



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**INDUSTRY-INFORMED DOD CYBERSPACE CHANGE
STRATEGIES TO ANTICIPATE UNCERTAIN AND
UNPREDICTABLE FUTURE CHANGE**

by

Michael J. Millar

June 2020

Thesis Advisor:
Co-Advisor:

Wade L. Huntley
Victor R. Garza

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2020	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE INDUSTRY-INFORMED DOD CYBERSPACE CHANGE STRATEGIES TO ANTICIPATE UNCERTAIN AND UNPREDICTABLE FUTURE CHANGE			5. FUNDING NUMBERS	
6. AUTHOR(S) Michael J. Millar				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The Department of Defense (DOD), private sector industry, and academia nearly universally agree that change in cyberspace is constant. This cyberspace change may be anticipated, but important dynamics are unpredictable or uncertain. To manage, mitigate, or anticipate change, an organization must strategize to be responsive to changes it cannot precisely predict. The DOD does not have the breadth and depth of expertise needed to prepare for these changes and tends to be slow to address unpredictability and uncertainty in cyberspace change in its strategy. This thesis investigates whether the private sector has strategy lessons that can be adapted or adopted by the DOD to build better and more robust multi-stakeholder strategies to address unpredictable and uncertain cyberspace change. Publicly available industry strategies were analyzed from a range of large and small organizations. Comparison of DOD/government and industry strategies demonstrated a higher degree of specificity and inclusion of significant strategic elements within industry strategy, which can be used to inform DOD strategy. Recommendations include developing a new strategy of cyberspace systems integration and utilizing observed measures of success, milestones and timelines, and specificity in industry practices that can decrease ambiguity identified in DOD cyberspace strategy.				
14. SUBJECT TERMS cyberspace, strategy, industry, innovation, unpredictable change, uncertain change, multi-stakeholder			15. NUMBER OF PAGES 143	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**INDUSTRY-INFORMED DOD CYBERSPACE CHANGE STRATEGIES TO
ANTICIPATE UNCERTAIN AND UNPREDICTABLE FUTURE CHANGE**

Michael J. Millar
Lieutenant Commander, United States Navy
BS, University of Colorado, 2006
MA, Liberty University, 2018

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

**NAVAL POSTGRADUATE SCHOOL
June 2020**

Approved by: Wade L. Huntley
Advisor

Victor R. Garza
Co-Advisor

Thomas J. Housel
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Department of Defense (DOD), private sector industry, and academia nearly universally agree that change in cyberspace is constant. This cyberspace change may be anticipated, but important dynamics are unpredictable or uncertain. To manage, mitigate, or anticipate change, an organization must strategize to be responsive to changes it cannot precisely predict. The DOD does not have the breadth and depth of expertise needed to prepare for these changes and tends to be slow to address unpredictability and uncertainty in cyberspace change in its strategy.

This thesis investigates whether the private sector has strategy lessons that can be adapted or adopted by the DOD to build better and more robust multi-stakeholder strategies to address unpredictable and uncertain cyberspace change. Publicly available industry strategies were analyzed from a range of large and small organizations. Comparison of DOD/government and industry strategies demonstrated a higher degree of specificity and inclusion of significant strategic elements within industry strategy, which can be used to inform DOD strategy. Recommendations include developing a new strategy of cyberspace systems integration and utilizing observed measures of success, milestones and timelines, and specificity in industry practices that can decrease ambiguity identified in DOD cyberspace strategy.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	UNPREDICTABLE AND UNCERTAIN CYBERSPACE CHANGE STRATEGY (UCCS) CONTEXT AND DEFINITIONS	1
	1. Contextual Alignment to the DOD Imperative for Partnerships with Industry	2
	2. Anticipated, Unpredictable, and Uncertain Change in Cyberspace: Context of Moore’s Law and Other Innovations	3
	3. Anticipated, Unpredictable, and Uncertain Change Distinction.....	4
B.	DEVELOPING UCCS IS A WICKED PROBLEM.....	5
C.	HISTORICAL AND SITUATIONAL CONTEXT FOR THE DOD AND U.S. GOVERNMENT APPROACH TO CYBERSPACE	6
D.	THESIS ROADMAP	12
II.	LITERATURE REVIEW	15
A.	PRIVATE AND PUBLIC SECTOR SIMILARITIES AND DIFFERENCES IN CYBERSPACE.....	15
	1. Similar Use and Disparate Meaning in Agility Strategy	16
	2. Similarities in Partnership Strategy.....	18
	3. Key Difference: Legal Authority in Law of Armed Conflict (LOAC).....	19
B.	PRIVATE-TO-PUBLIC STRATEGY TRANSLATION AND ADAPTATION.....	20
	1. Rate of Change Impacts Competitive Advantage and Implementation	21
	2. Private and Public Sector—Impact of Differences in Leadership	22
	3. Specific Model Contribution to Thesis.....	23
C.	DISRUPTIVE INNOVATION THEORY	24
	1. Criticism of Disruptive Innovation Theory	27
	2. Incumbents vs. Entrants.....	28
D.	CHANGE MANAGEMENT (CM)	31
	1. Leadership	34
	2. Strategic Communication.....	35
	3. Agents of Change vs. Reactors to Change	36

E.	INTERSECTION OF RESEARCH	37
III.	METHODOLOGY	39
A.	FRAMEWORK DESCRIPTION	39
B.	SOURCE DATA.....	40
C.	QUANTITATIVE METHODOLOGY	42
D.	QUALITATIVE METHODOLOGY	47
E.	SUB-QUESTION ANALYSIS	48
IV.	BASELINE ANALYSIS OF CURRENT DOD/GOVERNMENT STRATEGY.....	49
A.	EXPLANATION OF QUANTITATIVE RESULTS.....	49
B.	EXPLANATION OF QUALITATIVE RESULTS.....	55
1.	Common Themes That Address UCCS	55
2.	National Defense Strategy 2018 (NDS)	59
3.	National Cyber Strategy 2018 (NCS)	61
4.	The DOD Cyber Strategy 2018.....	63
5.	USCYBERCOM Command Vision 2018.....	66
6.	Sub-question Analysis.....	68
V.	ANALYSIS OF INDUSTRY STRATEGY.....	79
A.	EXPLANATION OF QUANTITATIVE RESULTS.....	79
1.	Average Unpredictable Change.....	81
2.	Average Empty Elements	82
3.	Discussion of Ratio Comparisons	82
B.	EXPLANATION OF QUALITATIVE RESULTS.....	84
1.	Key UCCS Lesson Learned.....	85
2.	Other UCCS Lessons Learned.....	87
VI.	CONCLUSION ASSESSMENT, LIMITATIONS, AND RECOMMENDATIONS FOR FUTURE RESEARCH.....	95
A.	CONCLUSION ASSESSMENT	95
1.	Literature Contribution	95
2.	Industry Specificity Contribution	95
3.	Integration between Systems, Not Just Operations	96
4.	Agility and Speed with Automation	96
5.	Partnerships.....	97
6.	Strategic Communication.....	97
B.	LIMITATIONS: SUBJECTIVE AND OBJECTIVE DIFFERENCES IN ABSTRACTION OF STRATEGY	97

C.	RECOMMENDATIONS.....	98
1.	Future Research Comparing More Similar Strategy Types	98
2.	Use the Literature for Unified Models.....	99
3.	Develop an Integrated Cyberspace Systems Strategy	99
4.	Increased Specificity	99
5.	Iteration and Strategic Communications.....	99
	APPENDIX A. DATA SOURCES.....	101
	APPENDIX B. DATA SPREADSHEETS	105
	LIST OF REFERENCES.....	113
	INITIAL DISTRIBUTION LIST	123

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Disruptive Technologies Model. Source: Christensen (2002).....	26
Figure 2.	Accenture Analysis “Big Bang Disruption.” Source: Nunes and Downes (2019).....	29
Figure 3.	DOD/Government Strategy Combined Averages.....	52
Figure 4.	DOD Combined Ratios across All Four Documents	54
Figure 5.	Comparison of Industry and DOD/Governmental Strategy Combined Averages	79
Figure 6.	Comparison of Industry and DOD/Governmental Strategy Combined Ratios	83

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Number and Percentage of Strategies That Address Unpredictable Change for DOD/Government Strategic Documents	50
Table 2.	Average Number of Implementation Elements per Section for DOD/ Government Strategic Documents	52
Table 3.	Number and Percentage of Strategies That Address Unpredictable Change for Industry vs. DOD/Government Percentage	81

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CM	Change Management
COTS	Commercial-off-the-shelf
DCO	Defensive Cyberspace Operations
DCO-RA	Defensive Cyberspace Operations Response Actions
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DOD	Department of Defense
DoDIN	Department of Defense Information Networks
FAR	Federal Acquisitions Regulations
FBI	Federal Bureau of Investigation
IC	Intelligence community
IT	Information Technology
LOAC	Law of Armed Conflict
MOE	Measure of Effectiveness
MOS	Measure of Success
NCS	National Cyber Strategy
NDS	National Defense Strategy
NIST	National Institute of Standards and Technology
NSA	National Security Agency
POR	Program of Record
OCO	Offensive Cyberspace Operations
R&D	Research and development
SWOT	Strengths, weaknesses, opportunities, and threats
USCYBERCOM	United States Cyber Command
UUCCS	Unpredictable and Uncertain Cyberspace Change Strategy

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

A special appreciation is due to my advisors, Professor Wade Huntley and Victor Garza, who provided solid strategy, writing, and cyberspace expertise to guide this thesis process.

Another special appreciation is due to RDML William Chase, whose time and guidance helped develop the value that this thesis might be able to present to support the Navy's efforts.

The Graduate Writing Center and Thesis Processing Office of the Naval Postgraduate School also contributed many hours to ensure that this thesis followed proper writing conventions.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Department of Defense (DOD), private sector industry, and academia nearly universally agree that change in cyberspace is constant. This cyberspace change may be anticipated, but important dynamics are unpredictable or uncertain. Many advanced analyses speak to the interrelationships of change, economies, politics, and cyberspace, and the uncertainties these interrelationships create.

Unpredictability and uncertainty are distinct types of cyberspace change.¹ These dynamics make vulnerabilities to malicious hacking, cybercrime and state-sponsored cybertheft immediate risks to national security, critical infrastructure, and commerce. To manage, mitigate, or anticipate change, an organization must strategize to be responsive to changes it cannot precisely predict. The DOD is less well-suited than other types of organizations for this kind of strategic planning. It does not have all the breadth and depth of expertise it needs to prepare for unpredictable change and tends to be slower to address unpredictability and uncertainty in cyberspace change in its strategy.

Strategy to address this unpredictable and uncertain cyberspace change is an organizational challenge and similarly faced by private and public sector organizations. This thesis investigates whether the private sector has strategy lessons that can be adapted or adopted by the DOD to build better and more robust multi-stakeholder strategy to address unpredictable and uncertain cyberspace change. This first chapter begins that work by elaborating the problem of building effective strategy in the dynamically uncertain conditions of cyberspace.

A. UNPREDICTABLE AND UNCERTAIN CYBERSPACE CHANGE STRATEGY (UCCS) CONTEXT AND DEFINITIONS

The foundational question this thesis asks is, “What lessons can the DOD realize from private sector strategies for innovation and change to build better and more robust multi-stakeholder cyberspace change strategy that anticipates uncertainty and

¹ Unpredictable change and uncertain change in cyberspace are further defined in Chapter I.A.3.

unpredictable future cyberspace change?” In the absence of literature to answer this question directly, this thesis brings together several fields of related work and private sector experience on unpredictable and uncertain cyberspace change and strategy to collate lessons-learned and recommendations to the DOD.

In answering this core question, several sub-questions further clarify UUCCS lessons learned from the private sector: Which of those strategies are the most successful, and what measurements are used to determine that success? Which strategies might translate into the public sector? Which strategies might help the DOD become more efficient and effective and maintain a competitive edge in cyberspace? To answer these questions, the definition for cyberspace for this thesis is a broad umbrella concept that integrates many elements in the private and public sector: technological hardware, software, networking, infrastructure, data, acquisitions, policy and governance, as well as the people responsible for research and development (R&D), engineering, manufacture, supply, sales, maintenance, operations, integration, offense and defense, utilization and daily use of such technology. Changes to any of these elements affect the other elements, some in anticipated ways and others in unpredictable or uncertain ways.

1. Contextual Alignment to the DOD Imperative for Partnerships with Industry

The DOD and U.S. Government strategies researched for this thesis—The National Cyber Strategy 2018, DOD National Defense Strategy 2018, DOD Cyber Strategy 2018, USCYBERCOM Command Vision to Achieve and Maintain Cyberspace Superiority 2018 (White House, 2018; United States Department of Defense, 2018b; United States Department of Defense, 2018a; U.S. Cyber Command, 2018)—all have many imperatives to partner with the private sector. These imperatives acknowledge private sector cutting-edge approaches, vast experience, and scope of ownership of technology and methodology that the DOD may not currently utilize to the same extent. Understanding how private sector partnerships and capabilities contribute to the public sector maximizes potential to leverage those capabilities.² Acknowledging the private sector’s role means recognizing

² See Chapters I.C.a, II.A, and III.A.1.

that the DOD is not the sole provider of strategic leadership in defense or development of the nation's critical infrastructure or technology; private sector cyberspace security and technology organizations have been successfully strategizing and practicing innovation for decades to maintain their competitive edge and protect their assets. To leverage this experience and success is the very impetus for partnership.

This thesis aligns to the imperative for partnership at a fundamental level by analyzing and publishing the lessons learned and contribution of the private sector strategies as an academic-military and private sector partnership. The lessons-learned generated from these private sector strategies are recommended contributions to the multi-stakeholder model for sound, anticipatory strategy that sharpens the competitive edge desired by both industry and the DOD in their respective areas of responsibility, from which both sectors would benefit.

2. Anticipated, Unpredictable, and Uncertain Change in Cyberspace: Context of Moore's Law and Other Innovations

Moore's Law is one of many indicators of change in cyberspace and contextualizes the exponential rate-of-change in transistor capacity and its effects in cyberspace over time. Simply put, the more transistors on an integrated circuit board, the effect is more storage and processing capability for that chip (Strawn & Strawn, 2015; TOP500.org, 2019). Many other technologies are enabled by transistor capacity and change as a natural evolution so quick that measurement and quantification is difficult.

Cyberspace change is not limited to Moore's Law, and includes other innovations like quantum computing, parallel processing, microelectronics, and significant price-performance efficiencies. Some change can be anticipated, such as Moore's Law and the exponential growth rate of periodically doubling transistor capacity. Some change is more unpredictable and uncertain, such as a disruptive technology. This unpredictability can be in the introduction of a technology itself, or in second- or third- order effects, where a new technology enables subsequent technology to grow in capability and market share. A good example of unpredictability is the U.S. Government declassifying geolocation technology,

making it available for public use. Since then, many technologies use geolocation capabilities in ways that were unanticipated by the original designers of the system.

These types of unanticipated uses of technology have significant and swift impact on subsequent technologies and the businesses that produce and utilize them. In this sense, Moore's Law has become a broader metaphor representing the uncertainty and transformative potential, as well as the exponential speed, of cyberspace change.

3. Anticipated, Unpredictable, and Uncertain Change Distinction

Complexity in cyberspace and interactions between varied technological, user, cultural, and government factors introduce second- and third- order effects in cyberspace change that become harder to predict. The importance of such unpredictability traces at least to Clausewitz in the mid-1800s. In Clausewitz's foundational book *On War*, after his experience in the Napoleonic wars, he described a concept now referred to as "the fog of war," where factors out of control of the commander influence the outcome of a battle and cause friction and difficulties (Keller & Widger, 2019). It is this friction and these factors that contribute to and provide the foundation of the definitions of unpredictability and uncertainty for this thesis.

Demchak (2012) applies this concept to cyberspace and explains the differentiation between unpredictable and uncertain cyberspace change. Unpredictable change means the novel, rogue, or innovative friction that an organization does not comprehend, plan for, or accommodate in advance. Uncertain change entails unpredictability but can include anticipated behavior in form or frequency of an event, competitor, or adversary, where the when and how of the anticipated behavior is unknown. Thus, an organization might anticipate the change and could mitigate in advance through a competitive or technological posture, depending on the effort of the organization. Demchak's explanation of unpredictable and uncertain change is used as a definition for this thesis.

The distinctions between anticipated, unpredictable, and uncertain change have significant strategic implications. Anticipated change is much easier to identify and strategize for; it makes sense logically, can be measured easily, and has effects and nuances that can be comprehended by common sense. Unpredictable or uncertain change is

theoretically impossible to anticipate completely and causes difficulty for decision makers. Organizational planning in an environment of unpredictable or uncertain change requires careful consideration for UUCCS, including both defensive positioning and proactive posturing. Unpredictable or uncertain change can span the spectrum of situations from market competition to cybersecurity.³

B. DEVELOPING UUCCS IS A WICKED PROBLEM

Cyberspace is a complex system, meaning that due to the sheer scale of interactions of independent elements or agents, outcomes are often hard or impossible to predict by simply looking at the individual interactions (Emmott, 2006). The complexity of the unpredictability and uncertainty in cyberspace makes strategizing for organizational success a “wicked problem.” Explaining this concept, McMillan and Overall (2016) describe complexity as entailing disorder, uncertainty, volatility, unpredictable consequences, and disruptions. Poorly structured problems stem from complexity due to conflicts and value variability with multiple stakeholders and particularly from a constant requirement for change. McMillan and Overall question whether strategy makers are truly capable of properly aligning decisions to poorly structured problems. Because of these poorly structured problems, the strategist therefore has difficulty knowing where to direct the organization, and consequently cannot determine how to reach objectives, which is the wicked problem. McMillan and Overall conclude that solving wicked problem requires a mindset capable of managing multilayered and complex circumstances.

Explaining cyberspace change as a wicked problem, Demchak (2012) argues that because cyberspace technology is built on previous technology, it is not entirely unknowable. Instead, surprises occur due to the “complexity [of] misplaced trust, opaque ownership, and socio-political impunity” in cyberspace (p. 264). These surprises include a spectrum of layers, from basic and inherent vulnerabilities of manmade products to highly skilled, intentional malicious actors who attack with precision and must be disrupted before gaining access to an organization’s cyberspace infrastructure. Demchak argues that cyber

³ Further discussed in Chapter II.E.3.

resilience is the primary and most economic posture and response to most unpredictability and uncertainty, but only active disruption might address the most devastating malicious actors' efforts before they gain access to an organization's cyberspace capabilities.

Further complexity stems from the interaction of individual elements of cyberspace change (rate of change, individual technologies, stakeholders, designs and intents of good, neutral, and malicious actors, strategy). The relational complexity causes challenges in strategic direction, consensus, and implementation, and is therefore a wicked problem for both private and public sectors. This complexity is magnified in the U.S. Government and the DOD due to complex interactions between increasingly numerous and disparate stakeholders, requirements, duties, adversaries and competitors.⁴ Consequently, strategies, decisions, and implementation take tremendous effort, time, resources, consensus building, and the fundamentally complex mindset as proposed by McMillan and Overall to solve this wicked problem.

This thesis brings elements of strategies for complexity already learned and applied in the private sector to provide solutions to the DOD to address UCCS. The following section depicts the DOD challenges for which such solutions are needed.

C. HISTORICAL AND SITUATIONAL CONTEXT FOR THE DOD AND U.S. GOVERNMENT APPROACH TO CYBERSPACE

There is a broad history of the DOD's efforts to respond to change in cyberspace. While the government was an agent of change in cyberspace in its initial development (Defense Advanced Research Projects Agency, n.d.), in recent decades the private sector has led innovation and organizational approaches to cyberspace. Arquilla and Ronfeldt (1993) identify as early as Operation Desert Storm the unprepared nature of the government to operate in cyberspace, arguing for highly trained, focused, and flexible teams capable of blitzkrieg and phalanx level execution of operations. The implication is that these small teams would be capable of responding to change faster than a large, massed force, as the

⁴ Further discussion on the differences in public and private sectors in Chapters II.A, II.B.

DOD tends to fund. Such recommendations on cyberspace strategy echoed by numerous other writers have been slow to be added to the DOD's strategy.

Additionally, some of those ideas may have been implemented, but research and development and use of the cyberspace domain had been previously classified by the U.S. Government, and so strategy and partnerships are largely out of the public eye. As the potential for military competition in cyberspace emerged, the United States perceived the need to institute an independent command responsible for cyberspace security, first setting up a sequence of joint task forces for network defense, then creating U.S. Cyber Command (USCYBERCOM) as a branch of U.S. Strategic Command in 2010 nearly two decades after the issue was identified by Arquilla and Ronfeldt, and finally elevating USCYBERCOM to an independent combatant command in 2018 (U.S. Cyber Command, 2019). By this time, cyberspace expertise had already become highly technical and highly sought after, and industry was already hiring and maintaining talent that the DOD then had to compete for. As acknowledged in the current strategies, much of the technical expertise, cyberspace reach, and situational awareness is not held by the government, but by industry or the already established National Security Agency (NSA). The authorities to operate are separate for NSA and the DOD, which creates significant challenges when providing manpower to either group. It took five more years for the military to implement centralized cyber teams, for both defense and offense. Even more recently, for example, the Chief of Naval Operations, Admiral M. M. Gilday (2019), set strategy to increase small cyber teams as forces for fleet commanders. This is a quarter-century gap between academic proposal of Arquilla and Ronfeldt and the U.S. Navy—not even the broad DOD level—gaining enough momentum to implement their suggestions in the strategy.

