the cyber organizational design. Following suit, the Army formed Army Cyber Command (ARCYBER); however, because of the uncertainty generated by the complexity and rate of change within the cyber domain, the Army is looking beyond just generating organizational structures to deal with cyber threats.

---

[55] Rita Tehan, "Cyber Security: Authoritative Reports and Resources" *Congressional Research Service* (2012).

[56] Steven Johnson, *Emergence: The Connected Lives of Ants, Brains, Cities, and Software* (New York: Scribner, 2012).

[57] Keith B. Alexander, "Building a New Command in Cyber Space," *Strategic Studies Quarterly* 10, no. 2 (2012), 3-12.

[58] Ibid., 4-5.

The U.S. Army Chief of Staff issued guidance directing the Army to develop organizational structures that can enable it to gain, maintain, and exploit competitive advantages within cyber space.[59] According to U.S. Army Training and Doctrine (TRADOC) Pamphlet 525-7-8, a significant advantage will go to the side that gains, protects, and exploits advantages in the contested and congested cyber space.[60] This pamphlet describes research focused on the development of U.S. Army cyber organizations and provides the U.S. Army with a cyber operational framework consisting of Cyber Situational Awareness (CyberSA), Cyber Operations (CyberOps), and Cyber Support (CyberSpt) components. The framework enables the Army to conceptualize the cyber environment and conduct a CBA to ensure that it is organized to satisfy the requirements of this environment. TRADOC Pamphlet 525-7-8 also identifies requirements for the Army to be prepared to partner with other national agencies in order to enable CyberSA and CyberOps; to satisfy these requirements ARCYBER needs the ability to solve both structured and ill-structured cyber problems.

The Army's institutional culture and organizational design remain challenged by the uncertain nature of the cyber domain and the ill-structured problems that it generates. For example, the Army recently solicited proposals from the technology industry to provide computer network operations in support of the 780th Military Intelligence Brigade, which suggests that the Army lacks the experts necessary to support its military mission.[61] Scholars and practitioners explain uncertainty as being the product of complexity and rate of change within the cyber domain, which challenge organizational designs with ill-structured problems.[62] Meanwhile, existing cyber attack trends suggest that the Army must develop organizational agility through

[59] Hite, *Cyber Space.*
[60] TRADOC, *Cyber Space Operations Concept Capability Plan*.
[61] Hite, *Cyber Space.*
[62] Bar-Yam, *Making Things Work.*

coordination and collaboration efforts with expert diversity similar to “skunk works”[63] team strategies.

Summary

It is widely recognized that the cyber domain is essential to U.S. interests.[64] However, the way in which the Army continues to develop organizations to deal with cyber threats seems to contradict the logic of both research and past historical precedent. The literature review demonstrates how levels of certainty and the presentation of ill-structured cyber problems guide organizational development efforts in this area. Army cyber concepts emphasize that effective cyber capabilities will enable the Army to seize the initiative and achieve a position of relative advantage in cyber space, a capacity that does not follow from the current cyber organizational development approach employed by the Army. The organizational design literature suggests that an organic or decentralized organization is in the best position to identify cyber security shortfalls and to collaborate with cyber capabilities to detect vulnerabilities. However, the literature further suggests that collective efforts between policymakers and military leaders are required to equip cyber organizations with the necessary agility to gain and maintain a position of relative advantage in the cyber domain.[65] Since cyber threats cannot be expected to come in a typical or predictable form, organizational designers should consider organizational designs that can handle uncertainty and ill-structured problems as well as well-structured problems.

The literature review also examined variables associated with developing cyber organizations and the impacts of the path dependencies that hierarchical organizations generate. While organizational theory offers explanations about how uncertainty influences organizational design, the literature suggests that different types of cyber attacks create different effects and

[63] Leland Nicolai, "Skunk Works Lessons Learned," in *AGARD Flight Vehicle Integration Panel symposium on Strategic Management of the Cost Problem of Future Weapon Systems* (1997).
[64] Hite, *Cyber Space*.
[65] Ibid.

drive different cyber security requirements.[66] The cyber domain offers opportunities to gain advantages over potential adversaries; however, since cyber organizations cannot be optimized for uncertain threats or anticipate ill-structured problems, cyber organizational design goals must focus on improving access to a diverse range of experts so as to enable agility**.** The Stuxnet cyber attack case and others offer an opportunity to evaluate the relationship among organizational design, uncertainty, problem structures, and access to experts to solve cyber problems.

[66] Kramer, *Organizing Doubt*.

METHODOLOGY

This monograph identifies the criteria that theory and past research efforts associate with organizational design and complex environments. It then uses organizational design models and definitions to conduct cross-case comparisons within the field of cyber security. As we have seen, two key variables, complexity and rate of change, generate different competitive advantages for organizational designs competing within the cyber domain.

This monograph examines four cyber attack case studies to identify the types of organizational designs competing within the cyber domain and to identify the environmental, social, political, and economic context of the attacks where available. This information will be used for the purpose of comparative analysis, using a common table of variables for each case study. The Gonzales model, adapted from the business management field, provides a method of categorizing organizational types.[67] To draw conclusions about the benefits and risks generated by the competing organizational structures and to offer relevant recommendations, the monograph employs scenario-planning techniques to highlight driving factors within the conclusions.