In a historic authority change, President Obama tasked the Department of Homeland Security (DHS) with overall engagement of the private sector in cyber defense. The Federal Bureau of Investigation (FBI), DOD, and law enforcement also operate in cyberspace, with the blurred international cyberspace boundaries complicating delineation of authority. Roles, responsibilities, and authorities for each entity is differentiated by law,

but requires laborious coordination due to cyberspace’s infrastructure.⁵ President Obama also focused on critical infrastructure, which has become fundamentally dependent on cyberspace and particularly vulnerable to unpredictable cyberspace change (White House, 2016). The DOD has also begun to acknowledge the value of cyberspace, with the most recent National Defense Strategy (2018) finally adding cyberspace into its language as a key warfighting domain to master and achieve its mission; it had previously only been addressed as a generalized concept or in separate strategies, and therefore less likely to be included in strategies for other warfare domains. Declaring cyberspace a domain so important as to call it a warfare domain that requires investment of talent and resources also consequentially leads to increased attention, application, proliferation, and resources for cyberspace in other domains—a stronger adoption by the government.⁶

While these changes broadened the base of governmental cybersecurity responsibility, the percentage of critical infrastructure owned by the private sector is estimated to be 90% (Gilliland, 2019), making the government’s reach limited to indirect action through laws, regulations, and partnerships rather than direct action and protection. As mentioned before, these conditions are complicated and challenging—a wicked problem—and efforts to address them have been slow to gain momentum and react to change. A more dynamic and responsive DOD strategy will recognize that the private sector is not only a source of lessons for strategizing the uncertainty of cyberspace, but also an active element of the problem set.

a. Cybersecurity Linkages of Private Sector and Government

To operate in cyberspace and protect assets is costly to both the private and public sectors. In addition to cyberspace uncertainty in critical infrastructure, other issues with hacking, cybercrime, and state-sponsored theft highlight extreme cost to both sectors, which Norton (2018) estimates to be a \$172 billion loss globally in 2017. The costs to defend cyberspace then further increase to prevent such losses, as quoted by Clinton

⁵ Further discussed in Chapter I.C.a.

⁶ Further discussed in Chapter IV.B.2.

(2015), who references \$100 billion spent on cybersecurity alone in 2014. Cybersecurity measures do not necessarily factor into technology modernization or upgrade, which becomes a further cost of doing business. The numbers speak for themselves, where the inability to address the uncertainty of who, what, when, where and how in cyberspace strategy may cost organizations tremendously.

Like costs, many of the tools and practices in cyberspace are similar for government and industry. For cybersecurity, both government and industry are protecting assets; adversaries can be state, non-state, or criminal actors, making cyber-attack attribution and tactics and procedures important for recovery or best protection practices. The refresh, modernization, and replacement product life cycle requirements are similar in both sectors.⁷ Critical infrastructure, while owned and operated by various private and public entities, is a significant governmental concern beyond the owners' interests because the interconnected nature of cyberspace creates national security implications as vulnerabilities come into the spotlight. This interconnected nature increases the stakeholders for critical infrastructure, linking back to the wicked problem of cyberspace, while increasing the necessity for private and public sectors to contribute to strategy and partnership.

b. Cyberspace Strategy Is Different from Traditional Military Strategy

These unique conditions of cyberspace mean that the requirements for DOD strategy are not the same as traditional military strategy, which challenges the DOD to learn how to address cyberspace in its strategy. To distinguish between cyberspace strategy and traditional military strategy, Kallberg and Cook (2017) highlight the following differences: cyberspace lacks object permanence, measurements of effectiveness in offensive cyberspace actions are inadequate or missing, decisions made at computational or machine speed decreases influence of strategic leadership, and cyberspace provides expansive capability for anonymous action. Similarly, Gartzke (2012) brings out a significant distinction between cyberwar and other military uses of force. He argues that

⁷ Refer to this thesis' definition of cyberspace in Chapter I.A.

cyber-attack would not be a cyber-Pearl Harbor, due to a general inability to cause durable harm on an adversary. He notes that a primary cyber action requires a backup of other modes of conflict to become effective to cause desired durable harm. He concludes that the internet becomes an “adjunct domain” to the traditional warfare domains. The differences in strategy mean that the DOD must learn new lessons on how to write effective cyberspace strategy and can take the opportunity to learn from the experience and expertise of industry partners who are also intrinsic elements of the domain.

A particularly important unique condition of cyberspace is that the boundaries and infrastructure are not the same as geographic boundaries, which impacts the limitations of the government to act and operate. Aucsmith (2016), a cyberspace subject matter expert in both private and public sectors, scopes cyberspace as a global common, with boundaries defined by the communications infrastructure, rather than geographic lines. Every node in the infrastructure therefore could become a vector to communicate—or attack—anywhere else in the infrastructure due the design of built-in-connectivity. He argues that the U.S. Government is unable to be everywhere in cyberspace that requires protection, pointing to limitations in size, scope, complexity, technical capability, and legal authorities. This inability to protect all the dot-com domain, where most of the private sector operates, requires that the private sector protect itself, including investing resources, managing tools, and utilizing tactics to accomplish on their own. Self-protection naturally increases the scope of change, due to the numerous stakeholders acting within cyberspace, all competing for advantage and protecting assets. Due to the integrated nature of cyberspace discussed above, the ability of private actors to protect themselves is cumulatively (and sometimes individually) a major element of national security. Thus, if the U.S. Government is unable to protect the dot-com domain itself, its cyberspace strategy must aim to achieve that security through broader means.

Shortcomings of U.S. Government cyberspace strategy in recognizing these unique qualities of non-geographic terrain and dynamic uncertainty are crucial to the direction of research for this thesis. Some of these shortcomings have been recognized. The U.S. Government Accountability Office (GAO) (2013) presented recommendations that “integrated national [cyberspace] strategy be developed that includes milestones and

performance measures; costs and resources; and a clear definition of roles and responsibilities” (p. 2). These elements are recommended to increase the effectiveness of the implementation and accountability; without these, the strategy becomes a limited tool to address the nation’s issues in cyberspace (p. 23). In a later report, the GAO found a gap in monitoring progress in cyberspace strategy implementation—a lack in feedback systems (2017). These findings are similar in an independent CNA report on the U.S. Marine Corp overall strategies, which cited a trend in strategies to be unspecific in prioritization, resource implication and leadership direction (Deal, 2013, p. 23). In response, the Cybersecurity National Action Plan (2016) took an initial, major step to codify efforts to dedicate additional attention, roles, manpower, training, and resources to cyberspace.

Because the implementation of strategy is as important as its aspiration, these noted missing elements of measures of performance, milestones, costs, resources, and roles and responsibilities fundamentally inform the research for this thesis. The methodology provided in Chapter III adapts these specific elements to derive quantitative assessment of DOD and government cyberspace strategies, and for comparative evaluation of industry strategies to develop lessons learned. For the remainder of the thesis, measures of performance, measures of effectiveness and measures of success will all be grouped into the term “measures of success or measures of effectiveness” (MOS/MOE) for simplicity. Milestones will be referred to as “Timelines” to clarify and differentiate from the MOS, where other documents may use “milestone” to mean MOS.

This introduction to UCCS discusses cyberspace complexity to demonstrate a significant need for building a better and more robust strategy to address UCCS. However, the government’s slow-moving nature and the complex nature of cyberspace makes this need a challenging wicked problem. The purpose of this thesis is to investigate in what ways industry’s experience may help the DOD and to address UCCS, provided the government’s partnership is strong enough to take advantage of industry’s expertise.

D. THESIS ROADMAP

This thesis compares key U.S. government and DOD cyberspace strategies to industry cyberspace strategies, focusing on whether those strategies address unpredictable and uncertain cyberspace change. This chapter has scoped cyberspace change to differentiate between anticipated, unpredictable, and uncertain cyberspace change, its complex nature as a wicked problem, and relevant historical context and criticism that contributes to the U.S. government and DOD's approach to cyberspace.

Chapter II demonstrates UUCCS has not been specifically researched as scoped. Instead, several fields of research contribute to understanding UUCCS: private and public sector similarities in cyberspace, how private sector strategy can contribute to public sector strategy, disruptive innovation and change management. Bringing these four fields of research together contextualizes UUCCS but does not answer this thesis' research question. Chapter III outlines the methodology of this thesis using quantitative and qualitative analysis to evaluate key DOD and U.S. government strategies and a sampling of industry strategies.

Chapter IV undertakes a background and framework analysis of the key DOD/U.S. government cyberspace strategies. Applying the quantitative and qualitative methodology, this chapter provides a detailed evaluation of how effectively these cyberspace strategies specifically anticipate change and implement that anticipation. On this basis, the chapter also establishes the foundation for comparison to industry strategies. These foundations highlight strengths and weaknesses of the key strategies as they relate to UUCCS.

Chapter V compares the key DOD/U.S. government cyberspace strategies to the sampled private sector strategies and presents quantitative and qualitative findings. Key findings are that anticipation of unpredictable and uncertain change in DOD/U.S. government cyberspace strategies is surprisingly robust, but that private sector strategies, on average, include more strategic implementation elements than the DOD/U.S. government counterparts, such as measures of effectiveness, Feedback mechanisms, and Timelines. These findings inform this chapter's development of a number of lessons learned applicable to improving DOD/U.S. Government cyberspace strategies.

Chapter VI draws overall conclusions from these findings and offers recommendations to the DOD for strategy changes. This chapter also points to areas for future research, including using a disruptive innovation theory model for strategic decision making and comparing the U.S. Government classified strategies to proprietary strategies unavailable for this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

As discussed in Chapter I, the unpredictable and uncertain nature of cyberspace change is complex enough to be categorized as a wicked problem set. To draw lessons from private sector experience that can inform better DOD strategies to meet this wicked problem set, this thesis focuses on four core topics: private and public sector similarities and differences in cyberspace, private to public strategy translation, disruptive innovation theory, and change management. While the specific intersection of these four areas has little-to-no scholarly research, existing knowledge in each area contributes to understanding the entirety of the problem, and so cumulatively contribute to translating UUCS from the private sector to the DOD.

There are, of course, plenty of opinion editorials and papers by subject matter experts on the DOD's efforts, some of which is utilized here to supplement the fields of research. But the focus is on what general knowledge in each of these four areas can contribute to the specific challenge this thesis addresses. Moreover, the specific contribution available from each core area is dependent on the predecessor to scope and validate its contribution to the research for this thesis. Hence, this chapter reviews sequentially the existing knowledge in these areas: private and public sector similarities and differences in cyberspace, private to public strategy translation, disruptive innovation theory, and change management.

A. PRIVATE AND PUBLIC SECTOR SIMILARITIES AND DIFFERENCES IN CYBERSPACE

A baseline premise of this thesis is that public and private sector cyberspace is largely and fundamentally the same. Without this fundamental similarity, translation of strategies across sectors is a non-sequitur. But the environments obviously are not identical either. Hence, delineating both similarities and differences is important when considering any cyberspace interaction or cyberspace relationship between sectors.

Existing literature addresses obvious similarities by inference, and two key similarities and one difference more significantly. The obvious similarities in cyberspace

between the private and public sectors are largely inferred in the literature: public and private sector have networks that utilize hardware, software, must store data, have interactions with internal and external users, communications, decisions, measurements, and computations. Innovations and new technologies are constantly being introduced and significantly changing the domain in speed or capability. Personnel and expertise must be trained, technology must be acquired, maintained, and replaced for any product. Adversaries of any kind can attempt to exploit vulnerabilities to gain unauthorized accesses or information, and this requires adherence to a defensive posture to prevent such exploitation.

Beyond obvious similarities in private and public sector cyberspace, which contribute indirectly to UUCCS, there are two significant similarities and one major difference that are solid references for analysis in Chapter IV.

1. Similar Use and Disparate Meaning in Agility Strategy

Agility is a heavily used concept in both private and public sector strategies. Despite this usage in DOD strategy,⁸ agility does not exist in the DOD Dictionary as of January 2020 (Joint Chiefs of Staff, 2020). Without a good definition, usage and communication is vulnerable to variability in interpretation and communication, which is easily demonstrated in the literature. The consensus in agility strategy is that an organization must be able to adapt to change to create or maintain its competitive edge. Horney et al. (2014), Worley et al. (2016), and Mireles et al. (2019) are good samples of the literature and use similar terms that communicate speed and adaptability. Adaptations discussed include personnel, process, and technology alignments, usually in a cycle. This cycle, variate in its details, is essentially to anticipate change, plan, initiate action, evaluate results. This is conceptually like Change Management processes.⁹

Specific findings for each study provide further insights into agility strategy and how implementation is intimately connected. Horney et al. highlight creative and flexible

⁸ Analysis for DOD agility is in Chapter IV.B.1.f.

⁹ Further discussed in Chapter II.D.

processes that should enable rapid learning and unlearning. They emphasize unlearning unproductive processes, discovered through the Feedback and evaluation process, in order to achieve agility. The Feedback and evaluation are also designed to go beyond internal processes as a capability for the organization to respond to any changes and make fast decisions. Similarly, Worley et al. (2016) collate adaptability, resilience, leadership and change research to address agility, understood as “timely, effective and sustained changes that maintain superior performance” (p 77). A fundamental finding is the importance of matching a process cycle to the pace of environmental and industry change. They also note that some processes require flexibility, and others might require rigid sets of steps for appropriate management.

Mireles et al. (2019) apply agility more specifically to cyberspace. At the level of practical application of agility strategy, they present quantitative metrics to evaluate both attackers and defenders’ effectiveness and how they adapt over time, which reflects cyberspace agility. They scope agility within an enterprise system (e.g., a network) as the ability to deal with changes as measured over time and effectiveness of response. They note that usually this is done using well-defined and accepted static metrics, which take a snapshot in time, but propose to use dynamic metrics instead. The framework considers the evolution of both attack and defense behaviors. They use a suite of metrics from multiple perspectives that are combined to show weighted averages, including specific time-linked metrics for attacker and defender, triggering time, evolutionary effectiveness, lagging time, relative and aggregated generational impacts. Also, they note that if they are to fully measure cyberspace agility, metrics need to measure ability to respond to new or zero-day attacks.

While much of the agility application by Mireles et al. is similar in mindset to the general agility mindset of other authors, the literature demonstrates that the definition of agility is variable in different applications.

2. Similarities in Partnership Strategy

Partnership is a foundational and consistent DOD, governmental,¹⁰ and industry cyberspace strategy, as demonstrated in the literature. Gillentine (2010) presents efforts in the previous decade, beginning with 2010, named Cyber 1.0 in the Space Symposium, which collected experts from leading organizations to collaboratively address issues in cyberspace. She observes that top organizations understand that they need the government to address vulnerabilities in cyberspace and need the government to take the lead. They want to work with the government to make cyberspace more secure, but the government in turn needs to listen to the industry leaders and make appropriate changes. Nearly a decade later, Johnson (2019) observes that industry still recognizes a relative incapability to deal with foreign governments and sophisticated hacking groups and must lean on the governmental expertise, intelligence, and authorities to combat these gaps in capability and capacity.

While the need for partnership between the private and public sectors in cyberspace is clear, the meaning of partnership is not, and presents an opportunity for improvement in UUCCS. Specifically involved in government-to-industry partnerships, Clinton (2015) writes about a leading model in the formation of President Obama's "Cyber Space Policy Review." He notes that the concept of industry-government partnerships is ambiguous, and there is strain in the relationships. He pushes several best practices for operating these partnerships successfully, notably personal commitment from government and industry, transparency, broad stakeholder involvement, and utilized the National Infrastructure Protection Plan (NIPP), developed in 2006 as a foundation for further efforts. Simultaneously, he cites decreased trust and a lack of transparency and inclusiveness by the government, which erodes industry involvement. However, he concludes that the National Institute of Standards and Technology (NIST) framework, launched by President Obama himself, became a fantastic and foundational success story, and firmly brought together government and industry to build an extensive set of cyberspace standards.

¹⁰ Partnerships in the four DOD/government cyberspace strategies discussed in Chapter IV.B.1.d.

Establishing NIST standards was a foundational example where partnerships with government and industry worked well. Another good example is the Tallinn Manual series (2017), led by NATO Cooperative Cyber Defence Centre of Excellence. Supported by legal and information technology experts, the Tallinn Manual addresses state responsibilities in terms of cyberspace and whether use of force criteria and the Law of Armed Conflict apply to states' cyber operations. They analyze principles of general international law for jurisdiction, human rights law, air and space law, among others, determining that the more common cyber incidents observed by states on a day-to-day basis is not generally considered to be use of force or armed conflict. The reality is that each sector acts in the international arena, and the process of continual updated of these documents aims to promote strengthening international consensus on global norms and practices. Tallinn Manual outputs are thus important to later reference as a foundation setting and the process is an exemplar of successful work between the sectors.

The main limitation of the prior research in this area is that it does not provide direction or clarify the ambiguity for the strategy to “strengthen partnerships,” as described in the DOD cyber strategies. The literature instead highlights the need for, and difficulty in implementation of, the strategy, particularly for UUCS, largely due to its ambiguous nature.

3. Key Difference: Legal Authority in Law of Armed Conflict (LOAC)

There are many differences in the private and public sector in general, and cyberspace is no different. For this thesis, however, the key difference is a legal one: The DOD is the sole authorized entity to act on behalf of the United States under the Law of Armed Conflict (LOAC). As a legal concept, different actions in cyberspace are regularly debated between nation states as to whether they are categorized as acts of war, espionage, cybertheft, or use of force, to name a few issues. Hacking domestically is a form of fraud (Symantec Corporation, 2019), and unauthorized removal of information is characterized as theft (Computer Crime and Intellectual Property Section Criminal Division, 2015). State and federal laws limit the private sector so that, even if attacked, private actors cannot hack the attacker back, even to attempt to retrieve stolen property (National Conference of State

Legislatures, 2019; Maroney, 2017). Internationally, the private sector, and the rest of the non-DOD public sector, are not allowed to act on behalf of the U.S. nation using actions that could be considered a “use of force” outside the LOAC (First Research, 2017). Much of the discussion of cyber use of force and associated issues in cyberspace is discussed by the Tallinn Manual series (2017), but significant international consensus is regularly being addressed. The legal status differences between private and public sectors significantly change strategies that can be applied, where a private corporation would only have legal proceedings available to them, and the DOD might have LOAC authorization as a recourse for cyberspace issues rising to the level of national security concerns. These legal differences are a potential barrier to cross-sector strategy translation due to the clear authoritative boundary.

Other differences of private and public cyberspace are discussed in the next section, as they do not directly relate to cyberspace, but to government and industry operations and management in general. These differences certainly affect cyberspace indirectly but are highlighted better by strategy translation.

B. PRIVATE-TO-PUBLIC STRATEGY TRANSLATION AND ADAPTATION

One of the core investigations of this thesis is how effectively private sector strategy can be used or adapted in the public sector, specifically the DOD, though the literature does not address UUCSS directly. Variation between public and private sectors makes strategy research a significant academic interest that has been pursued for decades.

Perry and Rainey (1988), Van Der Wal et al. (2008), Alford and Greve (2017), Bryson and Roering (2007), discuss the similarities and differences between public and private organizations to assess the usefulness of the distinctions in organization theory. While a challenge, they agree that the private sector is the originator of many planning and strategic approaches that the public sector can benefit from. Perry and Rainey summarize private and public sector similarities in three dimensions: ownership, funding, and mode of social control. These dimensions exist in both sectors but are different in execution. Additionally, the sector similarities extend to function, such as supply, administration,

operations, etc., despite organizational differences. Key differences are that public sector is managed by processes, rules, directives issued by the government, and social and political exchanges are used to influence the government, stakeholders, and multi-organizational processes, but private sector agents behave with the common purpose to engage in competitive market exchanges for goods and services.

Consequentially, public sector strategy tends to have more intangible goals, less incentive for cost reduction, less information about and incentive from the economic market, and a complex internal bureaucracy as compared to private organizations. Additionally, public managers have less autonomy due to government authority restrictions and are subject to multiple external authorities. These studies indicate that market forces are not constraints but provide input and trends that lead the efforts of organizations. This input specifically is not as easily applicable in the public sector.

The following discussion examines specific ways in which differences and variations function to complexify the government's ability to address UUCS and translate strategy from private to public sectors.

1. Rate of Change Impacts Competitive Advantage and Implementation

While the consensus of analysts of strategy translation between sectors leans toward the view that such translation is possible, the rate of change in the conditions organizations face presents challenges to strategy translation, which are particularly pertinent to cyberspace. Due to the high rate of change in the marketplace, Leavy (2014) argues that sustainable competitive advantage in the private sector, as a fundamental concept, is no longer relevant, and now organizations must "learn how to exploit short-lived opportunities with speed and decisiveness" (p. 3). He dubbed these opportunities as transient advantages, which require more adaptation and more innovation. The general premise is that in competition, advantages come and go fluidly, and therefore organizations cannot depend on maintaining that advantage without adapting to the next transient advantage.

For UUCS, the concept of transient advantage is particularly applicable. When conditions are changing rapidly, the next innovation might make previous efforts to

maintain any advantage, competitive or transient, less effective.¹¹ Transient advantage strategies may change rapidly, and the time entailed in translating these strategies from private sector to public sector can leave the public sector constantly behind the changes in the evolving conditions.

To address the rapidity of change, Poister (2010) suggests that organizations should shift thinking from episodic strategic planning to a broader process of strategic management on an ongoing basis. He observes that implementation and management of those same strategies must be better addressed and iterated, rather than looking toward newer strategies in a changing environment. Additionally, he discusses how public sector agencies regularly engage in annual strategic planning, not cyberspace specific in this case, but also observes that the extent to which an agency meets its own plan is rarely meaningful. He references U.S. Government Accountability Office (GAO) reports from 2004 and 2005, citing inadequacy in creating outcome-oriented goals that connect long- and short-term efforts, inadequate stakeholder involvement, and identifying supporting resources. These same difficulties are still described in the 2013 GAO report,¹² which depicts the opportunity for improvement that this thesis builds on for UUCCS.

2. Private and Public Sector—Impact of Differences in Leadership

Private and public sectors tend to desire certain values of leadership, which impacts the organizational strategy. Van Der Wal et al. (2008) determine several common values desired within leadership, including accountability, expertise, reliability, efficiency, effectiveness. They also make a case that certain values can be anticipated to be more valued in higher managers in one sector than in the other. The highest valued attributes in leaders in the public sector are accountability, lawfulness, incorruptibility, expertise, reliability, effectiveness, impartiality, and effectiveness. For private sector managers, the highest valued attributes are profitability, accountability, reliability, effectiveness,

¹¹ More detailed discussion on innovation and the effects on technology and transient advantage in Chapter II.C.

¹² Discussed in Chapter I.C.b.

expertise, efficiency, honesty, and innovativeness. While attributes like accountability and efficiency are highly valued in both sectors, divergence in such values as incorruptibility and profitability, for example, create differing sector environments as a natural result of differences in the leadership provided.¹³ Strategy reflects these differences in sector environments and values of the leadership, which makes the translation of strategies between sectors more challenging.

With the variation in the sectors and differences in values of leadership, Alford and Greve (2017) describe each sector's focus to create organizational value. Key in their conclusions is that public managers generally do not find perfect or optimal solutions but must "work with other stakeholders ... in wider democratic processes to achieve forward momentum" (p. 13). Public managers should attempt to form and shape public value propositions, while engaging stakeholders and citizens. The public manager can create both private and public value, but the public value is consumed by citizens collectively in contrast to the individual focus of the private sector. This particular perspective supports the partnership strategy significantly because it involves stakeholders in building consensus to create the collective value desired, potentially more successfully than any single organization could achieve independently. So while the public sector value brings in multiple stakeholders for consensus, as is the goal in partnership strategy, the differences in the leadership and inherent sector value creation must be taken into account by leadership when translating or adapting strategy to that public sector challenge.

3. Specific Model Contribution to Thesis

With the general consensus that there are differences and challenges in translating or adapting private and public sector strategies, this thesis adapts previously developed models to translate UUCCS that appear most cognizant of those challenges. Bryson and Roering's (2007) model echoes many recommendations in the GAO report (United States Government Accountability Office, 2013),¹⁴ including clarification of roles and

¹³ Further discussion on leadership in Chapter II.D.1.

¹⁴ Previously discussed in Chapter I.C.b.

responsibilities, as well as basic strategy imperatives. The model's process includes defining and clarification for:

- consensus of support for successful plan formulation and implementation.
- organization's mission, values, and requirements validation.
- strengths, weaknesses, opportunities, and threats (SWOT) analysis.
- identification of strategic issues that will have long-term impact.
- identification of practical alternatives for resolving the strategic issues.
- the organization's end-state, with actions and decisions for implementation and Feedback for evaluation. (Bryson & Roering, 2007, pp. 11–12)

They use this framework to analyze six different private sector models for applicability and usefulness to the public sector and conclude that each model provides strengths and weaknesses inherent to the model itself. In the process of adoption or adaptation of any of the six models, they suggest that the public sector adjust the model to the specific situation. The adaptation per situation creates a modified or hybrid-type of strategy that uses appropriate and situation -specific elements to fit the organization. Based on this recommendation by Bryson and Roering, this thesis adapts their model's elements for the qualitative analysis of the sampled strategies, developing a hybrid model that reflects SWOT analysis.

The limitation of the strategy-translation literature is that there is no research directly contributing to adoption by the DOD of private sector UUCCS. The consensus is that the translation and adaptation of private sector strategy to public sector is possible, and so this thesis presents initial solutions to present recommendations and open the field to further research.

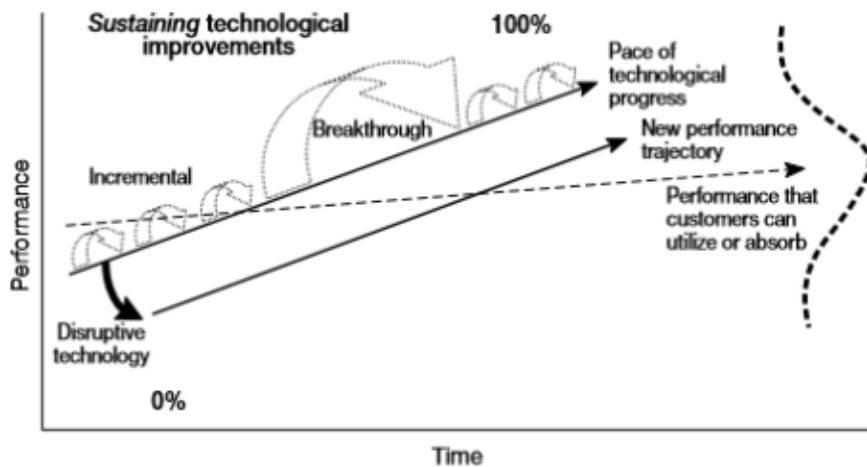
C. DISRUPTIVE INNOVATION THEORY

Disruptive innovation theory is a sphere of research addressing the nature of unpredictable and uncertain technology innovation which acts as a model for unpredictable change, regularly applied to technology, and for this thesis, cyberspace. This is a key model that the private sector uses when approaching change in cyberspace. While it takes time to develop a new technology, whether it makes other technologies obsolete determines its

unpredictability. Much of the literature agrees that organizations that are not attentive to disruptive technologies when they position themselves to utilize or adapt to changes have a higher probability to fail. The limitation for this thesis, however, is that the theory addresses the change itself, offering a model to think about how changes occur, but does not provide strategy directly. The literature is also exclusively for the private sector, and thus this thesis bridges the gap to the DOD, unlocking modelling of disruptive innovation as a tool that has previously not been utilized in the literature for DOD strategizing.

Disruptive innovation theory was introduced in 1996 by Christensen and Bower, which has spawned a tremendous amount of research and analysis, with articles numbering in the millions.¹⁵ Christensen's later work, partnering with several other writers (Christensen & Bower, 1998; Christensen, Suarez, & Utterback, 1998; Christensen, Hang, Chai, & Subramanian, 2010; Christensen, McDonald, Altman, & Palmer, 2018), has been wildly influential. The theory describes the effect of a disruptive innovative technology on a performance scale over time and how it compares to sustaining technological improvements. In Figure 1, the model shows two trajectories. The top one is based on current technology that continues to be developed through sustaining and incremental technological improvements. The bottom trajectory is the introduction of the disruptive innovation technology. These are bisected by the dotted line, which indicates that the level at which the technology is available to consumers is at that dotted line. As time progresses, both technologies improve, but once the disruptive innovation technology is mature enough to merit mass use, there is better performance by the disruptive innovation than the sustained technology. Innovations can get better performance than old technologies over time, ultimately replacing the old technologies through multiple factors, which might include decreased manufacturing costs, higher market shares, capability, or capacity with which older technologies eventually could not compete.

¹⁵ Much of the extensive literature on Disruptive Innovation Theory that is central to the field, on topics such as phasing, details, conflicts, caveats, and specific situations, does not directly address the focus of this thesis. Such works include Petrick and Martinelli (2012), Van Rensburg (2015), Walsh, Kirchhoff, and Newbert (2002), Yang, and Zhang (2013), Merali, Papadopoulos, and Nadkarni (2012), Aten and Thomas (2016), Zeng, Dong, Shi, and Li (2018).



Presented in a lecture at the 2001 Materials Research Society Fall Meeting

Figure 1. Disruptive Technologies Model. Source: Christensen (2002).

Many researchers have expanded on Christensen and Bower's work. Rogers (2003) contributes work used by both disruptive innovation theory and change management by creating foundational work on diffusion of products in a market with a core concept known as the adopter curve, originally published in 1962. He describes a normal bell curve and the sequence of market segments that adopt a product: innovators, early adopters, early majority, late majority, and laggards. This model is later used to show further application in the disruptive innovation curve, discussed below in Figure 2. Originally meant to describe consumers of the innovative products, Bry (2018) adapts the model to describe learning-fast and scaling-up methodologies to create competitive advantage among producers. Nunes and Downes (2019) show that innovators invest significant time and resources yet struggle to develop or apply new technologies. They argue that late adopters, however, may produce an equivalent product more cheaply after the product has been fully developed, decreasing the innovator's market share. Those late adopters benefit from the innovator's work and can imitate development or application of the product after inevitable issues have been solved, utilizing their own resources to produce and distribute the product.

Each addition demonstrates realities of unpredictability and uncertainty and suggest approaches that aid decision makers to lead their organizations through that change. As a key foundation for this thesis, such unpredictability may be in the form of technology

innovation, but also in processes and mentalities, which can follow the same patterns. It is a major concept whose application to government has not been given appropriate attention in the literature.

1. Criticism of Disruptive Innovation Theory

Critical literature shows that there is not a complete consensus on the theory, but also highlights that unpredictable and uncertain cyberspace change is a complex issue—a wicked problem—and so a single model may not be complete or address all situations equally. As an example of the debate in the field, King and Baatartogtokh (2015) report that “[t]he theory’s essential validity and generalizability have seldom been tested in academic literature” (p. 77), despite significant influence in industry. Furthermore, they call into question whether the cases used by Christensen’s research fit the conditions and predictions well. Finally, they conclude that a theory can provide a model, but is no substitute for thoughtful analysis.

Kane (2017) argues that the technology in and of itself is not the true key problem facing organizations. Rather, the problem for digital disruption is the “different rates at which people, organizations, and policy respond to technological advances” (para. 2). He references Deloitte’s 2017 Human Capital Trends study, concluding that “[t]echnology changes faster than individuals can adopt it, individuals adapt more quickly to that change than organizations can, and organizations adjust more quickly than legal and societal intuitions” (para. 2). This view reflects Rogers’ adoption curve, adapted to reflect communication application rather than product adoption. Kane’s work supports the overall disruptive innovation theory, while arguing that organizations should not be myopic in their focus of technology, and ensure the human factor be the primary focus.

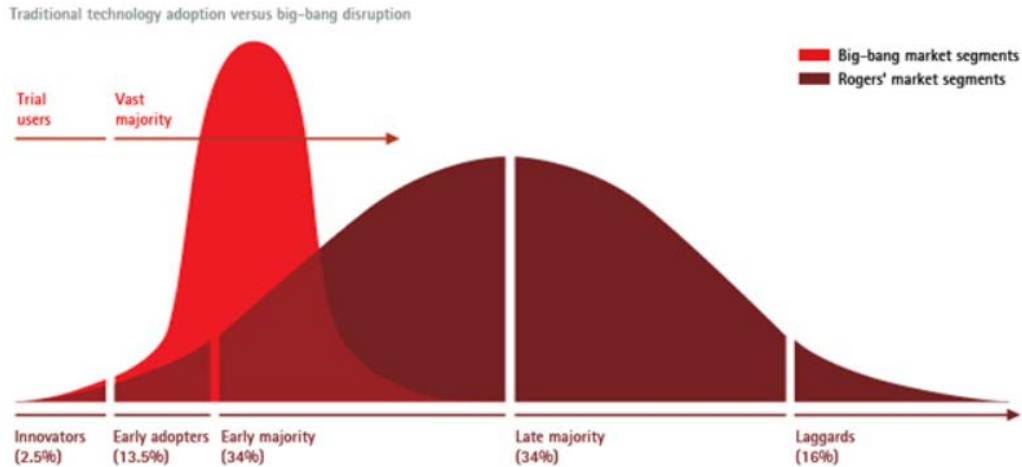
To prevent a sky-is-falling mentality, Sood and Tellis (2011) argue that the effects of disruptive innovation are generally exaggerated. Their study demonstrated that many disruptive technologies are not introduced in such a way as to cause industry disruption. Instead, only 16% of all technologies cause technology disruption. Additionally, 14% of all technologies cause firm disruption when the entrant innovation performs better than incumbent not in the primary dimension performance, but in a *secondary* dimension

performance. Their key findings are that potentially disruptive technologies “are not cheaper than established technologies,” “rarely disrupt firms,” and “are introduced as often by incumbents as by entrants” (p. 339). They do note that if a new technology can be produced at a low price, it increases the hazard of disruption, but this is generally not the case.

Key to this thesis, if the unpredictable change follows the same percentages observed by Sood and Tellis, then risk to the incumbent, specifically the DOD and governmental cyberspace, is not absolute, and the risk can be managed without expectation of overnight, total fundamental change to the entire organization.

2. Incumbents vs. Entrants

A significant vein of disruptive innovation thinking within the private sector more specifically applies the theory to two different types of organizations: incumbents and entrants. Numerous works compare the disruptive innovation adoption curve used by the disruptive organization vs. the established enterprise. Nunes and Downes (2019) summarize a higher-level analysis on how easy it is for an innovator to enter a market segment, vs. the methodologies of decision-making used by an incumbent, creating significant advantage to the innovator, calling it a “Big-Bang.” This effect describes the compact nature of disruptive innovation market segments as compared to the normal market segments proposed by Rogers. Figure 2 shows the Big Bang model, with the adoption curve as the normal bell curve shape, as proposed by Rogers. The Big-Bang market segments compressed in time show how much faster an innovation may be introduced.



Accenture Analysis “Big Bang Disruption” published in 2013, referenced by Nunes and Downes (2019).

Figure 2. Accenture Analysis “Big Bang Disruption.” Source: Nunes and Downes (2019).

Nunes and Downes also offer the alternative that incumbents have some advantages over entrants, specifically in established knowledge and experience. However, the incumbent must rapidly respond to asset relevancy and changing value due to the innovator’s introduction of new technology.

The adoption curve offers a model to determine the pace that the government and DOD adopt new technologies. This is a potential solution to a foundational challenge that this thesis seeks to address—how the government might deal with new innovations based on its placement in the curve and its ability to apply resources.¹⁶

Woahika (2018) discusses the same big-bang phases as Nunes and Downes and adds detail to the concept, calling into question the smoothness of a curve in case of roadblocks to the diffusion of the technology. His observation is that there would be multiple small curves in the early phases of development, as trial users work out flaws. After this point the diffusion of the technology to everyone else causes the large big-bang curve. While Woahika demonstrates variation in a curve, Lee et al. (2013) discuss the different effects over time for early and late adopters according to the theory’s model. They

¹⁶ Analyzed in Chapter IV.B.6.b.

highlight that the innovation effect is more pronounced within the innovator and opinion leader adopters, but the effect diminishes over time. Alternatively, the imitation effect is more pronounced within the early majority, late majority, and laggard adopters (p. 772). They demonstrate that the information and communication technology industries these effect patterns are especially impactful. They surmise that the product life cycle of a product shortens due to the capacity of other organizations to imitate the initial product.

This is important in terms of DOD cyberspace competition. Initial stages of malicious innovations by an adversary might be observed by the U.S. Government and monitored for changes. The goal would be to either delay proliferation, or posture to adopt responsive technology in the majority that reflects the operational need. This may be earlier for competitive edge, or later for cheaper and faster adoption throughout the organization.

Murphy (2011) uses Christensen's model to point out that part of the dividing line between an innovator and the incumbent is the performance that a customer can use. If performance in a technology is not optimal, then a disruptive innovation allows for new competitors to gain market share more effectively by introducing their technologies to close the performance gap. However, if product improvement and sustaining innovations increase performance of the incumbent technology, over time the incumbent is the more capable of the two competitors, until such a time that the disruptive technology's performance is cheaper and more effective. For UCCS, every new technology may not address the performance requirements for the DOD and government and requires careful acquisition management to meet mission requirements. As a potential application, the model helps to determine replacement cycles, where technology should switch to the newer innovation, rather than depending on sustaining and improving existing products, which may not maintain competitive edge.

To provide an organizational process to manage disruptive technology, Lindsay and Hopkins (2010) discuss an approach to innovation for incumbents, calling it a two pronged, offensive and defensive approach utilizing low-cost intellectual assets, e.g., small teams specifically designed to either defend against external competitive threats or offensively lay a foundation for future industry growth. They argue that both defending the current methodologies while preparing to integrate and incorporate the disruptive innovation offers

an alternative to a tendency of large organizations to attempt to ignore or crush disruptive innovations, which then does not adapt to the market reality of adopting that new technology. This approach is very similar to what has been put forth by Arquilla and Ronfeldt (1993), who in a military competition context advocate small and flexible teams to approach this problem, rather than a massive body of immovable strength. This work provides early recognition of the value of smaller units designed to respond effectively to unpredictable and uncertain cyberspace change, offering a partial solution for process change within the DOD.

In sum, the disruptive innovation model could be adapted in a novel way to apply to the DOD. In this application, the agents in the model would be nation-states instead of industry organizations, with the DOD considered as the incumbent in cyberspace, and the entrants as the adversaries who might present an unpredictable cyberspace change which diminishes the DOD's competitive edge. Conversely, the theory demonstrates that the DOD might still be an incumbent but innovate to act on the entrant curve, as suggested by Sood and Tellis (2011), using the model as a strategy to continuously gain competitive edge and usurp adversary capability.

Because disruptive innovation theory has not been applied to the public sector in cyberspace as a unified organizational model, the novel idea proposed above would require considerable development. This thesis will therefore contribute to the literature by analyzing innovation strategies that reflect disruptive innovation theory and proposing how its use by the DOD for risk management and prioritization may be possible.

D. CHANGE MANAGEMENT (CM)

Change Management (CM) is a foundational concept in the private sector and is a massive field of research. The management of the change itself is intimately integrated in standard industry practices and necessary to show how the private sector approaches change, both anticipated and unpredictable. CM describes a systematic approach for how an organization can deal with its leadership, people, customers, processes, and resources to effect change from a current state to a future state, internally and externally. In a sense this describes a culture change, where the organization holds its values and mission in such

a way as to respond to changes in a unified manner. The modernization and ubiquitous nature of cyberspace is emerging as a whole-of-organization issue, therefore having the entire organization united in a direction will make the organization postured better to address changes and threats. CM is the largest field of research applied to this thesis, due to its broad application to change and specific application to cyberspace change.¹⁷

While many organizations through history have managed change, the concept as such was formulated in early 1900, with the 1970s increasing the number of authoritative writers. As cited by Prosci (n.d.), Beckerd writes in 1969 about developing organization discipline using organization-wide planning and top-down management. The goal is to increase effectiveness using processes that are planned to use behavioral-science tools. Kotter (1978; 1979; 1988; 1999), is a major source of organizational change methodology; several books from the late 1970s to the early 2000s focus on organizational behavior, leadership, and management power. He makes the case from experience and observation that leadership is different than management, and power and the ability of managers and leaders to influence others is what makes the difference in effectiveness of an organization to make meaningful and profitable change. This section explains CM in general, then highlights several key areas of research that more specifically apply to UUCCS.

As the concept of CM has taken hold, many aspects have been researched and turned into processes to become the foundation of industry thinking. Appelbaum et al. (2012) provide a broad description of CM, analyzing the change model from 1996 to 2011 by revisiting the change management model proposed by Kotter and its relevance after fifteen years. They determine that though Kotter wrote for readability and practicality, the models did not include formal studies to support scientific consensus. That being the case, they conclude that Kotter's change management model is still valid, and their studies support the Kotter principles more empirically. Other experts in the field contribute their

¹⁷ There is a myriad of CM strategies available in the literature, which do not directly address the UUCCS focus of this thesis. They address aspects of CM, including phasing, details, conflicts, caveats, and specific situations, and deeper diving and combination of these strategies might be an area for future research. See, representatively, Liedtka and Rosenblum (1996), Liedtka and Kaplan (2019), Mayer and Vambery (2008), McMillan and Overall (2016).

specific recommendations, such as Kittinger et al. (1997) empirically discussing Business Process Change Methods, Techniques and Tools utilized in their consulting services.

An organization's approach to CM includes multiple elements or factors that direct its methodology. Tamilarasu (2012) discusses organizational change generally and highlighted three major aspects: adapting to change, controlling change and effecting change. His work collates much CM work to highlight principles for CM, processes, scope of change, why people resist change, and then looks at techniques for leadership to facilitate implementation. Similarly, Edmonds (2011) and Giniat et al. (2012) focus on how communication, education, and training can be used to decrease the fear of unknowns for employees, customers, and stakeholders by setting goals, objectives and budgets, by then involving, engaging, and educating the entire workforce of the organization, and by incorporating Feedback in response to changes. These authors also address factors that decrease success in CM, which include: general resistance to change, limitations of existing systems, lack of executive commitment or champions, unrealistic expectations, lack of cross-functional teams, inadequate team and user skills, and technology user un-involvement.

For the private sector, using these concepts to guide organizations through change provides them a competitive edge. Bureaucratic and diverse governmental institutions struggle to apply this lesson quickly yet can over time. However, ability to adapt with speed is central to qualifying CM, converging with the quality of agility already discussed.¹⁸ Agility is a central method of thinking in CM; each change is also subject to time. Decisions and changes must be timely to be effective, and sustained to maintain superior performance, and thus competitive advantage (Worley et al., 2016). This thesis investigates whether and how internalizing CM as a culture mindset, from leadership to subordinates to partners and allies, would help the government adapt to change, and specifically help it address UUCCS more effectively.

The following sections are central to CM and provide a lens for qualitative analysis on the sampled government and industry strategies. Each section below highlights elements

¹⁸ Previously discussed in Chapter II.A.1.

within the general literature that drive success in CM, and which the thesis applies to analyze how well individual strategies address UCCS.

1. Leadership

Much research is focused on individual elements of CM, to which leadership is central. The general consensus is that even the best planning, the best organizations, can become ineffective without proper leadership. Also central to leadership in CM is that the leader is the one who navigates through change, particularly unpredictability, and brings along the organization. Therefore, considering the centrality of unpredictable change in cyberspace, leadership must be dominant in the field of view.

The high impact and effect of leadership on CM has long been recognized by Kotter and other leaders in this field. Aiming toward governmental CM, McFarland (2015) specifically addresses governmental leaders who are required to do more with less, and faster than anyone else. His short paper applies a few leading concepts by other authors but highlights several issues within federal government that slow positive change, such as mission creep and scarce resources, and some capacities that require bolstering, such as human capital, leadership, infrastructure, and motivating employees to change. All these issues are dependent on the capability of the leader to bring about change, and the public sector requires leaders who can manage the incredibly large, dynamic, and complex governmental realities. He argues that it is not good enough to merely manage change, but the leaders must use change to fuel performance improvement.

Leadership recruitment is a sub-topic highly relevant to UCCS. Bunker et al. (2012) contend that status-quo, tried-and-true methodologies can cause difficulties for organizations when the environment changes quickly. They argue that the model for developing leaders who are capable of navigating volatile, uncertain, complex, and ambiguous situations is to first recruit talent for intelligence, technical skill, and high motivation, then teach relational and leadership skills. The key factor is to teach self-directed, experiential learning to decrease lead times and costs (p. 288). Similarly, Hechanova et al. (2018) discuss specific leadership competencies and their effect on CM in both industry and academic situations. They find that CM is more influenced by

execution competencies within industry leadership, and strategic and social competencies in academic leadership (p. 914). This observation converges with previously discussed work indicating that different leadership traits are valued in different sectors and have different impacts on their organizations.¹⁹ Therefore, methodology that guides recruitment of leaders and talent is highly relevant to UCCS and analyzed in Chapter III.

2. Strategic Communication

Strategic Communication is a core foundation of CM, required for any organization that desires to take charge and provide direction for change. Literature consensus is clear that strategy does not produce results by being written down and taped to the CEO's door—strategic effectiveness requires organizational direction, application, comprehension, support, and adherence at all levels, from board members to the newest employee. Strategic communication means conveying organizational direction through constant, consistent, and methodical communication, both top-down for unifying direction and bottom-up for effectiveness Feedback. Alternatively, if communication is not consistently applied in both directions, chance of strategy failure is increased, or effects of the strategy decreased.