[67] Rafael A. Gonzalez, "Developing a Multi-agent System of a Crisis Response Organization," *Business Process Management Journal* 16, no. 5 (2010): 847-870.

ANALYSIS

Case Study Approach

This analysis chapter is composed of three sections. The first section defines the criteria to be evaluated for each case study. The second section presents each case study in three sub-sections; context, criteria, and outcomes. The final section offers criterion comparisons.

Assumptions

1. Environmental and other contextual factors influence how different organizational designs respond to uncertain cyber threats.

2. The case studies selected for this monograph are representative of the wider population of cyber attacks.

Criteria

It is useful to separate a problem statement into its constituent parts in order to identify the criteria that we are trying to understand. Understanding the problem of cyber security is dependent upon understanding organizational design and problem structures. The literature suggests that organizational design can enable competitive advantages within the cyber domain, but the type of organizational design that is desirable seems to depend upon the variables of complexity and rate of change. These two variables can be operationalized in the cyber context as follows:

1. Complexity (connectedness). Cyber organizations are complex systems. They consist of hundreds of nodes and links that can encourage collaboration and cooperation to improve organizational understanding.

2. Rate of Change (responsiveness). Cyber organizations that sense and respond effectively to contextual changes that require organizational change can gain or maintain a competitive advantage.

The four case studies selected involve different types of cyber attacks and permit examination of how different organizational designs respond to cyber threats. Each cyber attack case study identifies the contextual variables and ends with an assessment of the cyber attack and the interaction between the various organizational designs.

Case 1: Cyber Attack on Iran

This case study highlights a cyber attack that presented an ill-structured problem to a mechanistic type of organization that could not identify the problem, let alone solve it, until a group of socially networked experts did so. In June 2010 a computer virus attacked the Iranian Natanz Nuclear Enrichment Facility and infected tens of thousands of systems with computer malware.[68] The malicious code, called Stuxnet, took over the Iranian command system with the intent of controlling a nuclear centrifuge. Beyond just controlling the centrifuge, Stuxnet also deployed codes to direct hundreds of machines to self-destruct. Prior to Stuxnet, viruses, malware, and computer bugs had been designed to enable cyber attackers to extract and manipulate information, not to destroy computer functioning. The novelty of Stuxnet caught the attention of media and policymakers by demonstrating how the cyber domain could be used to direct a nuclear facility to self-destruct.

The first reports about Stuxnet appeared in media sources on 23 September 2010. Jonathan Fildes, a technology reporter for BBC News, reported that that "the Stuxnet worm had targeted a high-value Iranian asset … the cyber attack was one of the most sophisticated pieces of malware ever detected." Ralph Langer, an industrial computer expert with Siemens, the manufacturer of the control system targeted by the Stuxnet worm, reported, "With the forensics we now have it is evident and provable that Stuxnet is a directed sabotage attack that involves heavy insider knowledge." According to Fildes, Siemens representatives claimed that Siemens

[68] Irving Lachow. "Stuxnet Enigma: Implications for the Future of Cyber Security," *Geopolitical Journal of International Affairs* 11 (2010): 118-135.

was not involved in the construction of the Iranian nuclear power plant and that it had not delivered any software or control systems to the Russian construction firm that assisted the Iranian construction efforts. Reporters and technical and security experts' sustained interest in the Stuxnet cyber attack by sharing theories and findings on blogs, speculating on what factors had enabled the attackers to threaten the nuclear facility so successfully.

Researchers identified uncertainty as a contributing factor enabling the unidentified organization to infiltrate the Iranian cyber security enterprise. Meanwhile, a distributed network of cyber experts used social networks and blogs to collaborate and share research efforts, seeking to identify who was behind the Stuxnet worm and how the attack was carried out. The researchers found that "Stuxnet was developed primarily to target the industrial control systems or set of similar control systems."[69] Mikko Hypponen, a chief researcher at F-Secure, told Fildes that "Stuxnet used not one, not two, but four zero-day exploit codes; cybercriminals and everyday hackers would not have wasted the effort to build so many together."[70] Another expert agreed that there was a "huge effort, very well planned, very well funded, [using an] incredible amount of code to infect those machines."[71] Langer's assertion that Stuxnet could have been targeting the Bushehr nuclear plant drew considerable attention because of the implication that national actors could be responsible for the attack.[72] The narrative of Stuxnet continues to evolve, mostly due to its sophistication and because the event remains largely classified. However, the open-source version of the story provides enough information to show how the Stuxnet cyber attack demonstrates the vulnerability of critical infrastructure and the need for improved cyber security expertise and policy.

---

[69] Ibid., 120.

[70] Ibid., 122.

[71] Liam O'Murchu, "Stuxnet Using Three Additional Zero-Day Vulnerabilities," Symantec Security Response Blog, entry posted September 14, 2010.

[72] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (2011): 23-40.