Elaborating this overall observation, Rogers highlights the differences between mass communication and interpersonal communication and how leaders use both to affect change in their organizations. Similarly, Giniat et al. argue that leadership must engage the workforce, as well as a stakeholder base, to address real issues, lead in mindsets, identify benefits and sustainable performances, and ensure the vision of change is carried out at a personal level (Rogers & Agarwala-Rogers, 1976; Rogers, 1999; Rogers, 2002; Giniat et al., 2012). As cyberspace has evolved and made information easily available, keeping stakeholders organized under the strategy through strategic communication is a key to success, a key to culture change, and a key to implementation. Analysis of the DOD strategies in Chapter III will show how the DOD uses strategy as its strategic communication, how it filters down, and how that communication causes challenges in the organizational unity of effort for cyberspace.

¹⁹ See Chapter II.B.2.

3. Agents of Change vs. Reactors to Change

Proactive and reactive approaches to change link Disruptive Innovation Theory and CM. Anticipated change is much less likely to cause problems for an organization because the organization can adapt proactively to meet the change through careful strategy. Yet, as discussed in the Disruptive Innovation Theory section, unpredictable or uncertain change can be devastating to any organization. Work on this topic identifies two categories: either the organization is the agent of change, e.g., the cause of the change, or the organization is a reactor to change, either proactively or reactively (Rogers, 2003; Nunes & Downes, 2019; Sood & Tellis, 2011; Lindsay & Hopkins, 2010). These key distinctions are observable in industry as leader organizations or follower organizations. The differentiation of agent and reactor may shift over time, however; an organization may react to a situation, and then be opportunistic and establish itself as an agent of change as the situation evolves. Alternatively, proactively posturing the organization for change allows for advantageous reaction as events occur. This is a spectrum of distinction, but significant in later analysis, which will rely on these distinctions heavily.

To provide opportunistic guidance on how to be an agent of change, Wiltbank et al. (2006) discuss the important independence of prediction and control. They imply that control-oriented approaches that are non-predictive may be successful. They emphasize asking the questions of “what next,” as well as the analyzing costs and risks of strategies and efforts to innovate. Rather than simply responding to changes in market/audience trends, they propose utilizing stakeholder networks and creativity to enter new markets and out-of-normal operations that expand the organization’s competitive edge. This means that instead of protecting against contingencies, an organization can seek to capitalize on the opportunities presented by such events. Furthermore, they recommend an evaluation of such events in terms of acceptable loss, rather than expected return. They take a view that instead of goal oriented strategies, which ask, “what resources, tools and tasks are needed to get to the goal,” organizations should ask questions based on organizational identity, resources, talent and networks that push in a direction that logically arrive at an action. This focuses on the already current strengths of the organization, rather than requirements to implement new change. While this approach is effectively a nuanced risk assessment, it

highlights a mentality that is aggressive in pursuing competitive edge in response to unpredictable and uncertain change.

E. INTERSECTION OF RESEARCH

Each of these major areas of research discussed in this chapter contributes its approaches to the question of UCCS individually but incompletely. At the intersection, however, conclusions can be collated and inferred. From Change Management, Leadership that is strong enough to lead through uncertainty and strategically communicates well contributes to the intersection. Also, agility strategies, both in decision making mindsets and cyberspace speed and reaction time, are significant contributors. Disruptive Innovation Theory demonstrates that “business as usual” can lead to the usurping of an incumbent. The research implies that not all innovations impact entire fundamental systems, however, decreasing immediate and catastrophic likelihood for any innovation. Also, innovations can be observed by competitors and incumbents in use at the innovation and early adopter phases before proliferation. The early observation allows some lead time for the incumbent to determine a response, either as an early majority, late majority, or laggard adopter, or by mitigation of current processes.

Fundamental similarities in cyberspace between the private and public sectors also indicate that strategy should be convergent in both environments. There may be differences in processes - government expresses consensus-based, multiple variate stakeholder processes vs. market-driven private sector entities that express more unity-of-purpose processes—that make strategy translation and implementation between these environments a challenge. Yet, increased partnership between the private and public sectors has been occurring, such as the establishment of the NIST and Tallinn 2.0 manual, which facilitates translation of strategic thinking between the communities. This engagement is also leadership dependent, where different traits are expected of leaders in each sector, but collaboration and partnerships are highly dependent on that leadership to hold together.

Key to each section are several consistencies. Strategic communication to employees, stakeholders and clients is vital to keep the organization on track, and organizations without such communication face increased likelihood of failed

implementation. Also, strategy should have goals which are implemented properly and are measurable, with some metric of success, all of which should be communicated out. This is applicable across all strategy but becomes even more imperative to apply to the wicked problem of unpredictable cyberspace change.

Additionally, the concept of small units capable of quick thinking and action, such as suggested by Arquilla and Ronfeldt (1993), is mentioned or implied in many previous works as a viable method of approaching a problem quickly, then applying significant changes to a greater organization after initially managed by the smaller unit. Also, determining which processes, products, and people require change is important throughout each section; some processes require more flexibility, and some require strict adherence to rules. This requires revisiting these implementations of strategy in an iterative Feedback process, instead of attempting to start from the beginning each time.

No single work has put all this research together to analyze both government and private sector strategies that use these areas of research and evaluate for application, adaption, or adoption across sectors. Collation of the research is therefore necessary and sets the stage for generally answering the UUCS question. The following chapter provides this collation in the context of framing the methodology of its application to the challenge of effectively strategizing for change in key U.S. Government agencies responsible for national cyberspace security.

III. METHODOLOGY

The core question of this thesis, discussed in Chapter I, is how the U.S. Government can draw lessons from private sector entities to improve its anticipation of unforeseeable developments in military cyberspace, and generate an Unpredictable and Uncertain Cyberspace Change Strategy (UUCCS) for this purpose. Chapter II presented the core existing bodies of knowledge from which this thesis draws to address that question. Chapter III outlines the methodology for this analysis, incorporating two frameworks introduced in Chapter II. Subsequently, Chapter IV applies this framework of analysis to the DOD/government strategies as a baseline analysis.

A. FRAMEWORK DESCRIPTION

Chapter III provides definitions, methodology, purpose, and reasoning to describe each researched data element. The quantitative framework is based on a CNA report by Deal (2013), which researched five U.S. Marine Corp strategies and categorized each with four general and overarching elements of strategy: “Diagnosis (Future threats & challenges), Guiding policy (Approach and priorities), Coherent actions (Coordinated & linked objectives), and Assessment Extend meets all elements” (p. 22). These are simply given a “yes,” “no,” or “some” value as assessment. This thesis takes this model and dives deeper to evaluate how much a strategy might be considered a “yes” or “some.” Additional categories are based on the GAO report on U.S. cybersecurity strategy (United States Government Accountability Office, 2013), which highlighted MOS/MOE, milestones, Feedback mechanisms, and resource allocation as requiring increased attention. Additional categories are added for clarity and to address UUCCS. This is further described in the Quantitative Methodology section of this chapter below.

The qualitative framework is loosely based on the work by Bryson and Roering (2007), which utilized SWOT analysis of strategies, primarily focusing on the strengths and weaknesses of the strategy. Deal (2013) also had short summaries of the documents assessed, pointing out trends, strengths, and weaknesses. In this thesis, trends are collated, and differences highlighted to draw out best practices and efforts. The DOD/government

strategies are assessed more thoroughly to describe strategies and trends that may already address UUCCS or highlight potential gaps. The industry strategies are collated as trends and summarized to only focus on those strategies that address UUCCS. In-depth strength-and-weakness discussion for entire strategies is not included here unless it better described how that organization addressed UUCCS. This is to scope analysis to only UUCCS relevant information. This is further described in the Qualitative Methodology section of this chapter below.

B. SOURCE DATA

The four key strategies analyzed are the National Defense Strategy 2018 (NDS), National Cyber Strategy 2018 (NCS) introduced by the White House, the DOD Cyber Strategy, and the USCYBERCOM Command Vision (United States Department of Defense, 2018a; The White House, 2018; United States Department of Defense, 2018a; U.S. Cyber Command, 2018). These are chosen due to the hierarchical nature and collective cyberspace focus. Rather than taking a single strategy, analyzing across multiple strategies provides greater insight into the effort by the DOD and U.S. Government to address the myriad of issues and challenges in cyberspace and how various levels interact and align with the others.

The thesis also analyzed strategies of 22 private sector entities, listed in the source reference list in the Appendix A. Although the four DOD/governmental strategies are readily provided through governmental websites, industry strategies are not readily available. Thesis research obtained these strategies through variate methods, including the organizations' SEC filings Form 10-K, organization website, and published investor annual reports. Attempts to obtain strategic documents via personal contact was attempted at the RSA 2020 conference and a Business Executives for National Security (BENS) conference, meeting, and networking with subject matter experts. None of the organizations provided their proprietary organizational strategy at the RSA 2020 conference, though many made recommendations and pointed to their public documents already mentioned. The data is therefore derived from what is publicly available, and generally focused on language indicating that the information is at least part of the

organization's strategy, i.e., "Our Strategy," or may have been a published product approach strategy for solving problems. The variate source data may account for variation in results. The validity of the data is assumed in that outliers are accounted for in the averages and ratio process. Additionally, business practices and product goals are assumed to be the results of the organization's strategy, and so are valid to represent the strategy, even if not labelled as such. Of note, Splunk is the only organization which had two separate groupings of strategy on its website and SEC filing Form 10-K, which is combined to provide the more comprehensive strategy of the organization.

The case studies are cross-sectional sample of industry organizations, including Fortune 500 cybersecurity organizations, technology organizations, non-cybersecurity technology organizations, and smaller organizations that may contribute diverse lessons for UUCS planning. Private sector strategies are not always directly comparable to U.S. Government documentation, and none are official cyberspace strategies, though the organization may have been built entirely around cyberspace technology. Some strategies may be simpler, yet potentially more succinct, concise, or precise. Some corporate strategies are not written as an explicit strategic document and must be inferred through a website or other documentation. Collation of the quantitative data tries to manage this comparability challenge.

Some of the data is difficult to abstract to the categories analyzed. For example, strategies discussing current products did not necessarily reflect a future change and demonstrated an ongoing production. These would not be included as in the Timelines category unless specifically provided with a term like, "daily," or "24 hours a day, 7 days a week." While the strategy assumes that the discussed products would be utilized daily, only specified language is included in the tally. Other examples include counting "making investments" as contributing a specific budget, or "customer service" specifically mentioned to handle Feedback issues. To be consistent, the MOS/MOE of strategies are not counted if achievement of the strategy is assumed but might have been counted if there is qualifying language, such as "effective." This is an attempt to follow the explicitly addressed strategy, even when it is obvious that the attainment of the strategy is its own MOS/MOE. This limitation is particularly obvious in the DOD/government strategies,

where the goal is clearly to perform the strategy, but not specified that the achievement is the MOS/MOE.

C. QUANTITATIVE METHODOLOGY

Quantitative analysis assesses the specific sections of strategic documents by measuring two variables: how much the strategic section addresses unpredictable or uncertain change, and the presence or absence of other elements related to implementation of strategy. Each document is broken up into its component sections, usually a paragraph under a title heading. For this thesis, these component sections are called, “strategic sections.” The first variable of unpredictable change is designed to assess how strongly the organization focused on being an agent of change—how big of a goal or lofty the aspiration of the organization. The second variable that measured the presence or absence of other elements of strategy informed how well the strategic section addressed the first variable’s claims to address change. The full data spreadsheets are in Appendix B.

The first variable is a measure of “unpredictable change,” which codes how the strategic section addresses unpredictable or uncertain change on a scale of 0–5. This may or may not be cyberspace specific. The higher the number, the more the strategic section is assessed to address unpredictable or uncertain change. Strategic sections assessed to be a 3 or higher on the scale are considered more valuable to this thesis’ considerations for lessons learned. The scale is as follows:

- 0 does not address change at all.
- 1 acknowledges potential for change.
- 2 is a response to some change that already occurred in time, i.e., modernization.
- 3 is a posture for anticipated change, with a single specific or vague uncertainty limited to a single or simple general concept.
- 4 is a greater posture for anticipated change, with broader general uncertainty that may include second- and third- order effects.

- 5 is an aim to act proactively to shape future conditions ahead of the unpredictability, therefore decreasing its unpredictability and uncertainty for the organization itself, and potentially causing it for others.

Many industry products are custom built but may or may not have been counted as a “5” on the unpredictable change scale depending on whether the language includes something like, “proprietary,” “innovative,” “cutting edge,” or “proactive.” Some of these could be assumed based on common business practices but are not counted because they are not specified in the strategy.

The second variable is the presence or absence of the other elements of strategy, which are based on the GAO (United States Government Accountability Office, 2013) report. The report recommended inclusion of more measures of success, milestones, Feedback mechanisms and resources dedicated. These recommendations, as the report suggests, would improve overall cyberspace strategy. This improvement of overall cyberspace strategy would therefore increase and address effectiveness of UCCS. The five categories tallied for each strategic section are: Action Items, Measures of Success or Measures of Effectiveness (MOS/MOE), Timelines, Feedback, Budget Allocated. These are defined and explained below. For each strategic section, these are counted and tallied and entered into a spreadsheet. These elements are multiplied by 0.01 for a computed number at the end of each strategic section as a coded number to show the total for that strategic section in the following equation:

$$\text{Unpredictable Change value} + (\text{total number of tallies for the strategic section} * 0.01) = \text{coded number, 1 of } <\text{total number of strategic sections in the document}>$$

This coded number provided an “at a glance” assessment of the strategic section, where higher number addresses UCCS better than the lower number. This computed coded number is the “Total” column.

Averages for the different elements are taken to provide the overall measure across the document. Combined Averages take the computed averages per document and averages them together to compare all the industry strategies against the DOD/government strategies.

Ratios are taken to reduce the variability between documents further, utilizing percentages to compare between detailed strategies and concise strategies. Combined Ratios take the computed ratios and averages them together to compare all the industry strategies against the DOD/government strategies.

“Action Items” are defined as a statement that declared an effort that “shall” be performed or promises to accomplish a task, all to achieve that strategic section’s overall goal. These are present in every section of every strategy. The number of Action Items varied from document to document, where some are more simple or concise, and others are packed full of direction and action points. Action item tallies are averaged per document to account for variability within the document. The document averages are then again averaged into the “Combined Average Action Items Per Strategy.” This average represented the average action item tallies across all documents. In general, the higher the tally of Action Items per strategic section, the more the section is directive and specific.

“Measures of Success or Measures of Effectiveness (MOS/MOE)” are an indicator that demonstrates that the strategy and/or the Action Items within the strategic section had been accomplished beyond a simple execution of the strategy, e.g., “success looks like _____.” These are tallied per strategic section. The tally would only increase if the strategy specifically mentioned the MOS/MOE, rather than implying that the MOS/MOE is for the strategy to be completed. Some MOS/MOE are the same as the Action Items, depending on phrasing. For example, Action Items might do X, Y, Z in order to do P, D, Q, and all 6 would be counted as separate Action Items, but only P, D, and Q would be MOS/MOE. This is because P, D, and Q would have to be accomplished for the Action Items to be completed. If the phrasing “enables the customer to do A, B, and C,” these are counted as an MOS/MOE, but not an action item because the organization is not doing the action. MOS/MOE tallies are averaged per document to account for variability within the document. The document averages are then again averaged into the “Combined Average MOS/MOE Per Strategy.” This average represented the average MOS/MOE tallies across all documents. In general, the higher the tally of MOS/MOE per strategic section, the more descriptive and meaningful the Action Items became.

While the GAO report used the term “milestones,” this thesis uses “Timelines” to differentiate and prevent confusion for the language that other documents may use to indicate that a milestone is a definition for a MOS/MOE. The definition for “Timelines” is necessarily broadly applied, because most strategies will not tie themselves to minutes or years, but use terms like, “rapid,” “timely,” or “efficiently.” These vague terms are included to acknowledge that there is some measure of time involved but would likely be defined at a lower level or could be situational. There are occasional Timelines, usually annual, which demonstrated some level of the organization’s strategic cycle. Timeline tallies are averaged per document to account for variability within the document. The document averages are then again averaged into the “Combined Average Timelines Per Strategy.” This average represented the average Timeline tallies across all documents. In general, the higher the tally of Timelines per strategic section, the more descriptive and meaningful the Action Items became.

“Feedback” included any specified situation or method where the strategy is readdressed for adjustments, another broad category. These included internal Feedback between departments, market Feedback, customer Feedback, or customer service, to name a few. Accountability is also included in this category, which is highly pertinent to the government. Feedback tallies are averaged per document to account for variability within the document. The document averages are then again averaged into the “Combined Average Feedback Per Strategy.” This average represented the average Feedback tallies across all documents. In general, the higher the tally of Feedback per strategic section, the more descriptive and meaningful the Action Items became.

The definition for “Budget Allocated” is any acknowledgement of resource allocation, either by mentioning a specific number of dollars, an annual budget specified, or even broad terms indicating “prioritization” of resources to the strategy. The scope of these categories is broad to cover artful sentence structures designed for readability and variation in responsible organization. Depending on the source data, this might be reflected more strongly, such as an annual report to investors, who are highly interested in annual returns and budgetary management.

Additional information is analyzed across the entire document, both for computational analysis and to compare strategies at a deeper level. These included the average empty elements, ratio of cyberspace specific strategies, and then ratios to normalize between strategies. The ratios help compare internal consistencies, where the organization may have a high or low number of Action Items, but using the ratio makes the strategy more comparable to the ratio/percentage of other organizations.

“Average Empty Elements Per Strategy” took an average of every “0” count in the Action Items, MOS/MOE, Timelines, Feedback, and Budget Allocated across the whole document. This measure is used to reflect how thorough the organization designed its strategy. The smaller the number, the fewer elements are ignored, which is better. The assumption is that having something tallied makes the strategy stronger and is better than nothing.

The “Cyberspace Specific Ratio” is designed to indicate how many of the strategic sections are related to cyberspace. For every strategic section, it is marked as a “1” for cyberspace specific, and a “-1” for non-cyberspace specific. The non-cyberspace specific strategies tended to be legal or financial focused. The ratio is the number of cyberspace-specific strategic sections divided by the total number of strategic sections. The purpose is to act as a corrective variable to determine whether organizations that are not cyberspace focused, e.g., had a low cyberspace ratio, had some lessons that might apply to UUCS.

The other ratios are computed by taking the MOS/MOE, Timelines, Feedback, and Budget Allocated averages for the strategy and dividing by the Action Items. After computing per strategy, the average is taken for all documents to create a Combined MOS/MOE, Timelines, Feedback, or Budget Allocated over Action Items value. This ratio is to account for style within each strategy, so that regardless of length or number of tallies, the ratio of implementational features to action items would be more comparable between strategic documents.

The total number of documents and strategies analyzed is 26, including the DOD/government strategies. The total number of computed and tallied data elements, which included total strategic elements multiplied by the number of strategic sections, including

the empty elements, all averages, and ratios, is 4,340 data elements. The total number of tallied items (the number of Action Items + number of MOS/MOE + number of Timelines + number of Feedback + number of budget) plus the computed cells is 12,113 individual data points that contributed to the data elements.

D. QUALITATIVE METHODOLOGY

The qualitative analysis is aimed at evaluating the more interpretative and idiosyncratic qualities of specific strategic sections that address UUCCS. The framework, based on Bryson and Roering (2007) and Deal (2013) as described at the beginning of this chapter, lends the model for analysis. The literature review also provides general categories to highlight, such as partnerships, agility, leadership, disruptive innovation, or change management designed to address UUCCS. Each document is analyzed for those general categories, and trends are collated.

The qualitative analysis of DOD/government strategies includes a section on the common themes that address UUCCS across the strategies. The analysis then develops individual strategy sections that highlight specific concepts or elements in each strategy that are stronger than or diverge from the other strategies. This analysis also includes identification of some weaknesses and gaps that do not address UUCCS. The in-depth analysis for the DOD/government strategies is to establish the baseline for comparison, determining what strategies address UUCCS well, and what might be missing or less effective in the future.

The qualitative analysis for the industry strategies are not presented as deeply per strategy; rather, the analysis provides only those trends and specific strengths that contribute lessons learned for UUCCS. This is done in a less in-depth manner to avoid confusing the results and scope for those strategies which only address UUCCS. Results of the collated trends are reported with a description of the strategy and the organizations that mention, utilize, highlight, or develop those strategies.

E. SUB-QUESTION ANALYSIS

Sub-questions are additionally applied to the analysis for clarity. The quantitative and qualitative analysis sections present the current strategies that address UUCCS, which leads to the natural question: Will these strategies be effective in the future? Here the analysis draws on the literature for anticipated effectiveness and combines the quantitative and qualitative information for more detailed analysis. Additionally, answering the second sub-question -- Can the DOD improve on strategies already in existence? -- leads to the further research into the industry strategies. This section includes observations of the strategies considering the key elements in the literature reviewed in Chapter II. Mapping the criteria through these two questions establishes the baseline of current U.S. cyberspace policy for comparison to the industry sampling data in Chapter V.

IV. BASELINE ANALYSIS OF CURRENT DOD/GOVERNMENT STRATEGY

This chapter develops the foundation to evaluate the question of UCCS by undertaking a baseline analysis of current DOD/government cyberspace strategy. Chapter III presented the methodology and framework which is applied to the DOD/government strategies and industry case studies. This chapter presents results of analysis of the four DOD/government strategies: The National Defense Strategy 2018 (NDS), National Cyber Strategy 2018 (NCS), the DOD Cyber Strategy (DCS), and the USCYBERCOM Command Vision (CCV). Quantitative results are followed by the qualitative, after which additional sub-questions are addressed for more in-depth analysis. Chapter V presents the findings for industry strategy and compares the information to the DOD/government results.

A. EXPLANATION OF QUANTITATIVE RESULTS

The quantitative results for the DOD/government strategies presents the baseline for comparison to the industry strategies in Chapter V. The core quantitative finding is the Unpredictable Change evaluation for the four DOD/government strategies. Every strategy was measured for how well it addresses change, on a scale of 0–5, as defined in Chapter III. The cumulative and combined categorical distributions for each section of the four strategies are shown in Table 1.

Table 1. Number and Percentage of Strategies That Address Unpredictable Change for DOD/Government Strategic Documents

Rating	NDS	NCS	DOD Cyber Strategy	USCYBERCOM Command Vision	All Four	Percent
0	0	1	0	0	1	0.80%
1	2	8	0	0	10	8.00%
2	2	9	2	0	13	10.40%
3	7	9	2	2	20	16.00%
4	13	20	9	4	46	36.80%
5	13	9	10	3	35	28.00%
Average	3.89	3.18	4.17	4.11	3.84	
Total	37	56	23	9	125	

Of primary significance to UCCS is the Combined Average Unpredictable Change element, at an average of 3.84. This means that on average, the strategies discussed are mostly aimed to posture for anticipated change, with specific or vague uncertainty limited to a single or general concept. Multiple strategies, such as those designed for innovation, designed to cause change, or including second- and third- order effects, raised the metric. Of note, the DOD strategies had fewer strategic sections per document as compared to the NCS but had higher averages to address the unpredictable change category. The NCS had significantly more strategic sections, but a lower unpredictable change category score, weighting the combined average lower. This is further discussed in the next section.

Overall, roughly one third of the strategic sections are coded category 0–3, meaning these elements are at best are designed to modernize or address a single specific problem, or possibly a broad general problem set that doesn’t consider second- and third- order effects. Roughly more than one third of the total strategic sections are category 4, designed to address second- or third- order effects, and a little less than another third is category 5—designed to cause change. The comparison to industry is in Table 3 in Chapter V.

Without further comparison, the data is indicative that a significant proportion of anticipating future change is already present in DOD and government strategy, though not all change is aimed at cyberspace. Ultimately, however, ideal strategy may not be represented by the highest ranking, or by having every strategic element be a 5 on the scale. Some blend of 0–5 to manage a multitude of issues allows for focusing on higher priority strategies that may require a higher dedication to change. Additionally, the narrative in a strategy that provides the qualitative information may use elements that focus the strategy more appropriately to drive the organization in the direction desired. These issues are discussed further in the qualitative analysis, below.

The focus of this thesis is to determine UUCCS, in which directs interest to the higher ranked strategic sections, and those that specifically apply to cyberspace. With approximately 80% of all strategic sections addressing some form of future change at a 3, 4, or 5, it is reasonable to conclude that DOD and government strategies do a good job of focusing its strategies to address change. Potential for the DOD to nevertheless improve on these measures is discussed at the conclusion of this chapter, following the qualitative analysis.

Anticipation of change in these strategies, however, is far more effective if the strategic provisions are accompanied by explicit provisions for implementation. As discussed in Chapter III, this research analyzed each strategic section to track Action Items, MOS/MOE, Timelines, Feedback, and Budget Allocation; and explicitly tracked when any of these elements were missing. Table 2 provides the data for the four strategic documents. Figure 3 shows the Combined Average tallies for Action Items, MOS/MOE, Timelines, Feedback, Budget Allocation, Empty Elements, and the Combined Average Unpredictable Change calculation. Full data tables are located in Appendix B.

Table 2. Average Number of Implementation Elements per Section for DOD/Government Strategic Documents

Element	NDS	NCS	DCS	CCV	All Four
Action Items	10.11	8.93	8.61	18.67	11.58
MOS/MOE	4.70	3.20	3.74	5.89	4.38
Timelines	0.51	0.18	0.70	1.33	0.68
Feedback	0.19	0.29	0.39	0.67	0.38
Budget Allocation	0.57	0.11	0.04	0	0.18
Empty Elements	2.32	2.66	2.22	2.11	2.33

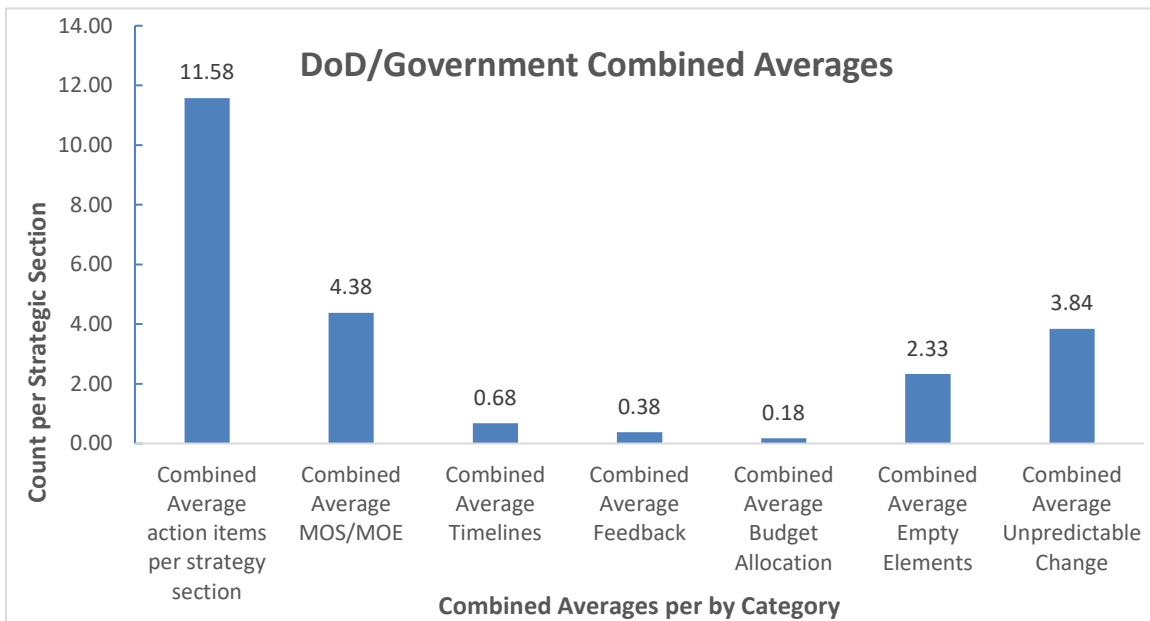


Figure 3. DOD/Government Strategy Combined Averages

The first major metric of significance is the Empty Elements per Strategic Section. On average, there are 2.33 empty elements per strategic section across all four documents. This means that for nearly every strategic section, two- to- three of five implementation categories are not included in the strategy. Mostly, these missing elements are Timelines, Feedback, and budget categories. These findings support the GAO 2013 report that indicates these elements tend to be missing. Therefore, while this area of strategy may have improved, there is still room for improvement.

There is an average of 11.58 Action Items per strategic section, indicating significant direction and action required of the organization for each section. For those Action Items, on average there are 4.38 MOS/MOE per strategic section. Sometimes the strategy's measure of success is obvious, such as from the NCS, "The Administration will clarify the roles and responsibilities of Federal agencies and the expectations on the private sector related to cybersecurity risk management and incident response (The White House, 2018, p. 8)." These kinds of strategies are assumed by leadership to not require clarification on a measure of success. A positive use of an MOS/MOE is from the DOD Cyber Strategy: "Expand crowd-sourced vulnerability identification: ... in order to identify and mitigate vulnerabilities more effectively and to foster innovation (United States Department of Defense, 2018a, p. 6)." The MOS/MOE is clearly noted as an end goal, strengthening the strategy's purpose.

As noted above, the elements that tended to be ignored in the strategies are the Timelines, Feedback mechanisms and Budget Allocations, with averages of 0.68, 0.38, and 0.18, respectively. This means Timelines, Feedback, or Budget Allocations are not significantly included in every strategic section. Timelines are observed to be neglected because many strategies are designed to direct regular activities that would never stop. Alternatively, there are many strategies that stated a fixed goal but no timeline to indicate the urgency of that goal or when it is to be accomplished. The lack of Feedback mechanisms may have been assumed by the strategy, in that accountability or official Feedback mechanisms are not necessary to include in the strategy. The better Feedback mechanisms assigned an entity responsible to monitor activities for effectiveness or completion of the strategy. Finally, federal and military budget is generally distilled to "prioritization in the budget" or a single reference to a national fiscal year budget in the NDS (United States Department of Defense, 2018b, p. 6). To align with the GAO 2013 report recommendations, these are elements that can use improvement.

More detailed analysis links MOS/MOEs, Timelines, Feedback, and Budget Allocation to the Action Items. As discussed in Chapter III, the ratios are designed to represent percentage of internal relationships between the Action Items and the associated elements that strengthen and clarify the strategic section. This ratio is to account for style

within each strategy, so that regardless of length or high or low tallies, the ratio would be more comparable between strategic documents. Figure 4 shows the ratio of these elements to the Action Items, which more clearly demonstrates how much or little the other elements of strategy are applied against the Action Items.

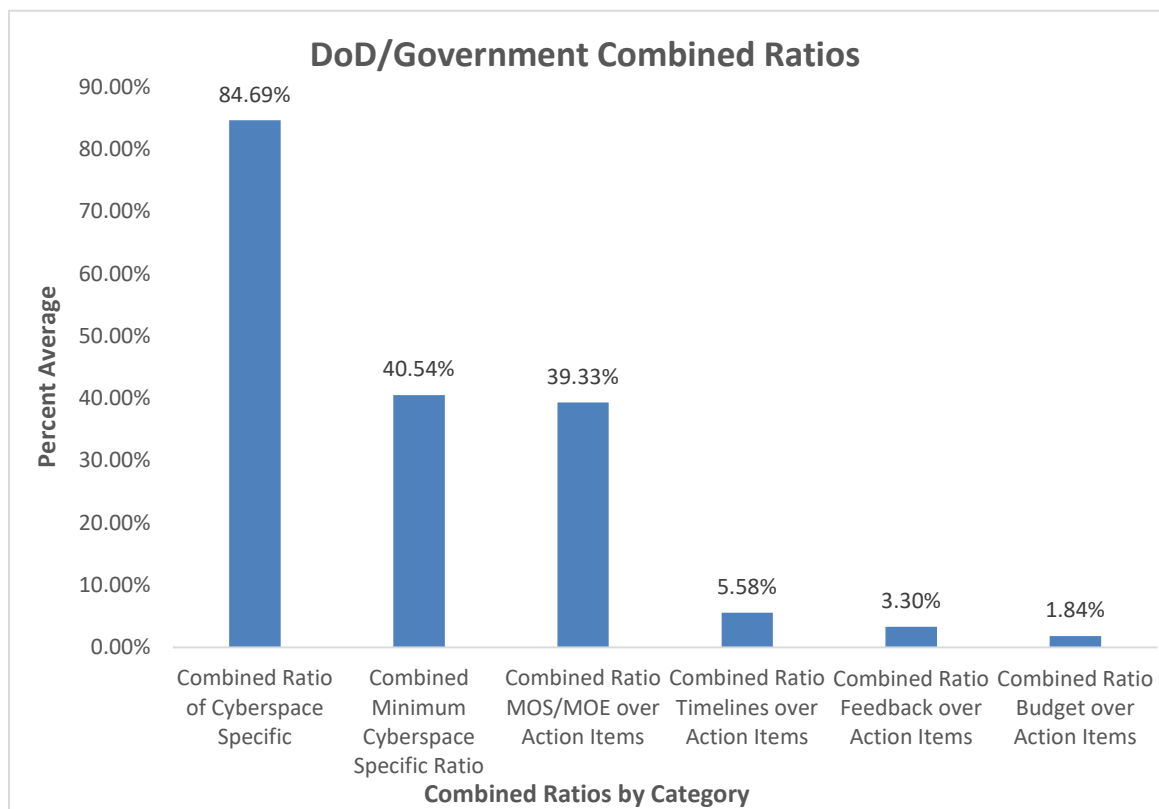


Figure 4. DOD Combined Ratios across All Four Documents

On average, approximately 40% the Action Items include MOS/MOE (combined ratio MOS/MOE over Action Items category), whereas less than 6% include Timelines (combined ratio Timelines over Action Items category) or Feedback mechanisms (combined ratio Feedback over Action Items category), and less than 2% include Budget Allocation (combined ratio budget over Action Items category). Again, the purpose of the ratio is to assess document-internal consistency. For example, the NCS has 56 strategic sections as compared to the U.S. CYBERCOM Command Vision's 9 strategic sections. The NCS includes approximately 9 Action Items and 3 MOS/MOE per strategic section,

and the U.S. CYBERCOM Command Vision packs nearly 19 Action Items and 6 MOS/MOE per strategic section. However, both demonstrated a similar ratio of MOS/MOE to Action Items at 35% and 31% respectively. Therefore, the ratio accounts for variation in style and is better able to show similarities and comparisons.

Additionally, the Combined Ratio of Cyberspace Specific strategies is nearly 90%, which is largely due to the use of three cyberspace-focused strategic documents (combined ratio of cyberspace specific category). The NDS had the lowest number of cyberspace-specific strategic sections at approximately 41% (combined minimum cyberspace specific ratio category). This is an expected finding, particularly because while the NDS is applied for the entire DOD, and the other strategies are specifically selected to look at cyberspace strategy. However, the comparison and significance are more obvious when compared to industry strategies in Chapter V and Figure 6.

B. EXPLANATION OF QUALITATIVE RESULTS

The following qualitative assessment first presents a collation of the common themes across all four DOD/government strategies, followed by sections for the individual strategies that highlight specific elements not seen in the others. Each section summarizes the approach taken by the DOD/government to answer the UUCCS question based on the qualitative methodology discussed in Chapter III.

1. Common Themes That Address UUCCS

As alluded to in previous chapters and evident in the data reviewed in the preceding section, there are elements common to each strategy that address some element of change, either directly or indirectly, cyberspace or non-cyberspace. Much of the analysis follows similar themes introduced in the literature, including partnership, innovation, and agility.

a. Competition and Persistence

In the NCS, NDS, and DOD Cyber Strategy, new language from previous strategies indicates a higher level of engagement in cyberspace. The emphasis is now on competition in cyberspace, which is a change in mentality from the previous “cybersecurity,” or “cyber warfare.” Now, each strategy includes new language referring to a higher state of

operations: in the NCS, “continuous competition” (White House, 2018, p. 2) and “now-persistent engagement” (p. 20); the NDS’ goal of “strategy to compete” (United States Department of Defense, 2018b, p. 1); and the DOD Cyber Strategy’s use of persistence (United States Department of Defense, 2018a, p. 4). This higher state of operations is a daily, 24/7 presence and effort to maintain competitive edge in cyberspace. This 24/7 presence is also being integrated into other areas that are becoming increasingly cyberspace related or dependent, and therefore requiring increased awareness among all personnel. This is especially evident in the DOD Cyber Strategy’s emphasis on institutional culture, for all personnel and at all levels, that is more aware of cyberspace and decision-making that involves cyberspace (United States Department of Defense, 2018a, p. 5).

b. Integration into Multiple Domains

Each strategy includes a significant priority to integrate cyberspace into the entire spectrum of operations. The NCS (White House, 2018) uses language that aims to include cyber into every element of national power (p. 20), later emphasizing diplomatic, information, military, financial, intelligence, public attribution, and law enforcement capabilities (p. 21). These are later echoed by the NDS (United States Department of Defense, 2018b, p. 4), which is then narrowed and focused for the DOD Cyber strategy into a deterrence strategic section (United States Department of Defense, 2018a, p. 4).

Integration strategy also continues bringing cyberspace out of an intelligence-only focus, recognizing the power and potential for supporting and enhancing other domains. Consistency on this theme through all four documents lends strength to the effort overall and assists in bringing the challenges of cyberspace to the forefront of every domain and element of national power, and to the many government agencies that are now utilizing and depending on cyberspace significantly. State and non-state malicious actors are already utilizing cyberspace technology, which poses a threat to U.S. efforts and interests. Recognizing the vulnerability in all aspects of life due to cyberspace requires bolstering the integration of cyberspace efforts in anticipation of adversary aggression (United States Department of Defense, 2018b, p. 3).

c. Automation and Data Analytics

The NDS and DOD Cyber Strategy highlighted automation and data analytics significantly, acknowledging the need for data processing and speed not attainable by human operators alone (United States Department of Defense, 2018b, p. 7; United States Department of Defense, 2018a, p. 4). These are merely mentioned in NCS, but not at all in USCYBERCOM Command Vision. The NCS, being a broader national strategy, does not cite very many specific technologies, particularly because it is addressed also to private sector partners which are so varied that significant technological specificity might hinder rather than enhance. The focus for the NDS and DOD Cyber Strategy on automation are to gain military advantage, identify malicious cyber activity, and improve defensive posture. The specificity and direction offered here is focused and clear toward cybersecurity posture, which addresses concerns of ambiguity previously mentioned in GAO reports and by Clinton (2015). Chapter V will discuss how this particular strategy may be expanded.

d. Partnerships, Understanding Differences in Industry, and Information Sharing Analysis

Significant portions of the baseline strategies are dedicated to partnerships. These partnerships include industry, academia, intra-governmental agencies, and inter-government relationships. This is a significant recognition that the government is not the only entity required to defend and use U.S. cyberspace capabilities, that the DOD will not have all the answers to unpredictable and uncertain cyberspace change, and requires close relationship with the industry that will have necessary expertise, resources, capability, and focus to address those changes.

Listed partnerships included international partners, government agencies, private sector, and academia. Partnerships are further refined to include shared challenges and interests, and which also provide regional coalitions and security cooperation. The NDS also includes “small companies, start-ups” as partnership opportunities (United States Department of Defense, 2018b p. 8). It also recognizes that every ally and partner is unique and emphasizes that interoperability between these relationships is required. Other partnership purposes highlight trade, energy, and political stability, as well as an exchange

of ideas and best practices (United States Department of Defense, 2018b, p. 9; White House, 2018, p. 26).

Three directions are held in common in the partnership strategies are: Information sharing, reporting, and coordination. Reporting and coordination between government agencies are already a part of policy and procedure, though they can always be improved. Information sharing, however, is a strategy that leaves much to be desired. The strategies do not clarify the legal separations, de-classification, and inter-agency coordination needed to support cross-sector information sharing, using terms like “as much as possible” in the NCS (White House, 2018, p. 9) or “to the maximum extent possible” in the USCYBERCOM Command Vision (U.S. Cyber Command, 2018, p. 10).

Most especially, the strategies direct “timely” information sharing, such as the NCS (United States Department of Defense, 2018b, p. 21), leaving significant room for interpretation. Because information loses intelligence value over time, particularly for imminent attacks, timely information sharing might be subjectively interpreted by the government. This may potentially cause delays in time-sensitive actionable information. Instead, the bureaucratic processes, de-classification, and potential risks of loss of governmental intelligence capability become a strong barrier to the information sharing process.

e. Imperatives for Cultural and Technological Innovation

Innovation is regularly referenced within each strategy as a necessity. The DOD Cyber Strategy offers the most specific direction and definition for desired results, echoed by the USCYBERCOM vision statement’s focus on disruptive innovation: innovate for agility to keep pace with evolving threats and technologies in cyberspace faster than strategic competitors (United States Department of Defense, 2018b, p. 4; U.S. Cyber Command, 2018, p. 8).

Innovation is defined both culturally and technologically. Culturally, in the NDS, “Organize for innovation” and “evolve innovative operational concepts” are kinds of strategies to address unpredictable change because they are intended to cause change internally (United States Department of Defense, 2018b, p. 10, 7). Further clarifying this

direction, the NDS provides a measure of effectiveness, that “[i]f current structures hinder substantial increases in lethality or performance, [then] Service Secretaries and Agency heads will consolidate, eliminate or restructure (p. 10).” Similarly, each strategic document acknowledges the need to innovate, which is indicated to be one of the strongest UUCCS elements: to be proactive, be ahead of developments, and to cause change that can be managed rather than react to change.

f. Agility Aspirations

Each of the strategies includes agility or a similar term to address change, either anticipated or unpredictable. The NCS focuses on the terms, “adaptability,” “resilience,” and “innovation” in cybersecurity (White House, 2018, p. 15). The NDS, DOD Cyber Strategy, and U.S. CYBERCOM Command Vision each use agility for posture, innovation, processes, or operations (United States Department of Defense, 2018b, p. 7; United States Department of Defense, 2018a, p. 4; U.S. Cyber Command, 2018, p. 9).

Agility is assumed to be understood, is broadly applied, and is not necessarily specific to cyberspace, as in the NDS, but is included by implication. As mentioned in Chapter II, the DOD Dictionary does not include a definition for agility (Joint Chiefs of Staff, 2020), and the inferred definition from Joint Publication 5-0 indicates an ability to adapt in a timely manner based on a situational context (Joint Chiefs of Staff, 2017, p. I-15.b). There are no sections that direct a specific metric framework to unify the entirety of the DOD or government. Connecting agility to cyberspace is further discussed in the Sub-Questions Analysis section below.

2. National Defense Strategy 2018 (NDS)

The National Defense Strategy (NDS) (United States Department of Defense, 2018b) is the guiding strategic document for the entire DOD and is not cyberspace centric. The primary and most relevant key strength to UUCCS in the NDS is the acknowledgement of a prioritization of cyberspace (p. 6). A section including cyberspace as a warfighting domain had not been prominently presented in previous versions of the NDS. This section directs that cyberspace should be prioritized for investments and integration into the spectrum of military operations. The prioritization had not appeared quite so strongly in

previous national-level defense strategy and speaks to the recognition that the DOD is not immune to cyberspace change, despite previous superiority. This acknowledgement aims to bring the change to the forefront of national efforts to integrate and modernize cyberspace capabilities.

However, this section specifically differentiates cyberspace from Command, Control, Communications, Computers and Intelligence, Surveillance, and Reconnaissance (C4ISR), which is heavily dependent on cyberspace, if not specifically a part of cyberspace. Differentiating the concepts confuses authorities, and roles and responsibilities. At best, the difference is largely ignored, but makes the strategy more ambiguous and decouples cyberspace integration into the full spectrum of military operation, as is directed (p. 6).

Also, the NDS includes key terms and concepts such as “agility” and “resilience,” highlighting those desired outcomes for all domain capabilities (air, surface, subsurface, etc.). As discussed in the previous section, these concepts are assumed to be understood but particularly difficult to apply and implement in cyberspace at an every-day, operational or lower level.²⁰ Yet, despite the difficult nature in translating into the low-level of cyberspace, fostering a competitive mindset or culture that includes agility and resilience can be applied to cyberspace and the problem of uncertainty and unpredictability, just like for industry.