First, the case demonstrates the scale of responsiveness by a mechanistic organization experiencing a cyber attack by another mechanistic organization. Iran's organizational responsiveness to the cyber attack was low; in fact, the mechanistic Iranian organization did not actually detect the attack. Once aware of the problem, this mechanistic organization behaved as organizational design theory suggested that it would, seeking to cooperate with experts in order to identify problem structures and find solutions. Interestingly, the case also demonstrates how the cyber domain enables organic organizations (like decentralized groups of bloggers) to leverage social networks and facilitate the collaboration of experts to solve ill-structured cyber problems.

In terms of complexity, the mechanistic organization under study (Iran) seems to have desired absolute centralization to ensure the security of its critical infrastructure. Meanwhile, the organic organization, made up of self-organized bloggers, seems to have balanced efficiency and effectiveness when it organized access to experts through the use of social networking strategies. However, while the mechanistic organization attempted to create both physical and electronic barriers to protect itself against a cyber intrusion, its efforts actually enabled the cyber attack because it did not fully appreciate the complexity of the environment and believed that it could isolate its networks and equipment. In contrast, the organic organization, i.e., the socially networked experts, embraced the complexity of the environment by using it to identify and offer solutions to the cyber problem.

Table 1: Cyber Attack on Iran Case Study Assessment

Attack Type	Context Assessment	Aggressor Organizational Type	Complexity Assessment	Rate of Change Assessment	Victim Organizational Type	Complexity Assessment	Rate of Change Assessment
Botnet	Nuclear materials production plant Iranian Nuclear capabilities contest Introduction of code to control equipment failure	Mechanistic organization	Low	Low	Mechanistic organization (Iran) M-Type Organization (Experts Blog)	Low (Iran) High (Experts Blog)	Low (Iran) High (Experts Blog)

Source: Created by author.

Case 2: Cyber Espionage

This case study highlights a cyber attack that presented itself initially as a structured problem to a matrix-type organization; however, in the course of its problem-solving efforts the organization realize that it had failed to identify, for years, an ill-structured problem in the form of cyber espionage. South Korea received this cyber attack, which it later assessed as cyber espionage. On 20 March 2013 a cyber attack caused significant damage to affected organizations across South Korea, resulting in the wiping of tens of thousands of computer hard drives. McAfee labs researched the event that became known as operation "Dark Seoul" and determined that the event was more than just cyber vandalism, but rather was part of an extended cyber espionage campaign.[73] Although McAfee could not identify the attacker with certainty, it suspected that two groups coordinating their efforts conducted the attack. However, since the two groups had no prior connection before the attack, McAfee suspected that the activities of these two groups were coordinated by a higher organization. Additionally, McAfee determined that the motive for the data wiping was to cover up the theft of data, which included vast amounts of personal and security information.[74]

The context surrounding this espionage campaign consisted of two major operations conducted by two or more groups that were supported by a larger centralized organization. The first phase began in 2009 when South Korea received distributed denial-of-service attacks and continued into 2010 and 2011, when South Korea experienced Trojan attacks focused on the financial industry. The first phase ended in 2012 when the South Korean media was attacked by the same code used to attack the financial industry. The second phase began when previously detected malware began to conceal itself and infiltrate specific South Korean targets. On 20 March 2013 two suspected groups utilized bots to exploit espionage malware with the intent of

[73] Newton Lee, "Cyber Warfare: Weapon of Mass Disruption," in *Counterterrorism and Cyber Security* (New York: Springer: 2013), 99-118.

[74] Ibid., 100-106.

crippling military networks. Importantly, these cyber attacks were conducted while tensions between North and South Korea were at a high point. The North Korean test of a ballistic missile in February 2013 had brought negative international reactions and threats of further sanctions and isolation. The Dark Seoul incident is believed to have been a long-term cyber hacking operation that transitioned into a cyber attack to collect intelligence from military networks and then destroy them so as to provide a cover for concurrent cyber espionage activities.

This case demonstrates the scale of responsiveness of a mechanistic organization experiencing a cyber attack conducted by an organic organization. It shows low responsiveness by the mechanistic South Korean organization in response to cyber espionage, suggesting that mechanistic organizations face serious challenges in actually detecting the cyber espionage. On the other hand, it shows that organic organizations backed by mechanistic organizations are able to effectively employ cyber espionage against other mechanistic organizations. Meanwhile, the mechanistic organization conducting cyber espionage seems to have balanced efficiency and effectiveness, given the complexity of the environment and the use of its experts to achieve organizational aims. This organization harnessed the complexity of the environment by resourcing an organic organization as a proxy to create cover for its overall operational objectives. While the mechanistic organization could detect cyber espionage but could not embrace opportunities in the cyber domain to prevent cyber espionage.

Table 2: Cyber Espionage Case Study Assessment

Attack Type	Context Assessment	Aggressor Organizational Type	Complexity Assessment	Rate of Change Assessment	Victim Organizational Type	Complexity Assessment	Rate of Change Assessment
Cyber Espionage	North and South Korea (USA) tensions high South Korean business and media services hacked and lose data	Organic organization serving as a virtual proxy for a Mechanistic organization	High	High	Matrix organization	High	Low

Source: Created by author.

Case 3: Cyber Hacking

In this case a cyber attack presented itself as a structured problem to a matrix organization that rapidly identified the problem and solved it, using its extensive access to networked experts and systems. The cyber hacking of Google reverberated across the global marketplace generating concerns among policymakers to identify and implement better cyber security mechanisms. In 2010, hackers using varying tactics that included encryption and stealth programming, using unknown holes in Internet Explorer, attacked Google and a dozen other large international corporations to obtain their source code. Later McAfee analysts described the hacking efforts as a "highly sophisticated and coordinated hack attack."[75] The hackers, using Internet protocol locations from China, used dozens of pieces of malware and several levels of encryption from individual hacking operations.

Google reported that its proprietary source code was the target of cyber attacks that originated from Mainland China. Google's vulnerability demonstrated to experts how the cyber attack was phased.[76] First the attackers conducted reconnaissance and surveillance prior to launching their attack. Then they focused on probing executives, who later described how accurate the personal information was when they received a phishing communication designed to scam the executive into providing access to personal contacts and other business networks. Security experts described China's hacking success in terms of its durability and tempo. The depth of the hacking, as assessed by the FBI, included numerous U.S. business sectors such as information technology, marine systems, aerospace, clean-energy technologies, advanced materials and manufacturing, healthcare, pharmaceuticals, agriculture, and business

[75] Stew Magnuson, "Stopping the Chinese Hacking Onslaught," *National Defense: Journal of the American Defense Preparedness Association* 97, no. 704 (2012): 26.

[76] James W. McGuffee and Nadine Hanebutte, "Google Hacking as a General Education Tool," *Journal of Computing Sciences in Colleges* 28, no. 4 (2013): 81-85.

information.[77] The major challenge associated with China's hacking exploits was that the targets did not detect the espionage exploits until after the information stolen was exploited by China.

China's extensive cyber hacking efforts and its organizational efforts to dynamically and persistently conduct espionage suggest that these efforts could only be possible with the support of centralized national resources. Meanwhile, as the Google attack indicates, the U.S. organizational approach of denying cyber hacking suggests that current diplomatic, information, military, and economic resources do not effectively deter centralized organizations from conducting cyber hacking on other centralized organizations. Cyber hacking and the individual efforts necessary to hack into an organization are enabled by the conditions of the low threat response environment; therefore amateurs can learn to eventually defeat a system without having to rely on a network of experts to accomplish their goal. According to the DHS, hackers are talented programmers who harm society by finding vulnerabilities in computer systems and attack them by creating and distributing virus-containing codes. According to the Homeland Security Operations Center (HSOC), the national agency responsible for sharing domestic incident management between federal, states, territorial, tribal, and private-sector partners with respect to cyber attack trends, more than 60% of cyber hacking goes unreported.[78] Because of this high rate of unreported attacks, hackers are emboldened to continuously attempt to subvert the defenses of networks.

This case demonstrates the scale of responsiveness of organic organizations experiencing a hacking cyber attack by another organic organization. The recipient organizations were able to detect and respond to the attack. However, the case suggests that an advantage can be gained by organic organizations employing cyber hacking in cyber space against another organic organization.

---

[77] Ibid., 83.

[78] Nataliya B. Sukhai, "Hacking and Cybercrime," in *Proceedings of the First Annual Conference on Information Security Curriculum Development* (2004), 128-32.

Meanwhile, the organic organizations conducting the cyber hacking seem to balance efficiency and effectiveness, given the complexity of the environment and the use of experts to achieve organizational aims. This organization harnessed the complexity of the environment to enable its operation. The organic organization that detected the cyber hacking, on the other hand, embraced the opportunities that the complex and interconnected environment provided, thereby enabling it to detect the cyber hacking.

Table 3: Hacking Case Study Assessment

Attack Type	Context Assessment	Aggressor Organizational Type	Complexity Assessment	Rate of Change Assessment	Victim Organizational Type	Complexity Assessment	Rate of Change Assessment
Hacking	Global information provider Large scale theft of business intelligence	M-Type organization	High	Low	Matrix organization	High	Low

Source: Created by author.

Case 4: Directed Denial-of-Service Cyber Attack

This case highlights a cyber attack that presented itself as a structured problem to an M-type organization that rapidly identified the problem and solved it by using its access to distributed experts. On 8 August 2013 Twitter was shut down for hours by what it described as an "ongoing" denial-of-service attack, which resulted in the silencing of millions of persons who would have normally sent messages during that time. Twitter claimed that it was the service's first major outage in months and the first one that it believed to truly be sabotage. The outage lasted approximately three hours and appeared to impact users worldwide. Twitter reported the initial denial of service as a "site down" message on blog sites. Twitter did not initially report that it was experiencing a denial-of-service attack and did not request outside assistance to counteract it. Approximately two hours after the attack began, Twitter posted on a blog that it was the target of a denial-of-service attack and called it a malicious effort orchestrated to disrupt and make

unavailable services that Twitter intended for customers and users. Further, Twitter reported that it was defending against the attack and would continue to update its status by blog as it defended against and investigated the matter. Approximately an hour latter Twitter was able to slowly reestablish its service. The international context was again important, as the outage took place during the height of the anti-government protests in Iran, and much of the blocked discussion would have originated from the hemisphere that serviced the Middle East and Europe.