The NDS discusses talent, acknowledging that military, civilian and contractor personnel are all responsible for the best practices and accomplishment of the mission. Leadership is highlighted for education and development for decision making. This is specifically differentiated from the civilian workforce, which aims to bring in new and critical skills. As compared to the other DOD strategies, this section on talent management is more specific in who the strategy supports and what actions shall be taken to achieve the goal. The primary specification is the Professional Military Education (PME), which is not specifically repeated in the other strategy documents (United States Department of Defense, 2018b, p. 8).

²⁰ Also discussed in Chapter IV.B.1.f.

The NDS offers speed of relevance as a key to success, desiring to change the current DOD culture that is “over-optimized at the expense of providing timely decisions, policies, and capabilities...” (United States Department of Defense, 2018b, p. 10). As a strategy, it is both aspirational and necessary. The difficulty in this strategy will be in the implementation, and that there is no direction on measure of success, who will be responsible, or Feedback to demonstrate success or even iterate this strategy as it is implemented. Additionally, the interpretation of “speed of relevance” hypothetically increases risk. The risk is that various stakeholders may use ambiguity to accomplish their revenue goals over the DOD’s mission focus, particularly if a long-term “speed of relevance” increases profits for that organization.

Overall, the NDS strategizes increased military capability and includes cyberspace significantly in that projection. Specifically, this increased military capability includes modernization to address anticipated change, and innovation to address unpredictable and uncertain change.

3. National Cyber Strategy 2018 (NCS)

The National Cyber Strategy 2018 (NCS) (White House, 2018) is an all-of-government strategy, and so has elements of law enforcement, DHS, DOD, IC, and FBI included throughout the document. Most importantly, this strategy is the first actual national cyberspace strategy, as opposed to the previous Cybersecurity National Action Plan (White House, 2016). Of note, the strategy follows some recommendations made in the 2013 GAO (United States Government Accountability Office, 2013) report by addressing integration and more clearly defining the roles and responsibilities of the government and enacting cyberspace into clearer national level strategy.

One of the key differences in the NCS from the others is a paragraph in the introduction section dedicated to the definition of success in cyberspace. It is broad, encompassing vulnerability identification and protection, resilience, incident response, destabilizing malicious cyber activities, deterrence through imposition of costs through both cyber and non-cyber means, and using cyber capabilities to accomplish U.S. national security objectives (White House, 2018, p. 3). As compared to the DOD strategies, having

this particular section demonstrates a more concise direction, despite the higher-level and broad nature of the document.

Also specific to the NCS is the clearest “partnership” directive out of all the strategies. A specific section directs subordinates to “Leverage information communications technology providers as cybersecurity enablers (White House, 2018, p. 9).” This is the only strategy of all four that highlights a specific group of stakeholders for partnerships with a specific task implication. This highlights the unique position of communications providers to handle risks within their networks or for customers that the DOD/government is unable to reach. Part of the advantage is that a private sector entity can respond to unpredictable and uncertain market changes or threats (which is its own incentive and the organization’s best interest) quicker than the entirety of government, since this is what keeps the organization’s competitive advantage.

The NCS is the only document of the four that directly addresses supply chain risk management. This has been increasingly of concern, where vulnerabilities at any point in the chain weaken the whole structure (p. 6–7). This is a newer strategic concern that the private sector has been addressing for decades already, but is meant to control the uncertain possibility of adversaries inserting vulnerabilities and malicious cyberspace capability into the supply chain in such a way they would be undetected and gain adversarial advantage in the future.

The strategies for talent management are concerned with hiring good talent or leveraging partnerships that might have talent capability not contained within the government. This is the most specific strategy of the four on this issue because it establishes the National Initiative for Cybersecurity Education (NICE) framework as the methodology to use for standardized cyberspace hiring practices (p. 17). This is not repeated or reflected in the DOD strategies. These strategies also include incentives to retain talent, including training and operational opportunity, but are limited because much of any normal incentive is monetary. The government cannot compete with industry for monetary incentive, having rigid pay scale structures that are generally considered non-competitive when compared to industry for the same jobs. Rewards, recognition, and training are included, but not specified, and are also limited by the same resource constraints for monetary reward.

Related to talent management is the assignment of significant roles and responsibilities to specific leadership, such as departmental Chief Information Officers (CIO), and the expectation to hold leadership accountable for risk management decisions and information technology (IT) procurement (p. 7). The other strategies do not include specific roles or address cyberspace leadership specifically.

One theme throughout the whole document is the development of metrics and the use of risk management, but most of it is assigned to the current White House administration for action (p. 7, 8, 10, 11, 14, 15, 17, 20, 21, 25). This is a very significant observation: in other strategies, the entity assigned responsibility for action is vague or non-existent; here, the administration is taking responsibility to develop those metrics and apply the risk management. Assessing the implementation of this strategic element is out of scope for this thesis, but future research should assess whether those recommended metrics and tools are pushed down to be used at all levels, which would make the strategy more valuable. Due to the DOD's size and the government's bureaucratic nature, change to utilize these tools at all levels can be expected to be a significant difficulty.

4. The DOD Cyber Strategy 2018

The DOD Cyber Strategy (United States Department of Defense, 2018a), subordinate to the NDS and NCS, brings in elements of both and has a few increasingly specific elements that apply directly to the DOD. Where the NDS aims to integrate into strategic competition “multiple elements of national power—diplomacy, information, economics, finance, intelligence, law enforcement and military” (United States Department of Defense, 2018b, p. 4), the DOD Cyber Strategy loses the connection to several key elements of strategic competition. Instead, strategic competition is distilled in cyberspace only to military, infrastructure, and economic threats. Diplomatic, information and law enforcement efforts are only referenced in coordination or sharing with other Federal departments and agencies, and those not specifically, but rather as “partners” (p. 5). Of interest, this leaves efforts to generate diplomatic and informational effects to the other agencies and does not provide for diplomatic and informational capabilities within the department for its own missions. The NCS demonstrates that diplomatic and informational

capabilities are becoming increasingly important as missions and operations can be exposed quickly with decreased secrecy due to media and propaganda proliferation (White House, 2018, p. 2). This language is lost in the DOD Cyber Strategy and leaves a significant capability gap that remains unaddressed.

Other themes are also addressed in the other documents, but increased direction would be expected in a subordinate strategy. Issues such as accelerating cyber capability development, streamlining acquisitions, and the challenges of commercial-off-the-shelf (COTS) products are discussed in all the strategies, but are not further refined as a subordinate strategy. These strategies are also difficult to measure and define as successful, making implementation at all levels difficult, and individual interpretations that stovepipe efforts cannot be integrated or compared to other efforts at a larger scale. Additionally, many jobs have been created for the sole purpose of processing and handling acquisitions and maintenance of these systems, and to streamline these might remove these kinds of positions, where removing positions and reorganizing is a significant challenge in the government. These types of challenge tend to reside at a very high level, as similarly discussed in the NDS, and in some cases may not be applicable because the DOD is bound by the rules of governing policies, like the Federal Acquisitions Regulations (FAR), limiting how fast and effective changes can be made when it comes to acquisitions. The Sub-Question Analysis section below further discusses this topic.

The DOD Cyber Strategy continues to highlight critical infrastructure, in line with efforts originally presented by the Cybersecurity National Action Plan (White House, 2016). The DOD strategy distinguishes two definitions: The Defense Critical Infrastructure (DCI) and U.S. Critical Infrastructure. DCI is applied to the systems and infrastructure of the DOD and non-DOD assets to support DOD (United States Department of Defense, 2018a, p. 2,3), whereas much U.S. Critical Infrastructure falls under DHS in authority. Some of the document describes the critical infrastructure information sharing previously mentioned in other strategies, but this falls under DHS largely (Congressional Research Service, 2019, p. 3). Much of the sharing is also handled at a very high level, and so the strategy becomes minimally applicable to lower-level operators. However, the effort to defend critical infrastructure is significant, and this attention is a recognition of the

tremendous vulnerability within these systems that increases the likelihood of unpredictable or uncertain malicious efforts.

One concept in the DOD Cyber Strategy that connects to Cold-War nuclear era thinking is “deterrence,” which is used in many broad DOD strategies, as well as in the NCS. The NCS discusses deterrence in the context of all instruments of national power, modernization of statutes and norms, and international coalitions (White House, 2018, p. 21). The specificity from the NCS is lost in the DOD Cyber Strategy. Instead, deterrence becomes less specific concept, perhaps depending on prior thinking to provide definitions and scope for cyberspace deterrence.

Deterrence in cyberspace has been a contested concept for a long time, with significant evolution of thinking and contributions from many strategic specialists.²¹ Research shows that the ease of entry and cost for malicious actors is very low compared to the potential gains.²² Proof of guilt and attribution, global reach, and obstacles to punitive responses make the concept of deterrence in cyberspace difficult. Without serious consequences, applied quickly, consistently, and publicly, the malicious state actor tends to have little to fear, particularly across international jurisdictional lines, as discussed by Demchak (2012). Yet, despite these challenges, trenchant insufficiencies of defense in cyberspace keep deterrence in the forefront of strategic thinking, as is exemplified by one of the newest articulations, the Cyberspace Solarium Commission Report (King and Gallagher, 2020).

Certainly, effective cyber deterrence would be highly beneficial to prevent unpredictable and uncertain issues before they arise. While this aspirational deterrence goal in the DOD Cyber Strategy is desirable, the strategy does not clarify what direction to take, or include Action Items, Feedback, metrics, or Timelines for implementation. This leaves unclear what deterrence might mean, how it can be applied, and how much our strategy can depend on it. Certainly, the research makes obvious that many malicious cyber actors

²¹ For a seminal work, see Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009), ISBN 978-0-8330-4734-2.

²² See section I.C.a

are not deterred often, and yet any successful deterrence is not made common public knowledge, further weakening perceived results in a deterrence strategy.

Talent in the DOD Cyber Strategy is addressed more vaguely than the NDS. The majority of the four sections distill to some variation on building and supporting talent, offer a few skills desired, but demonstrate that much of the work to develop incentives and programs has yet to be established (United States Department of Defense, 2018a, p. 6). Naturally, that is what a strategy is for, but this highlights that the human resources capability for cyberspace has still not caught up to modern talent management methodologies. Nearly a decade after the establishment of USCYBERCOM, the need to *develop* talent management practices over *adjusting* practices that should have been already established demonstrates how far behind the DOD is to industry in talent management.

Lastly, the document offers a short and specific note on the use of crowd-sourced vulnerability identification as a strategy. This is a newer concept, adopted from industry, that allows for outside sources to comb through networks and applications to find vulnerabilities that the engineers or operators may not have found. This is a specific action that is not in any other strategic document, certainly is an effort to address cyberspace changes, and has been proven to be effective, both in cost and in generating increased resilience.

5. USCYBERCOM Command Vision 2018

The USCYBERCOM Command Vision (U.S. Cyber Command, 2018) contains many of the same elements of the first several strategic documents, including: partnerships, agility, and increased resiliency. A notable variation observed for this document is use of the term “persistence” in lieu of the term “competition” (p. 6). This may be due to the translation from high-level document to lower level application of the strategy, but it could also reflect a refinement of thinking about how specifically the U.S. should engage adversaries in the competitive cyberspace environment. Indicatively, persistence is well defined in the CYBERCOM Command Vision, answering the questions of “how,” “where,” “when,” and “why” (p. 6).

Of note, the spirit of this document is focused on defensive and offensive cyber operations, which have specific meanings and authorities, but the usage does not reach into the other domains that utilize cyberspace just as heavily. The other domains have high tech cyberspace components, such as modern guided weapons, radars, aircraft, submarines, ships, vehicles, and communications between all of them. All of these technologies have hardware and software associated with them, but USCYBERCOM is largely uninvolved in the acquisitions, security, monitoring, or vulnerability analysis of these systems outside of the network they connect to, and has no authority to impose actions to integrate into the other domains. This is partially addressed by partnering with the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the rest of the Intelligence Community (IC), which may have more insight into the other domains (U.S. Cyber Command, 2018, p. 7). The strategic limitation in resources is specifically addressed in the Risk Mitigation section, which projects that the scarce resource of USCYBERCOM's capacity would be directed for strategic use, depending on increased resilience in DOD systems to combat malicious actors.

The USCYBERCOM Command Vision has a new element that the previous strategies did not: a full section describing USCYBERCOM's approach to Risk Mitigation (p. 10). Specifically, constrained resources require prioritization of adversary targets and care to mitigate diplomatic risk in cyberspace actions. The section self-identifies a weakness to address change, particularly due to a capacity limitation to respond to the diplomatic issues. But it does not discuss that the U.S. Department of State handles many diplomatic issues, which might be clarified with a stipulation on partnership between the departments. Instead, operations are done with "allies and coalition partners," which is not indicative of whether the Department of State is included. The constrained resources also show that outside the prioritized targets, the "high-demand, low-density maneuver force" is not likely to respond to changes quickly, due to prioritization already being applied. This is a self-declared limitation in capacity to address change. The proposed mitigation is to increase resiliency to DOD systems and sharing intelligence with intra-governmental partners.

The last section of this document is an implementation guidance to the subordinate forces and includes specific Feedback mechanisms and responsibilities under the USCYBERCOM Chief of Staff. Additionally, the mentioned key measure of success is execution by all personnel (p. 10). As a measure of success, this is a challenge, because it does not include any measurable definition which makes it difficult to hold subordinates accountable. However, this section provides the most specific Feedback mechanism and expectation of execution by subordinates, which is not included in the higher-level documents.

6. Sub-question Analysis

The core question of UUCCS requires addressing additional sub-questions to further refine the baseline analysis of these DOD/government strategies. The quantitative results measure how much each element of strategy is provided within each strategic section and then in a combined method. The qualitative sections built on this overarching cumulative data by discussing specific DOD/government strategy results that address UUCCS. Assessing the two sets of results together helps answer the sub-questions.

The first sub-question considers whether these strategies will be effective in the future; an assessment drawing on the preceding quantitative and qualitative analysis identifies potential gaps and the opportunity for the utilization of private sector lessons learned. The second sub-question uses the prior assessment to determine whether the DOD can improve on the current strategies, and whether certain aspects of strategy may not be required to be addressed. These questions lead to Chapter V, where the lessons learned for UUCCS are presented and compared.

a. Effectiveness of Cyberspace Strategies in the Future

The assessment of quantitative and qualitative results poses challenges for the future effectiveness of U.S. cyberspace strategies. To start, while agility is mentioned in some form in each strategy, ambiguous used of the term raises some issues. Chapter II demonstrated that agility can be applied to thinking and cyberspace metrics and leaves

much room for interpretation.²³ Agility is one of the more explored concepts in the literature, but if it is not specifically defined, particularly for cyberspace at a fundamental level, the DOD may not get the desired effect out of its strategy.

The reason is a technical one: much technology, particularly networked cyberspace, requires disparate elements to follow standardized rules that generally remain static to interface with other disparate elements. The internet, for example, specifically communicates using protocols that allows communication to pass through and interact with numerous organizations, hardware, and software to get from its originator to destination. Much of this standardization is *static*. To create agility within a network introduces an amount of unpredictability and uncertainty for adversaries, but also increases complexity for the owners and administrators of the network, potentially giving the administrators the same amount of unpredictability and uncertainty that the adversary has. For the administrator to decrease the unpredictability and uncertainty despite increased complexity requires increased control and knowledge of the network.

As the government is discovering, there is already tremendous complexity in the interfaces between the extremely large set of DOD and contracted networks and other networks and critical infrastructure not owned by the DOD—a wicked problem. Whereas the DOD Cyber Strategy specifically aims to “Innovate to foster agility” (United States Department of Defense, 2018a, p. 4), Schousboe (2020) cautions that innovations do not always benefit the organization, and quotes Demchak to say that innovation may increase organizational complexity even while increasing organizational effectiveness. This complex system decreases the amount that individual administrators can know and control. At a broader level, attempting to know and control these complex systems requires integration of cyberspace systems, rarely emphasized in the DOD/government strategies, which requires an *increase* of static standardization so the systems can interact with each other. This effort aims to decrease complexity and the difficulties that arise with that complexity, yet it is antithetical to agility.

²³ See Chapter II.A.1.

The technical discussion on networking is an example, but the issue extends to all of cyberspace. Cyberspace operates at a technical and logical level, and requires stable, static protocols to operate smoothly. While the stable nature of cyberspace is desired for the smoother operations, malicious actors take advantage of such stability for their operations. Additionally, as technologies change or are added, and organizations scale in cyberspace, current technology also must keep pace with growth. Thus, for cybersecurity and technology change, agility as a strategy has been conceptualized in both public and private sectors as a key concept for decades. But the concept becomes ambiguous as a DOD cyberspace strategy without reinforcing that strategy with higher definition, measures of effectiveness and success, and other direction and definition to move beyond a buzzword and into practice. Without the unification of a single system of measurement, quality decisions on the effectiveness of an “agile” capability are less likely because the information provided to decision makers will require further analysis to compare differences and meaning.

Similar to agility is the concept of “speed of relevance,” designed to streamline acquisitions and development, discussed in the NDS and DOD Cyber Strategy (United States Department of Defense, 2018b, p. 10; United States Department of Defense, 2018a, p. 4). The specific section on the “speed of relevance” proposes streamlining rapid, iterative, and modular upgrade approaches from development to fielding new technologies. This is admittedly necessary for competitive edge, and a quality mindset to address unpredictable and uncertain cyberspace change. However, this strategy can be difficult in its implementation due to governmental acquisitions regulations that are broader than the DOD and restrict the effectiveness of this very effort. The Federal Acquisitions Regulations (FAR) (2020) determines actual acquisitions processes for the DOD, challenging the effectiveness of this strategy. The DOD is not responsible for managing these regulations and is subject to follow them. Therefore, aiming to streamline acquisitions at the speed of relevance may not be as effective simply because the DOD must still follow external regulations.

In addition to regulation restrictions, scalability applied across the DOD at a macro, departmental level, as opposed to a micro, more tactical unit level, takes many years to

implement, which is very rarely considered “rapid.” In addition, there are numerous limitations to apply use of already developed-commercial-off-the-shelf (COTS) cyberspace tools into the broader DOD, IC, and Federal cyberspace systems. The main limitation is that the certification process for a COTS system to be allowed into a government system has a high barrier to entry and high cost, both in resources and time. This tends to preclude smaller industry organizations that could potentially field cheap and reasonable solutions to problems, but would cost too much to certify, pushing that solution to different, lower cost markets.

Similarly, the concept of modernization, while purposeful, necessary, and well-reasoned in the strategy, presents some challenges. Modernization as a strategy is closely related to innovation and speed of relevance cycles which may be an issue in the future. Much strategic cyberspace infrastructure and capability has been showing its age and increasing vulnerability and decreased capability in comparison to modern capabilities.

To develop and manage technologies and capabilities, many Programs of Record (POR) have been established within Major Commands or System Commands. These PORs take on the responsibility of development, acquisitions, funding, and fielding the technology to the warfighters. These PORs have decades of effort invested, contractual obligation, and huge funding lines tied to them. Some PORs have proprietary elements, contracts lasting for decades, and are applied at a macro level across the entire DOD, meaning the funding is in the billions of dollars. Many of the contractual obligations lock down the ability to change or adapt without a new contract, which takes tremendous time, potentially delaying delivery to the warfighter. If a technology becomes obsolete or less effective as compared to a new technology, the contracts keep the POR in place, despite better solutions being available. To close an entire POR and replace with a new one is extremely difficult for the government; it takes significant coordination, funding approvals, research, and development (R&D), and much time.

The DOD/government cyber strategies do not differentiate what technology would constitute a need for modernization, and what could continue in use for the next decade. Modernization requires direction, prioritization, and planning to prevent reactionary responses to technology changes, which may not succeed in addressing the unpredictable

and uncertain cyberspace future. Also, many contracts are solidified in such a way that they are applied at the time of agreement, but implementation might be several years after agreement, after which the cyberspace capability in question has become obsolete. To update or change the requirement is very difficult and usually incurs significant cost. Some of this is addressed in most recent strategies, which aim to “...examine the use of emerging technologies, such as artificial intelligence and quantum computing,” and “promote government identification and support to these technologies” (White House, 2018, p. 15), or “Leverage automation and data analysis to improve effectiveness” (United States Department of Defense, 2018a, p. 4). Yet the language of “examine” and “identification” found throughout the different strategies speaks to the discovery nature of the strategy rather than providing concrete goals for solution of those problems. Similarly, “leverage” and “effectiveness” speak to utilization of tools already created, rather than the aggressive, specific, and speedy implementation of tools to address general change, much less unpredictable or uncertain change.

Another major set of strategies to address UUCS is the heavy reliance on partnerships and information sharing. From the government side, information sharing is a major challenge due to cyberspace classifications, potential intelligence losses, and coordination, as has already been pointed out. From the industry perspective, information is a resource. The information on security posture, proprietary technology design, research and development, breaches, and data, etc., are resources and a source of revenue. Therefore, handing over data is tantamount to giving a resource away for free, which is not generally in industry’s best interest. This causes challenges in efforts that are specifically mentioned to increase information sharing, because there is little incentive for industry to participate, particularly if it means losing resources by the industry organization.

Also, of concern to industry is that an organization’s public disclosure of cyberspace breaches can expose it to risk unrelated to the breaches, such as bad publicity and legal issues, obviously not in industry’s best interest. Therefore, because of strategic ambiguity the sectors are likely to have difficulties in matching interests and adhere to the strategy in the same direction, potentially decreasing the effectiveness of the strategy. The provisions in the DOD/government strategies are not specific on how to execute the

partnerships or information sharing beyond “strengthening” (United States Department of Defense, 2018a, p. 8; United States Department of Defense, 2018a, p. 5). A formal process is not discussed or referred to, leaving the accomplishment of such information sharing ambiguous.

Considered cumulatively, the DOD and government strategies here are in a hierarchy and act as strategic communication to the rest of the government and subordinate units. The NCS is directive to the entire U.S. Government under the authority of the President, and the NDS is over the DOD. Military strategies are supposed to follow the hierarchy and clarify the strategy from the higher levels as they subordinate. Thus, NDS is over the DOD Cyber Strategy, which is over the USCYBERCOM Command Vision. As the layers decrease, the target audience is smaller and smaller, where generally only the subordinates of that department or unit are receiving or adhering to the strategy. The concern, therefore, is that those who may need to be directed by this strategy may not include the unified cyberspace strategy into their plans. Additionally, as discussed in Chapter II, strategy requires iteration, revision, and updating. If the strategy is not updated and those revisions supplied to the entire force, the strategic communication effectiveness becomes limited.