This case demonstrated a high degree of responsiveness, as the organic organization was able to reestablish services only three hours after the directed denial-of-service cyber attack began. Twitter's organic organizational design was effective in response to what was most likely a structured problem, although even organic organizations struggle to actually prevent distributed denial-of-service attacks. Meanwhile, assuming that the aggressor was an organic organization that purposefully conducted the distributed denial-of-service attack, that organization seems to have managed to balance efficiency and effectiveness within the context of a complex environment and was able to use its experts to achieve its organizational aims, albeit briefly.

Table 4: Directed Denial-of-Service Case Study Assessment

Attack Type	Context Assessment	Aggressor Organizational Type	Complexity Assessment	Rate of Change Assessment	Victim Organizational Type	Complexity Assessment	Rate of Change Assessment
Directed Denial of Service	Global communications platform Time of attack daytime in Middle East, nighttime in N. America	Mechanistic organization	Low	Low	M-Type organization	High	High

Source: Created by author.

CONCLUSIONS AND RECOMMENDATIONS

This monograph has focused on how organizations deal with cyber threats. First it examined organizational theory and empirical studies to identify the driving factors associated with cyber threats. Then, by reviewing four cyber attack case studies, it sought to identify whether it matters how the U.S. Army organizes to deal the with driving factors behind cyber threats. Although the cyber domain is relatively new, the problem types generated by the cyber domain are not new; therefore, case studies can be used to identify insights about organizational design solutions. Organizational design theory suggests that organizations derive their purpose from the problems that they intend to solve.[79] Organizational design theory also suggests that different organizational designs create different strengths and weaknesses with regard to either exploiting or mitigating the driving factor of uncertainty associated with the cyber domain. Further, organizational design research demonstrates that structured problems drive organizational design, while ill-structured problems[80] drive organizational design uncertainties.[81] The goal of this monograph was to answer the primary research question: Does it matter how the U.S. Army organizes to deal with cyber threats?

Based on theory and past empirical research, it was hypothesized that complexity and rate of change would combine to increase the uncertainty associated with cyber attacks. The findings derived from cyber attack case studies suggest that having access to experts improves an organization's ability to deal with ill-structured cyber problems. Increasing complexity and rate of change seem to increase the uncertainty associated with cyber attacks; by maintaining access to a diverse range of experts, organizations can improve their ability to anticipate and mitigate even ill-structured cyber problems.

---

[79] Mary Jo Hatch, *Organization Theory: Modern, Symbolic and Postmodern Perspectives* (New York: Oxford University Press, 2012).

[80] Herbert A. Simon, "The Structure of Ill-Structured Problems," *Artificial Intelligence* 4, no. 3 (1974): 181-201.

[81] Hatch, *Organization Theory.*

Research Questions

1. What potential relationships are exposed by comparing cyber attack types, organizational types, level of complexity, and rate of change?

Potential relationships were identified by comparing cyber attack types to organizational types in four case studies while assessing the level of complexity and rates of change. The case studies suggested that mechanistic organizations are competitive in environments with lower complexity and a lower rate of change, while organic organizations are more competitive in those with higher complexity and a higher rate of change. They also demonstrate that organizational designs are more successful when they anticipate competitive factors. The findings appear to validate organizational design theory, which asserts that mechanistic organizations tend toward centralization of effort to gain the benefit of efficiency at the detriment of lowering its ability to sense the need to adapt. The cyber attack on Iran case study demonstrates how complexity and rate of change overwhelm mechanistic organizations and render them unable to sense organizational change requirements. More importantly, the case study demonstrated how vital experts are to enable mechanistic organizations to make sense of ill-structured problems in their environment.

2. Do complexity and rate of change generate the organizational competitive advantage that organizational design theory posits?

In the cases where competing organizational types were different, the competitive advantage offered by organic organizations followed theory, that organizational complexity and rate of change offer organic organizations advantages over mechanistic organizations. Meanwhile, mechanistic organizations also followed theory, in that lower organizational complexity and lower rate of change enabled these organizations' greater responsiveness and ability to rapidly reorganize to gain competitive advantages. The cyber attack on Twitter case study demonstrates how responsive an M-Type organization can be to a directed denial-of-service

cyber attack; Twitter had available experts prepared to solve this structured problem, and therefore it took Twitter just hours to repulse the cyber attack.

3. How did the different types of organizations respond to ill-structured cyber problems?

Mechanistic organizations within the case studies responded to structured cyber problems with forces that are manned, trained, and equipped to address the problem. Meanwhile, ill-structured problems challenged the mechanistic organizations just to identify the problem, let alone generate solutions to it. However, organic organizations responded to structured problems with the resources necessary to accomplish their goals, and they responded to ill-structured problems by leveraging their agility to identify and access the expert diversity needed. Interestingly, the cyber attack on Google demonstrated the effect of an M-Type organization attacking a matrix-type organization. The analysis suggests that M-type organizations are able to leverage experts and ideas more effectively than matrix-type organizations.

Case Study Findings

Table 5: Case Study Comparison

Attack Type	Context Assessment	Aggressor Organizational Type	Complexity Assessment	Rate of Change Assessment	Victim Organizational Type	Complexity Assessment	Rate of Change Assessment
Botnet	Nuclear materials production plant Iranian Nuclear capabilities contest Introduction of code to control equipment failure	Mechanistic organization	Low	Low	Mechanistic organization (Iran) M-Type Organization (Experts Blog)	Low (Iran) High (Experts Blog)	Low (Iran) High (Experts Blog)
Cyber Espionage	North and South Korea (USA) tensions high South Korean business and media services hacked and lose data	Organic organization serving as a virtual proxy for a Mechanistic organization	High	High	Matrix organization	High	Low
Hacking	Global information provider Large scale theft of business intelligence	M-Type organization	High	Low	Matrix organization	High	Low
Directed Denial of Service	Global communications platform Time of attack daytime in Middle East, nighttime in N. America	Mechanistic organization	Low	Low	M-Type organization	High	High

Source: Created by author.

Answering the Research Question

So does it matter how the U.S. Army organizes to with cyber threats? Yes, it does. Organizational theory, research findings, and case studies suggest that the Army should strive to gain and maintain access to M-Type organizations to enable it to solve ill-structured problems. Case studies demonstrate how expert diversity, such as in the "skunk works" teams,[82] enable

[82] Leland Nicolai, "Skunk Works Lessons Learned," in *AGARD Flight Vehicle Integration Panel symposium on Strategic Management of the Cost Problem of Future Weapon Systems* (Drammen, Norway,

mechanistic type organizations to overcome their lack of internal experts necessary to break down ill-structured problems. As there is no one optimal way to organize to deal with cyber threats, diversity and availability of experts seems to increase organizational ability to deal with cyber attacks that present themselves as ill-structured problems.

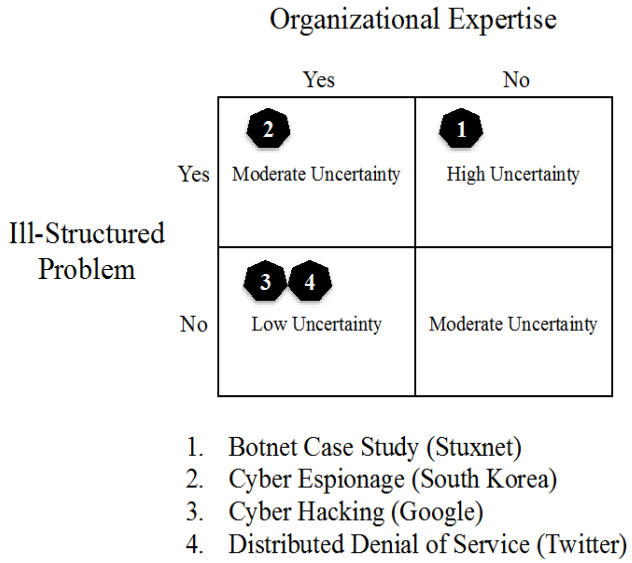

Figure 5: Case Study Analysis

Source: Created by author.

This monograph constitutes an exploratory study to analyze four case studies that represent high and low levels of complexity and high and low rates of change in the context of the cyber domain. It employs scenario planning to identify trends and analytical insights regarding past organizational performance within the cyber domain. The case studies suggest that relationships between organizations and experts enable solving of ill-structured problems. Although mechanistic organizations, such as the U.S. Army, already have well-developed systems to solve structured problems, ill-structured cyber problem are likely to drive future

---

1997), 22-25.

requirements. Therefore, as the Army continues to use organizational design to deal with emerging cyber threats, it must gain and maintain access to expert diversity so that it can deal with cyber attacks that present themselves as ill-structured problems. Meanwhile, complexity and rate of change are likely to continue to generate uncertainty in the cyber domain and degrade the Army's ability to adapt internally. Although the Army encourages individual and organizational initiative toward problem solving, ill-structured problems often require organizational resources and coordination beyond the capabilities of individual initiative.

Contributions and Implications

This monograph contributes to the understanding of how different types of organizational designs respond to different types of cyber attacks. The findings suggest that organizations that form to satisfy requirements in the cyber domain can benefit from a mechanism that enables them to sense and adapt to environmental change. This monograph demonstrates the implications of organizational design shortfalls. Further, the monograph demonstrates the implications of not coordinating national policies and not enforcing collaboration between the Army, DHS, and private corporations to unify cyber security efforts. As cyber threats continue to proliferate, cyber security requirements for military and civil agencies will continue to rise; therefore the Army must leverage and embrace cyber security partnerships.