As a practical example, ‘unrelated’ domains from cyberspace, such as aviation, subsurface, supply or acquisitions, are not expected to dig into the subordinate cyberspace strategies (such as the DOD Cyber Strategy) which do not apply to their own domains, yet cyberspace is intimately integrated into every one of their capabilities and requirements. The question then arises as to whether personnel in these other domains know that they are expected to integrate cyberspace in accordance with subordinate strategy that they are never expected to see. Other domains are not explicitly directed to integrate cyberspace strategy by the higher-level strategies, which weakens the imperative to integrate cyberspace strategy into the other domains. This limitation has serious implications for UUCS, where vulnerabilities and changes become increasingly likely outside of the USCYBERCOM authority, potentially to the detriment of the DOD as a whole.

Due to the domain differences, roles and responsibilities become ambiguous. The missions of offensive cyberspace operations (OCO), defensive cyberspace operations

(DCO), defensive cyberspace operations-response action (DCO-RA), DOD information network operations (DoDIN Ops), not to mention programs of record and acquisitions, are not differentiated in any of these strategies, making vague the responsible entity for integration. Further information is required to determine that USCYBERCOM's missions generally cover OCO, DCO, and DCO-RA, as opposed to DISA's responsibility for DoDIN Ops, and other responsibilities include testing and certifying joint IT capabilities for interoperability (Defense Information Systems Agency, 2019).

As noted, there is ambiguity within each of the documents, some of it purposeful, some to enable the documents to be written more concisely, some to allow subordinate units to properly apply specificity (or improperly apply, as the risk may indicate), and some because the U.S. Government and the DOD are such large organizations that any specificity limits the potential for flexibility in the future.

Ambiguity and vague strategic nature allow for the strategies to be applied broadly without changing the strategy for the future, because the vague application supposedly applies to all situations. Yet, this broad application may not have the power to lead the organization in a defined way, and makes these strategies effectively “no-fail,” strategies, where any effort at all can be considered to have accomplished the entirety of the strategy without consequence or risk. However, the literature suggests that this methodology is not effective in the long run; rather, iterative changes and close monitoring of the effectiveness of the strategy are required.²⁴ The organization that does not take heed of changes and move with the changes is likely to fail.

Lastly, the quantitative analysis in this chapter demonstrates that some of these strategies do not define or include significant elements of strategy meant to clarify, strengthen, and implement the objectives. These missing elements include MOS/MOEs, Timelines, Feedback, or resource allocation (as previously discussed in the quantitative results section; see in particular Figure 3 and Figure 4). Leaving these very important components out of the strategy decreases the likelihood of accomplishment of the strategy at all (United States Government Accountability Office, 2013, p. 2). The subordinate

²⁴ Discussed in Chapter II.B.1.

employee reading the strategy may not be able to determine when the strategies should be accomplished, or how broadly the strategy applies. Without a measure of success, the subordinate commander, unit, or employee cannot declare completion or accomplishment of the strategy, making it an endless goal. Similarly, because the strategies are designed to direct immediate subordinates on a strategy, the more distant and low-level employees may not expect to implement the strategy when much of the implementation only exists at the highest levels. Without the differentiation, the entire force is not included in the strategic efforts. Instead they must go discover for themselves what the full answers might be, but do not have a guide as to where to find those answers. These are the kinds of considerations that should be addressed in the DOD strategies, according to the GAO report and affirmed by the research in this thesis.

Some would argue that these strategies are set so that subordinate commands clarify implementation for each unit. However, the risk exists that lower level units may ignore the strategy altogether if they believe it does not apply to them, when, in fact, cyberspace applies to everyone. When it is not easily discernable what actions should be taken at the high, low, or designated level, the impact of the strategy for the entirety of the department is weakened. The DOD is so broad, so diverse, and so varied, that increased direction and unity will bring the DOD better in line to address UUCS. Later analysis of the industry strategies will compare them to the DOD/government strategies in terms of these quantitative measurements and qualitative analysis to determine whether these questions can be answered, improved, or informed by industry.

b. Potential for the DOD to Improve on Current Strategies

The quantitative data presented at the beginning of this chapter demonstrates that there are some good advantages in the current strategies. Table 1 indicates that the average strategic sections are aimed at UUCS, either in a single aspect, (a 3 on the scale), second- or third- order effects (a 4 on the scale), or causing the change (a 5 on the scale), for a Combined Average of Unpredictable Change of 3.84. Table 2 and Figure 3 show that there are plenty of Action Items for the DOD to perform to implement these change-oriented

elements, and some MOS/MOE are present. Most of the included Timelines refer to a speedy capability in operations, rather than a timeline to accomplish the goal.

While the ratios in Figure 4 show that some elements of strategy are supported by MOS/MOE, Timelines, Feedback, and Budget Allocation, the average of Empty Elements shows that improvement can be made to better manage change. However, many of the strategies are designed to pass down to subordinates for action, leaving the change methods and other strategic elements to the subordinates. This leaves significant gaps for unified approaches to effect change from a current state to a future state, internally and externally, in areas such as leadership, employees and stakeholders, processes and resources. For example, strategies that demand “agility” and “speed” are not just a technological strategy but require a certain type of thinking that is not addressed, motivated, or championed. Instead, the expectation is that it will be executed, simply because it is written in the strategy.

That said, there is some attention to culture by the NDS, which states, “We must transition to a culture of performance where results and accountability matter” (p. 10). This is followed by a statement to empower leadership to take advantage of opportunities and to conduct effective stewardship of taxpayer dollars. Similarly, the DOD Cyber Strategy directs a culture change to include cyber awareness into the DOD. However, there is nothing that indicates how much cyber awareness is required, or how to measure the accomplishment of a culture of performance.

Disruptive Innovation theory, reviewed in Chapter II, helps illustrate the more holistic and complex challenges that DOD/government faces in anticipating and incorporating cyberspace change.²⁵ DOD strategies show that the DOD is acting as both an “incumbent” and as an “innovator,” with several individual strategic elements undertaking both direct innovation and modernization, and so evincing both types of organization that Disruptive Innovation Theory considers. With the modernization strategies, the DOD behaves as an incumbent organization, seeking to sustain performance

²⁵ See Chapter II.C.

with current technologies; with the innovation strategies, the DOD is seeking to improve performance by adopting innovative technologies.²⁶ Each of these roles has challenges. If the DOD is the incumbent for a certain technology, it must be aware of the comparative effectiveness of newer, innovative technologies with which it might compete. Similarly, if the DOD is the innovator, it must determine how to ramp up levels of performance that compete with current technology's use.

Disruptive Innovation Theory can also guide procurement and acquisitions processes. For incumbent organizations, the adoption of modern technology might occur in the "Late majority" or "Laggard" time frames to take advantage of the development of more mature and cheaper technologies.²⁷ For budget-minded organizations, this is an advantage: the cost of modernization is lower, and the technology has matured enough to reduce the number of problems that occur earlier in the development process. The U.S. Government, in its domestic role, may be well advised to lag behind private sector entities in the adoption of dramatic new technologies, allowing market-driven actors to "work out the bugs" before implementing new technologies at much larger scales.

However, for states competing with other states, adoption of new technologies might be more time sensitive. The disruption model demonstrates that incumbent organizations may not have the power to compete against organizations that utilize innovative technologies to improve their capabilities (if new technology adoption goes relatively smoothly). This is where the earlier adoption becomes more relevant, and the DOD and government may need to move adoption into the "Early majority" time frame. Security competition in international politics especially pressures governments toward early adoption of potentially "game changing" technologies which may still entail significant risks of performance failure or collateral impacts, due to the much greater risk of being on the short-end of a war-deciding technological innovation.

One historic example of this occurred in World War I, where in the early years of the war the German Navy was able to leap-frog 100 years of submarine development by

²⁶ See Figure 1 in Chapter II.C.

²⁷ See Figure 2 in Chapter II.C.2.

other nations and utilize the matured technology in innovative ways that the Allies, with heavy existing investments, were hard-pressed to emulate (A&E Television Networks, 2018; International Encyclopedia of the First World War, 2017). In this example, the German Navy was the innovator, and the Allies were the incumbents. As an incumbent response, the Allies were forced to modernize their navies, merchant forces, and submarines (Vergun, 2020). Similarly, much of cyberspace has been developed by the United States, and now other nations are making innovative advances based on that development.

Therefore, most of these DOD/government strategies could benefit from using the disruptive innovation model to determine whether circumstances call for a sustaining or innovative strategic approach, and whether to adopt new technologies earlier or later in their development. Using this model would at least guide decision makers in a unified methodology, rather than on instinct or by the ad hoc consensus of stakeholders that vary from element to element.

In sum, while some DOD/government cyberspace strategies already address UUCS, there is room for improvement. Strategies that include agility, speed, partnerships, and innovation are aimed strongly to address UUCS. However, because the DOD is so broad and varied, these strategies lack some of important elements, such as Timelines and Feedback. This decreases the unifying function of the strategy, pushing the execution to separate departments, commands, and units, which may not have all the experience, resources, expertise, or guidance to apply the strategy in a direction the leadership desires.

To bolster DOD/government strategies and make progress in areas open for improvement, the DOD can apply many of the best practices and lessons learned from industry. Chapter V presents and compares a range of private sector strategies to these DOD/government strategies in order to identify the practices and lessons offering greatest prospects for advancing the improvements to DOD/government cyberspace strategies discussed in this chapter and deepening its capacity for achieving UUCS.

V. ANALYSIS OF INDUSTRY STRATEGY

This chapter presents the results of the quantitative and qualitative methodology of the industry strategies sampled for this thesis. Quantitative results are followed by the qualitative, which are compared to the DOD/government results. Best practices and lessons learned from these results are presented for Chapter VI's conclusions.

A. EXPLANATION OF QUANTITATIVE RESULTS

Overall comparison of industry strategies to the DOD/governmental strategies demonstrated significant differences in measurements across most categories, but similarities in two important categories. Figure 5 summarizes these results.

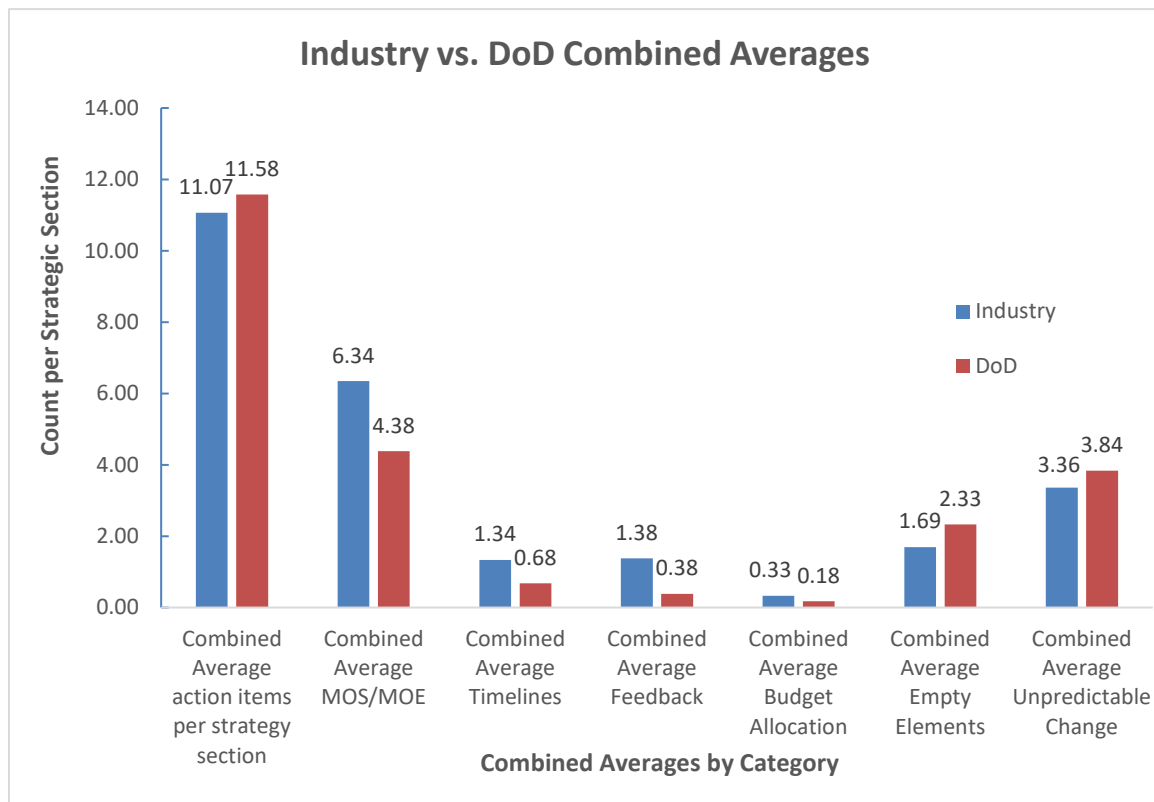


Figure 5. Comparison of Industry and DOD/Governmental Strategy Combined Averages

Perhaps most important for this thesis, the Combined Average Unpredictable Change category indicates that the DOD/government strategies address change at a higher ratio of 3.84 than does industry at 3.36. Given the conventional wisdom that private sector entities are more innovative, nimble, and forward-looking than government agencies, this finding is a surprise. This finding is discussed in more detail in Section A.1., below.

Regarding implementational measures, Figure 5 shows that in the Combined Action Items per strategy section category, DOD/government strategies yield slightly better results than industry strategies. The Combined Action Items measure shows that the DOD/government had more Action Items per Strategic Section at 11.58 than did the counterpart industry strategies at 11.07.

However, in the other categories industry nearly doubles the content when compared to the DOD/governmental strategies. Industry MOS/MOE average 6.34 to the DOD/government's 4.38. The industry at least managed 1.34 Timelines per strategic section to the DOD/government's 0.68 average. Similarly, industry had 1.38 Feedback mechanisms defined over the rarely mentioned DOD/government's Feedback mechanisms at 0.38. Finally, the Budget Allocations, while not significant for industry, are nevertheless utilized twice as often as the DOD/government. As directed in the NCS, best practices from partners, e.g., industry, are to be promoted and adopted (White House, 2018, p. 14, 26). Although adopting "best practices" involves more than emulation, increasing the other elements of strategy to match or exceed those of industry is a desirable first step.

Some of the results may have been skewed by the type of information, source information, and specificity provided by whatever the source information labelled as a strategic element. For example, the industry documents ranged from an average of approximately 23 Action Items to 4 Action Items for the total combined average of 11 Action Items per strategic section. Some organizations are much more specific, and others are more vague. The number of strategic sections also varied, from 5 sections total to 38, which is what motivated the ratios for more accurate and normalized comparisons, discussed in Figure 6.

1. Average Unpredictable Change

Table 3 compares the percentages at each rating level of industry and DOD/government strategies that are designed to address unpredictable change. As noted above, overall, the DOD/government strategies addresses change at a higher overall average than industry, 3.84 compared to 3.36. Interestingly, the DOD/government strategies have higher percentages in categories 4 and 5, and industry scored higher in addressing change in categories 2 and 3. This means that, in general, the DOD/government is tending to utilize strategies that rank higher and address deeper dimensions of change more than does the average industry counterpart. Specifically, recalling the definitions for the ratings presented in Chapter III, this means DOD/government strategies posture more to anticipate change that may include second- and third- order effects and to act proactively to shape future conditions ahead of the unpredictability; industry strategies incline more to respond to past change or anticipate only specific future changes.

Table 3. Number and Percentage of Strategies That Address Unpredictable Change for Industry vs. DOD/Government Percentage

Unpredictable Change	Industry Count	Industry Percentage	DOD/Govt. Count	DOD/Govt. Percentage
0	4	1.45%	1	0.80%
1	11	4.00%	10	8.00%
2	43	15.64%	13	10.40%
3	85	30.91%	20	16.00%
4	67	24.36%	46	36.80%
5	65	23.64%	35	28.00%
Total	275		125	

This finding does not mean that the DOD is better at change. Industry strategies may articulate or focus aspirations in such a way that the strategic section may not rank a 4 or 5. Moreover, being “better at change” also involves implementing strategy, not just envisioning it. However, this reinforces the general observation that the DOD tends to utilize strategies that are fairly well designed for change.

Overall, industry and the DOD/governmental strategies tend to address change strategies similarly, with individual strategies focused on innovation or new changes, and most either responding to a change in the technology/economy or posturing for the uncertainty the technology/economy presented. Many of the industry strategic sections that had a higher score are under a Research and Development (R&D) section, and the organizations that tended to have the highest average scores tended to represent the leading provider of the service or product, such as Intel Corporation (2019), Microsoft Corporation (2019), or Akamai Technologies Inc. (2019). The forward leaning nature is reflected in the strategy largely by specifically discussing innovation, creative solutions, and investment into the development beyond other organizations. The sampling of different organizations does show a spectrum of leading organizations to niche organizations, and the strongest strategies to address UUCS are the leaders in the industry.

2. Average Empty Elements

One of the results that most reflects concerns in the GAO reports is in the category of average empty elements. In this category, the figure indicates the average number of missing implementation elements per strategic section, including MOS, Timelines, Feedback, and budget items; this category is the only one for which a lower score is better. Figure 5 shows that industry strategies are missing an average of 1.69 and the DOD/government strategies missing 2.33 elements. On average, each industry category included at least one of every element, except for budget items.

Notably, for both sets of strategies, budget is the most common empty element. Some organizations are more forthcoming in the number of dollars invested in the strategy, such as Intel Corporation (2019), which included growth in a specific strategy in the millions of dollars. This growth strategy demonstrated high investment commitment in the technology that was being developed.

3. Discussion of Ratio Comparisons

Because of the variation in strategies, ratios are included as a single metric that normalized the comparisons, shown in Figure 6. First, the combined ratio of cyberspace specific strategies highlights that the DOD/government strategies are clearly more focused

on cyberspace than the sampled industry strategies. This difference can be explained by the sampling methods: research for industry strategies aimed to get non-technological organizations included in the study, whereas the DOD/government samples are primarily cyberspace specific strategies. The minimum cyberspace specific ratios represent the organization that included cyberspace strategy the least, which is the NDS at about 41% and Tesla at 9%. This may be explained by the sampling methods again, where the strategy sampled for Tesla, which is an organization lauded for its advanced technology, is not one that is focused on cyberspace. The other industry organizations that had low cyberspace ratios were Marsh & McLennan Companies (2018), Pebble Beach Community Services District (1997), and Bank of America (2020), each of which had a cyberspace specific ratio for their strategic sections of under 20%.

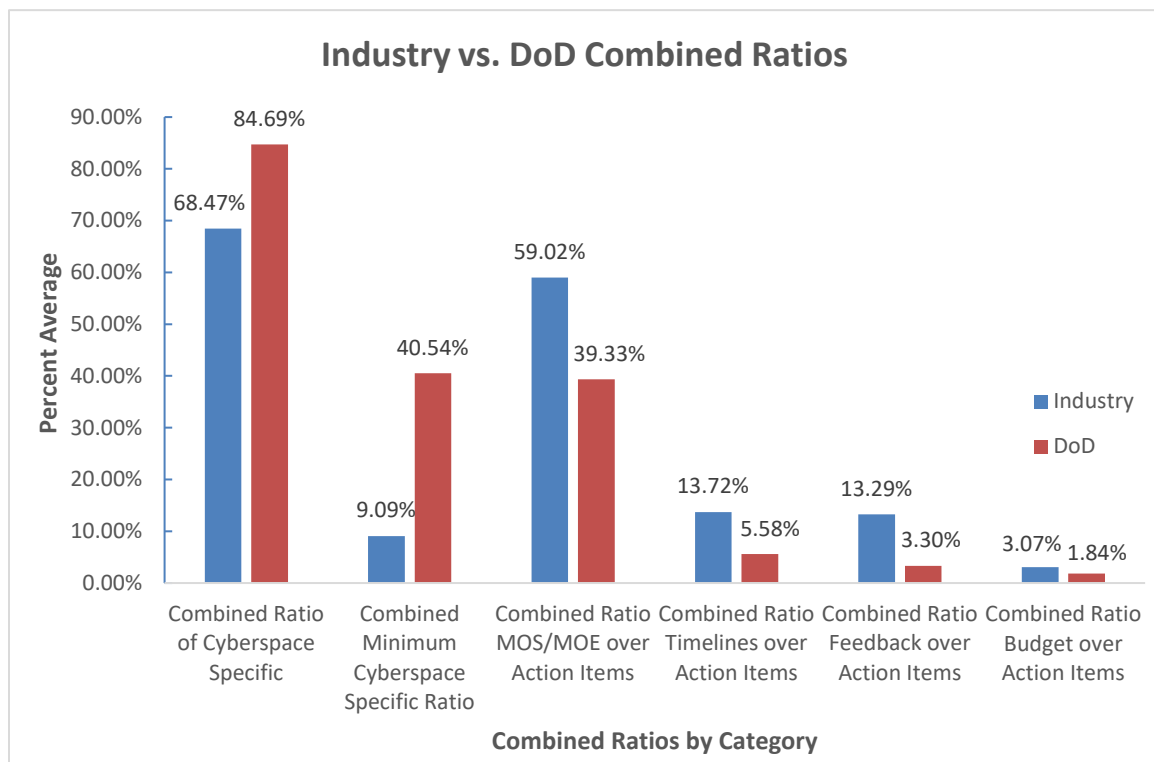


Figure 6. Comparison of Industry and DOD/Governmental Strategy Combined Ratios

The remaining ratios represent a percentage of how many implementation elements within the category are directly associated with the Action Items discussed. This measure indicated that nearly 60% of industry strategy Action Items are associated with a MOS/MOE, as compared to about 40% of DOD/government strategies. Nearly 14% of industry Action Items included Timelines, as compared to not quite 6% of DOD/government Action Items. Feedback mechanisms presents a more skewed 4-to-1 difference in ratios. Finally, only about 3.1% of the industry Action Items included specific Budget Allocation or prioritization, as compared to the DOD/government 1.8%. Each ratio demonstrates a significant difference in how industry operates its strategy by including nearly double the elements per Action Items, as compared to DOD/government.

These results underscore the concerns in the GAO reports, and represent a significant area of improvement for the DOD in cyberspace strategy. As a best practice, the ratio may be a better indicator to follow for the DOD/government to improve its strategies, where shorter or longer strategies simply apply a ratio to attain the proper number of supporting strategic elements to match the industry's best practice ratios.