Strengths and Weaknesses

The primary strength of this monograph is its reliance on theory, history, and models to underpin its thesis, methods, and analysis. An additional strength is the study's reliance on multiple disciplines to build conceptual frameworks to analyze the four separate case studies. The weakness of the monograph is the limited number of case studies examined to offer analysis of cyber attacks and how structured or ill-structured problems impact different organizational designs competing in the cyber domain.

Recommendations

Although this study contributes to our understanding of the relationship between organizational design and cyber attacks, however, large gaps remain. Further research could focus on regional cyber security policy implications as well as cultural implications, since the literature review and case studies suggest that different regions and different cultures seem to value cyber space differently. Research could perhaps identify what regions and cultures value cyber space as a national interest, thus indicating likely areas of future cyber domain competition. Not too long ago the U.S. Army organized to fight and gain dominance in the air domain; today the cyber domain offers the same opportunity, but further research is needed to demonstrate the necessity of moving beyond the strategy of simply generating forces.

While this monograph stressed the importance of experts, contracting as a solution generates a new range of problems that the Army must study and understand before creating organizational dependencies upon contractors as a source of expert diversity. This monograph suggests that how the U.S. Army organizes to deal with cyber threats does matter. Further, it demonstrates the importance of coordinating and collaborating to obtain expert diversity, which offers a way for the Army to gain the capability that it requires to deal with growing ill-structured cyber problems.

APPENDIX: DEFINITIONS

Cyber attack - A deliberate exploitation of computer systems, technology-dependent enterprises, and networks. Cyber attacks use malicious code to alter computer code or initiate self-destruct logic directed at systems or data, resulting in disruptive consequences that can compromise data or make possible cyber crimes such as information and identity theft.[83]

Cyber security - The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and the assets of users and organizations. Such assets may include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization's and users' assets against relevant security risks in cyber space.[84]

Cyber space: This term has become a conventional means to describe anything associated with the Internet and the diverse Internet culture. The U.S. government recognizes the interconnected information technology and the interdependent network of information technology infrastructures operating across this medium as part of the U.S. national critical infrastructure.[85]

Ill-structured problem – A situation in which the existing state and the desired state are unclear and, hence, methods of reaching the desired state cannot be found.[86]

---

[83] Wilshusen, Gregory, C. *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities*. (Washington, D.C: Government Accounting Office, 2011), No. Gao-11-75.

[84] Ibid., 4-7.

[85] Ibid., 8-9.

[86] Herbert A. Simon, "The Structure of Ill-Structured Problems," *Artificial Intelligence* 4, no. 3 (1974): 181-201.

BIBLIOGRAPHY

Alexander, Keith B. “Building a New Command in Cyber Space.” *Strategic Studies Quarterly* 5, no. 2 (2011): 3-12.

Argyris, Chris, and Schön, Donald A. *Organizational Learning: A Theory of Action Perspective.* New York: McGraw-Hill, 1976.

Axelrod, Robert, and Michael D. Cohen. *Harnessing Complexity: Organizational Implications of a Scientific Frontier*. New York: Free Press, 2001.

Bar-Yam, Yaneer. *Making Things Work: Solving Complex Problems in a Complex World.* Boston: Massachusetts Knowledge Press, 2004.

Bousquet, Antoine J. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. New York: Columbia University Press, 2009.

Boyd, John R., Col. USAF (Ret). *A Discourse on Winning and Losing.* Unpublished briefing slides archived at the Marine Corps University Research Archives, Quantico, VA, 1986.

Brafman, Ori, and Rod A. Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Free Press, 2006.

Brenner, Joel, and Mark Frazzetto. *America the Vulnerable*. New York: Penguin, 2011.

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What To Do about It.* New York: Harper Collins, 2010.

Clausewitz, Carl. *On War*. Princeton, NJ: Princeton University Press, 1989.

CSIS Commission. *Securing Cyber Space for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, 2008.

Dearth, D. H., and Williamson, C.A. “Information Age/Information War.” In A. D. Campen, D. H. Dearth, and R. Thomas Goodden (eds.), *Cyberwar: Security*, Strategy and Conflict in the Information Age. Fairfax, VA: AFCEA International Press, 1996.

Denmark, Abraham, & Mulvenon, James. (2010). *Contested Commons: The Future of American Power in a Multi-polar World*. Washington, DC: Center for a New American Security.

Durfee, Edmund H. "Distributed Problem Solving and Planning." *Multi-agent Systems and Applications* 2, no. 1 (2006): 118-49.

Farwell, James P. "Industry’s Vital Role in National Cyber Security." *Strategic Studies* 10, no. 4 (2012): 10-41.

Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival* 53, no. 1 (2011): 23-40.

Farwell, James P., and Rafal Rohozinski. "The New Reality of Cyber War." *Survival* 54, no. 4

(2012): 107-120.

Gonzalez, Rafael A. "Developing a Multi-agent System of a Crisis Response Organization." *Business Process Management Journal* 16, no. 5 (2010): 847-870.

Hatch, Mary Jo. *Organization Theory: Modern, Symbolic and Postmodern Perspectives*. New York: Oxford University Press, 2012.

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Washington, DC: Cyber Conflict Studies Association, 2013.

Hite, Steven L. *Cyber Space: Time to Reassess, Reorganize, and Resource for Evolving Threats*. Carlisle, PA: Army War College, 2012.

Hurwitz, Roger, Herbert Lin, Martin C. Libicki, and Panayotis A. Yannakogeorgos. "Depleted Trust in the Cyber Commons." *Strategic Studies* 21, no. 3 (2012): 20-45.

Johnson, Steven. *Emergence: The Connected Lives of Ants, Brains, Cities, and Software*. New York: Scribner, 2012.

Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Kelly, Terrence K., and Jeffrey Hunker. "Cyber Policy: Institutional Struggle in a Transformed World." *Information Society Journal of Law and Policy* 8, no. 2 (2012): 211-439.

Kramer, Eric-Hans. *Organizing Doubt: Grounded Theory, Army Units and Dealing with Dynamic Complexity*. Copenhagen: Copenhagen Business School Press, 2007.

Lachow, Irving. "The Stuxnet Enigma: Implications for the Future of Cyber Security." *Georgetown Journal of International Affairs* 11 (2010): 118.

Lee, Newton. "Cyber Warfare: Weapon of Mass Disruption." In *Counterterrorism and Cyber Security*, 99-118. New York: Springer, 2013.

Magnuson, Stew. "Stopping the Chinese Hacking Onslaught." *National Defense-Journal of the American Defense Preparedness Association* 97, no. 704 (2012): 26.

McGuffee, James W., and Nadine Hanebutte. "Google Hacking as a General Education Tool." *Journal of Computing Sciences in Colleges* 28, no. 4 (2013): 81-85.

Miller, Jennifer L. "Conducting Business in a Fast-Paced World: The Importance of Change Management." *Student Pulse* 2, no. 10 (2010): 1-31.

Mintzberg, Henry, and Joseph Lampel. “Reflecting on the Strategy Process.” *Sloan Management Review*, 40, no. 3 (1999), 21-30.

"Mission Command Center of Excellence, U.S. Army Combined Arms Center, Fort Leavenworth, Kansas, 7 January 2013." *Military Intelligence* (2013): 53.

Mitchell, Ellen. “Odierno: Army Will Have Clearer Cyber Strategy In Coming Months.” *Inside the Army*, May 24, 2013, http://insidedefense.com/index.php.

Nicolai, Leland. “Skunk Works Lessons Learned.” Paper presented at the AGARD Flight Vehicle Integration Panel symposium on “Strategic Management of the Cost Problem of Future Weapon Systems,” Drammen, Norway, 22-25 September 1997.

O’Murchu, Liam. “Stuxnet Using Three Additional Zero-Day Vulnerabilities.” Symantec Security Response Blog, entry posted September 14, 2010. http://www.symantec.com/en/aa/outbreak/?id=stuxnet (assessed 20 July 2013).

Simon, Herbert A. "The Structure of Ill-Structured Problems." *Artificial Intelligence* 4, no. 3 (1974): 181-201.

Sukhai, Nataliya B. “Hacking and Cybercrime.” In *Proceedings of the 1st Annual Conference on Information Security Curriculum Development* (InfoSecCD '04) (pp. 128-32). New York: ACM, 2004. http://doi.acm.org/10.1145/1059524.1059553 (assessed 10 August 2013).

Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2010.

Tehan, Rita. *Cybersecurity: Authoritative Reports and Resources*. Washington, DC: Congressional Research Service, 2012. www.fas.org/sgp/crs/misc/R42507 (assessed 18 September 2012).

TRADOC. *The United States Army's Cyber Space Operations Concept Capability Plan: 2016-2028*. Pamphlet 525-7-8.

Tushman, Michael L., and C. A. O'Reilly III. "Building Ambidextrous Organizations: Forming Your Own ‘Skunk Works.’ ” *Health Forum Journal* 42, no. 2, (1999), 20.

Tversky, Amos, and Daniel Kahneman. "Judgment under Uncertainty: Heuristics and Biases." *Science* 185, no. 4157 (1974): 1124-31.

U.S. Army. *Draft FM 3-38, Cyber Electromagnetic Operations*. Washington, DC: Department of the Army, 2013.

U.S. Joint Forces Command. *The Joint Operating Environment.* Norfolk, VA: Author, 2010.

Wilshusen, Gregory, C. *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities*. No. GAO-11-75. Washington, DC: Government Accounting Office, 2011.

Wilshusen, Gregory C., and David A. Powner. *Cyber Security: Continued Efforts Are Needed To Protect Information Systems from Evolving Threats*. No. GAO-10-230t. Washington, DC: Government Accountability Office, 2009.

Winton, Harold R., and David R. Mets, eds. *The Challenge of Change: Military Institutions and New Realities, 1918-1941*. Lincoln: University of Nebraska Press, 2000.

Young, Mark D. "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power." *Journal of National Security Law and Policy* 4 (2010): 173-196.

Zaltman, Gerald, Robert Duncan, and Jonny Holbek. *Innovations and Organizations*. New York: Wiley, 1973.