B. EXPLANATION OF QUALITATIVE RESULTS

The qualitative results for industry strategies yield a few observations. In comparing the spectrum of strategies, the larger organizations tended to have similar strategies to the NDS, with broader application and less specificity. This means that there are generally fewer sections, seven or eight, for the entire presented strategy, and like the NDS each used language that tended to have more ambiguity in tone. Some of the smaller and more niche organizations had significantly more sections—twenty or more—which also tended to have more precise language.

Additionally, the technology/cyberspace organizations had significantly different strategies than the non-tech companies, which is reflected in the ratio of cyberspace specific strategies. Of note, even the organizations which included cyberspace the least still had some reference to embracing technology, and the majority did better than the NDS's 40.5% cyberspace specific ratio. A possible explanation for these trends is that specificity for the larger organizations is found at lower levels or departmental strategies, mirroring

how the DOD Cyber Strategy and USCYBERCOM Command Vision carry more specificity than does the NDS for cyberspace. These lower-level industry strategy analogues were not available for the research for this thesis. Despite the effort, each of the nearly fifty organizations approached at the RSA 2020 conference claimed that the desired cyberspace-specific strategy is proprietary and would not be available publicly (similar to the DOD, which also has a classified portion of its strategy). Obtaining lower-level strategies and proprietary strategies to compare to the structure provided in the layered DOD strategies is a potential future research opportunity.

Beyond these overarching observations, qualitative review of the industry strategies suggests a number of key lessons that could be incorporated into the DOD/government strategies to improve their capacities to prepare for and manage uncertainty and unpredictable change. The remainder of this section explores these learning opportunities.

1. Key UUCCS Lesson Learned

Possibly the most important lesson learned from industry for UUCCS is how industry focuses on integration of its *systems*. The DOD/government strategies already emphasize integrating cyberspace into operations. As a broad, DOD/government-wide strategy, this is absolutely imperative. However, industry's focus on cyberspace itself demonstrates that integration of systems, for cybersecurity, management, analysis and assessment, oversight, and insight into the status of cyberspace systems, is high in industry's strategic priority list.

DOD strategies rely heavily on integrating cyberspace into other domains, but none point to interoperability between systems. Interconnectivity, collection of disparate data, centralized control, and detection for AI capability, all require integration of systems. There is no strategy to deal with legacy systems that will not be replaced in modernization efforts. Additionally, there is no direction for who is responsible for integration of systems that are not a network specifically, which falls under the DoDIN.

This is contrasted greatly with industry, of which many organizations aim to integrate variate systems for central control, monitoring, and vulnerability analysis. Symantec Corporation (2018), McAfee LLC (2020), Palo Alto Networks Inc (2019),

Splunk Inc (2020), Edgescan (2020) and others either provide capabilities to use in addition to current infrastructure, are tailored for the customer, or can integrate into the infrastructure, not to mention build from scratch. Most include some method of vulnerability assessment, reporting and management, as well as ongoing updating and intelligence reports that keep the user apprised of threats. This specific strategy is one that directly addresses UCCS and has been neglected in the overall DOD strategy.

While challenging, a strategy of system integration would increase the capability of the DOD/government to address UCCS, particularly for cybersecurity and agility. For example, many systems are aging, proprietary, and disconnected from each other, requiring laborious manual assessment to manage the highly technical analysis required to discover malicious actor activity. If systems are centrally monitored and managed, malicious actor activity would be more readily identified across the disparate systems, as central control allows for experts to mitigate and make decisions faster. Centralizing and managing such systems would provide increased oversight and management to the warfighters. Having a central management system increases ability to be agile as well, where issues are more quickly realized and can be mitigated faster than disconnected and manual systems would. This also addresses the increasing sophistication of malicious actors, where centralized management and monitoring allows for greater visibility to mitigate and respond to threats.

The NCS has laid the groundwork for such a strategy, centralizing management of the government's cybersecurity efforts under DHS, but this specifically excludes the DOD and the IC (White House, 2018, p. 6). This also includes assessment and review of Federal contractor cybersecurity risk management and practices (p. 7). The DOD Cyber Strategy phrases this differently to "set and enforce standards for cybersecurity, resilience, and reporting; ... when requested and authorized, to provide direct assistance, including on non-DOD networks, prior to, during, and after an incident" (United States Department of Defense, 2018a, p. 3). Advancing cyberspace strategy for the excluded DOD and IC that corresponds to the NCS's centralizing strategy, rather than remaining in a "responsive" posture, may be the next step for the DOD to address UCCS.

2. Other UUCS Lessons Learned

The strongest industry strategies aimed to be proactive, integrated, automated, multi-sourced, and innovative with specified purpose. Many of these used artificial intelligence, machine learning, big data, and cloud solutions to automate their processes and information. A few examples are included here:

- Splunk Inc. (2020) claims to be able to take in any type of data from any source for analysis, which is a very aspirational and highly technical claim.
- Intel Corporation (2019) claims to be a leader in their field, and the innovative strategies reflect their leadership status. As one of the most established organizations in the sample group, longevity and experience are reflected in the MOS/MOE, Feedback mechanisms, Timelines and budget goal metrics which are all clearly incorporated and established into the strategy.
- Akamai Technologies Inc (2019) uses its control over its vast network to correlate data that would not be connected otherwise. Their products are designed to detect change, evaluate, and respond automatically throughout their services and products.
- McAfee LLC (2020), FireEye, Inc (2019), Symantec Corporation (2018), Security Compass (2020), Cisco (2019), and other companies heavily rely on automation to push their information-value to the stakeholder. Many of these solutions are customized and integrated to include multiple systems, networks, and cyberspace operations, as well as presented in such a manner to make management centralized and easy for the organization.
- Palo Alto Networks Inc. (2019) centralizes control and integrates every acquisition into everything it does. It is specific in the technologies acquired, what it brings to the product, and how it is integrated into every solution and every system.

- Many organizations include R&D strategies, of which the best include the purpose and goal of the research and investments that reflect the commitment to that goal.

a. Automation and Data Analytics

As mentioned in Chapter IV, the focus for the NDS and DOD Cyber Strategy on automation are to gain military advantage, identify malicious cyber activity, and improve defensive posture. This focus misses out on many automated capabilities available in the private sector, such as medical advances, HR processes, maintenance life cycles. Many forms of automation are designed to comb through data faster than a human can, and many organizations present the capability to apply to a spectrum of problem sets. These included: Splunk Inc (2020), Security Compass (2020), McAfee LLC (2020), Ixia (2016), and others. As mentioned, Splunk specifically mentions the capability to incorporate any type of data from any source. This could apply very specifically to the DOD, whose acquisitions have come from many variate organizations that may not integrate systematically with each other and have proprietary information designs.

Additionally, cloud services are heavily emphasized, which is only mentioned once in the DOD Cyber Strategy (p. 6), and nowhere else in the other DOD/government strategies. These are not only storage, but computing solutions, networking, and data analytics capabilities. Many large-scale capabilities are being moved to the cloud because the amount of processing, tools, and data managed and required are so much larger and require more coordination and connection than individual organizations can produce or utilize independently. Industry is heavily emphasizing solutions and services in the cloud, which is a reasonable expectation to have addressed specifically in the DOD/government strategies. Particularly because of inherent security and control risks involved in cloud services, in addition to anticipation of costs and storage control, future strategy needs a high-level unifying strategy that guides use of cloud services. This is also an opportunity to demonstrate where the DOD has applied its own strategy, by highlighting the JEDI contract with Microsoft or Amazon (Stewart, 2020).

b. Agility, Speed with Automation, Standardization, and Compliance

Many examples of agility include automation. Speed generally is related to automatic Feedback systems that incorporate data to push back out to customers. Systems achieving both agility and speed tend to include some mechanism, such as a dashboard, alert, or report, for diagnosing issues, vulnerabilities, and potential threats, and for integrating intelligence from other sources. Agility, if not mentioned by name specifically, is usually in reference to adaptation to the environment in relation to a cyberspace threat. The actions taken are usually integrated with other data, tracked, and performed at speed. The word “rapid” is used regularly across many organizations and is regularly used as a measure of effectiveness and as a timeline for achievement. Key to this observation is significant use of automation, where the system could adapt on its own, or changes realized outside the system could be updated automatically, seamlessly, and transparently without waiting for an administrator to do the work manually. These capabilities are then associated with a decreased burden on the customer’s workforce, while still working at the speed of the machine. Nearly every industry strategy studied included some measure of speed, agility, and automation throughout their systems.

Change in regulations is acknowledged in a few organizations, which support the customer by determining applicability of the regulations to the customer and working to bring the customer’s systems into compliance. The NCS notes several times that the government must adhere to its own regulations and adopt best practices that are required of the private sector. It is reasonable to expect ongoing changes and updates with government regulation and changes in standardization to be reflected in the strategy. It can be argued that the language in the NDS, which refers to “frequent modular upgrades (p. 10),” covers this reality. However, compliance and standard changes can require significant or costly technology overhauls and might be larger than a modular upgrade. This becomes a risk that tends to be addressed on a case-by-case basis.

c. Strategic Specificity

Many of the organizations included examples of successful efforts and major products to highlight their focus. This specificity made the strategy clearer as to the

direction the organization is heading and where resources are prioritized. While this may not be directly addressed at UUCCS, the bolstering of all strategy is of benefit. For example, Intel Corporation's report (2019) announced a significant shift to a type of memory chip and represented the dollar amount invested in the development for the past several years. Several organizations provided the estimated millions of dollars invested in Research and Development, with several initiatives defined to have a specific purpose. Strategies of Security Compass Inc. (2020), Bank of America (2020) and a few others were very specific in efforts to incorporate Feedback mechanisms into productivity and discussed precisely who and how that mechanism functioned. Multiple organizations discussed their acquisitions or divestiture of smaller companies with clarification on what this brought to the overall strategy. Most of the acquisitions are to further develop a product or service, and some divestitures are pure business capital decisions.

The more specific strategies also used percentages as goals. These included achievement of previous goals as an orientation and a MOS/MOE, as well as a goal for the future. General Electric Company (2019) demonstrated an achievement of a specific growth goal and how much the goal is surpassed as a measure of effectiveness (p. 4). These measures of success clearly demonstrated strategic metrics utilized by the organization. Similar metrics utilized within the DOD/government may bolster cyberspace strategy more effectively if included.

Some of the strategies are differentiated to where the capability, service, or product pushed or pulled the daily work. Some strategies provided a packaged and standardized system, such as McAfee's (2020) security application. Others offered capability or product that is standardized or customized, such as Optimal IDM (2020) to allow the customer to utilize the capability as desired. This pushed the daily workload to the customer. Others are designed to act as a service that performed the work on behalf of the customer by pulling data and Feedback from sensors, processing and analyzing the information and pushing results as value to the customer. Several, such as the aforementioned McAfee, had both capabilities depending on the customer. These strategies are well defined and demonstrated the goal and application of the expertise of the organization.

Only a few strategies included a differentiation between what leadership is going to do versus what other employees are expected to do. General Electric Company (2019) is one such organization that historically has emphasized leadership, and included a large section discussing new efforts within the leadership to improve the overall organization. This included collaboration at a high level, as well as leaders working with subordinates. Cisco (2019) included a significant section that highlighted its leadership and their capabilities. The annual report used is not their official business strategy but reflected the values and emphasis of the organization.

The NCS highlights risk management and assessment throughout the document, and the NDS and DOD Cyberspace strategies refer to a transition to a culture that takes measured risks. The USCYBERCOM Command Vision however has an entire section dedicated to risk management, with specific and real vulnerabilities and how the organization would approach it. To compare to industry, Bank of America (2020) emphasized a specific risk management framework at the *beginning* of its strategy to encompass, repeat, and frame the remainder of its strategy. Cisco (2019) established its own framework and standardized its use in its organization. A similar approach is not visible in the DOD/government strategies.

Change Management practices are specifically mentioned by Tesla (2019), acknowledging the science of change. Similarly, many organizations like Microsoft Corporation (2019) included strategies that updated business processes. The DOD/government strategies do include sections about updating business practices and best practices, and so are similar. In the future, the field of CM research and other examples of CM in industry may provide specific models to adapt the DOD cyberspace strategy for UUCCS. This would likely require more in-depth research into large organizations for implementation efforts to compare global and disparate element integration and use those best practices.

Overall, the observed specificity within the industry strategies is higher than the DOD/government strategies. This specificity provides stronger direction to decision makers, managers, and employees in utilization, acquisition, partnerships, and Timelines. Additionally, customers, investors, and partners have a better idea as to what to expect

from the organization based on the strategy, increasing the trust required to solidify such a relationship.

d. Strategic Communication

Much of the data analyzed represented a form of strategic communication, either to stakeholders and investors, customers, or reflected the internal strategy for the organization. Most are obtained via annual reporting, in an investor's annual report or SEC filing Form 10-K. Language specific to that year's activities demonstrated at least some effort to revisit the strategy by the organization, and in many cases clearly demonstrated the past year's success and the future year's goals. When changing circumstances compel an organization response, a change in the published strategy communicates to the stakeholders the direction of the organization. Updating the strategy more iteratively and publishing regularly demonstrates a higher commitment by industry to strategic communication compared to the less frequent updating of DOD and government strategies, particularly given the rate that cyberspace changes. The literature reflects industry's push toward iterative changes,²⁸ which more closely reflects the cycle of change. At the time of publication of this thesis, the DOD/government cyberspace strategies had not been updated since 2018, a period of two years and counting, though some high-level government efforts, such as the Cyberspace Solarium Commission (King and Gallagher, 2020), show movement toward updating the cyberspace strategy.

e. Partnerships

Many industry partnerships mentioned in the strategies have a specific purpose. Some are explained as contractual relationships, as part of the supply chain, or as compliments to capability. Some of the partnerships mentioned are clearly part of an acquisition strategy. Some of the partnerships are designed to outsource certain types of work, including customer service, marketing, data sources, or as a major consumer of the organization's product to create a higher-level product.

²⁸ See Chapter II.B.1.

Additionally, some partnerships, such as those of FireEye (2019) and Apple Inc (2019), are discussed as “ecosystems,” apparently associated by mutual benefit rather than by contract. When defined further, these included customers who interacted with each other as well. Splunk Inc. (2020) is particularly specific that its customizable product is designed to integrate third-party products and provides multiple forums for support from these third-party designers, customers, and customer service. This example is the most specific of all case studies included and demonstrated a particular effort to include outside entities as part of corporate strategy. Integration of customers-assisting-customers and third parties contributing to each other’s products through their forums goes beyond standard customer service.

While the government’s efforts at partnerships in strategy have some purpose attached, thinking of some partnerships as “ecosystems” as described by these industry organizations may provide more best practices to adopt and include in later iterations of DOD/government strategy. This model may be especially useful in providing definitions of who is a strategic partner and who might be excluded for engagement at a lower level.

f. Innovation

In a resource constrained environment, where there is not enough time, money, manpower or expertise to attack all problems, innovation to solve key problems would be particularly useful, as opposed to a more open-ended imperative to innovate for agility. Technologically, clarification for innovation that might guide resource prioritization is left rather open ended. Despite the aspirations to cause change, the sheer massive size of the DOD and its traditional, bureaucratic, and repeatable processes are generally resistant to change such as structural organization changes, experimentation, and risk taking. Many organizations, like Intel Corporation (2019) and Splunk Inc (2020), are specific in what their innovations are designed to do, how much they invested resources and expertise, and who is involved in the development. A good example is Akamai Technology Inc’s (2019) proprietary partnership with the Massachusetts Institute of Technology (MIT). For the very disparate DOD, composed of several developmental agencies and commands, specifying roles and responsibilities to increase coordination and interoperability, as well as connect

non-R&D commands to the authority, would strengthen the strategy. This strengthening would certainly emphasize UCCS more, bringing R&D efforts to the forefront and providing direction for the rest of the DOD to support those efforts and requirements.

VI. CONCLUSION ASSESSMENT, LIMITATIONS, AND RECOMMENDATIONS FOR FUTURE RESEARCH

A. CONCLUSION ASSESSMENT

This thesis has asked: “What lessons can the DOD realize from private sector strategies for innovation and change to build better and more robust multi-stakeholder cyberspace change strategy that anticipates uncertainty and unpredictable future cyberspace change?” The basic answer to this question is: there are numerous lessons.

Chapter II discussed the absence of literature to answer this question directly. Accordingly, the thesis collated several fields of related work and explored private sector experience to generate lessons-learned and recommendations to the DOD. The preceding two chapters presented, in some detail, the range of findings from this research and the specific lessons they yield. Following are concluding highlights of lessons learned.

1. Literature Contribution

The literature provides a wealth of general information on translating private sector strategy to public sector strategy, including major elements in change management and disruptive innovation theory. Particularly interesting is the disruptive innovation model adapted to include the adoption curve, which may provide a model for use in UUCCS and predictive methodology. While reflecting change, there is a balance between the necessity to adapt and the smaller likelihood that innovative changes will disrupt fundamental systems completely or overnight. Literature guidelines include regular iteration of strategy at the pace of change, also noted within the NDS. Specific literature recommendations include utilizing small teams to iterate solutions quickly until they can be applied more broadly across an entire organization.

2. Industry Specificity Contribution

Based on the quantitative analysis, while DOD/government strategies are laudable in their anticipation of change, industry’s strategies include nearly double the number of measures of effectiveness/measures of success, Timelines, Feedback mechanisms, budget

contributions, and the corresponding ratios as compared to the DOD/government strategies. These measures of implementation corresponded to a higher level of specificity as well, decreasing ambiguity. Additionally, methods that adhere to principles of Change Management, particularly leadership direction, provide clearer bearings and expectations in the organization. To build better and more robust multi-stakeholder strategy, lessons learned in this area will improve strategy overall, which will also improve UCCS.

3. Integration between Systems, Not Just Operations

Many of the sampled strategies emphasized integration between systems even more than between operations. For UCCS in the DOD, this emphasis is lacking, glimpsed only in providing direction to integrate cyberspace into broader operations. Using the lessons and emphasis by industry in integration would likely provide better direction for a future DOD cyberspace-specific strategy. This kind of strategy would help address UCCS by centralizing vulnerability assessment, reporting, management, and ongoing updating of intelligence reports that keep the user apprised of threats. As sophistication of malicious actors has increased over time, the capability to better monitor, mitigate, and respond to threats has become more relevant. Centralizing management allows visibility and insight into systems, and enables agility of action, because the knowledge of the system and threats is better than the current manual and disassociated systems.

4. Agility and Speed with Automation

Many industry strategies include agility, adaptation, or speed as part of the product, service, or capability. In contrast to DOD/government strategy, which mentions speed and agility a few times or in an introduction, agility, adaptation, and speed is regularly repeated throughout each strategic section. This repetition highlights more specifically where agility, adaption, or speed is to be applied. Specific capabilities might take time to develop, so categorizing them carefully helps clarify the objective. Most of the key agile, speedy, and adaptable capabilities and services are automated to rapidly update the stakeholder. This automation significantly increases the scale at which information, capability, and security is delivered. Specifying where to use speed, adaptation, speed, and automation in

each strategic section helps UUCCS by increasing focus for each objective, rather than utilizing a broad, document-wide application.

5. Partnerships

The best partnerships are well defined and included a purpose for the partnership. The most specific included what level the partnerships exist at, either contractual, supply, an ecosystem of support, channels of sales, distribution, training, or marketing, with some performed by the leaders of the organization, and others performed by employees. These strategies demonstrated what the goal of the partnership is, what benefit is garnered, and how it is currently utilized.

6. Strategic Communication

Because of the public nature of industry strategies, they are addressed to multiple stakeholders, including employees, customers, investors, and partners. They show where the organization has come from and where it is going and do so in each strategic section. While individual organizations may have only addressed the data source to a specific audience, these reflected the organization's strategy presented to other stakeholders. Both the literature and demonstration by these organizations agree that regular iteration and revision of the strategy in response to change, all strategically communicated to stakeholders, increased the strength of the strategy.

These specificities lend strength to and decrease ambiguity within industry strategies, all of which could be used to improve UUCCS.

B. LIMITATIONS: SUBJECTIVE AND OBJECTIVE DIFFERENCES IN ABSTRACTION OF STRATEGY

The primary caveat of the findings of this thesis is that the research required analytical judgments regarding the meanings and contexts of the source documentation. Both the quantitative and qualitative assessments of DOD/government and industry strategies required interpretations of specific narrative content reflecting divergent purposes and functions. In particular, the coding methodology to distill strategy quantitatively is sufficiently abstract to permit comparative numerical observations but

may not represent the effectiveness of the organization's strategy by doing so. Language could have been concise or purposely vague to allow flexibility for subordinates, which would have changed the abstract measurements.

In the industry strategies in particular, much of the data is addressed to potential customers or investors, and so required some extrapolation of strategy from the sales pitch. The assumption is that if a capability claims to accomplish something, it is part of a development strategy—otherwise, it would not have been developed. Because the data are not always from the organizations' official strategies, which may vary from published material, results may have been skewed from the real strategy.

Quantitative assessments attempted to consistently measure the same data points, but necessary judgments regarding the definitions, language application, and translation to the framework leave room for interpretation. Because of the subjective abstraction process, other researchers repeating this process might generate different results. The thesis reports all the core data in Appendix B in order to promote efforts to replicate the study. Such additional efforts would demonstrate either the robustness of the findings or the sensitivity of the findings to these interpretative issues, either of which would productively build on the knowledge generated herein.

C. RECOMMENDATIONS

1. Future Research Comparing More Similar Strategy Types

Further research is recommended to compare the classified DOD cyberspace strategies to industry proprietary strategies. Not all the industry case studies are focused on cyberspace and contributed fewer lessons learned. Focusing on cyberspace leaders' strategies may also contribute higher quality lessons. Additionally, many industry strategies referenced separate strategies for "business," "marketing," "sales," "production," etc., pointing to strategic documentation beyond what is made publicly available. Further research that compares a proprietary cyberspace strategy to the counterpart DOD strategy might provide further insights.

Also, focusing further into organizations designed for cyberspace, and performing a deeper analysis on the effectiveness of proposed strategies, might provide additional

lessons or insights not discovered here. The implementation could also be included, particularly regarding how effective a broad and disparate organization is at incorporating its own cyberspace strategy.

2. Use the Literature for Unified Models

Change management and disruptive innovation theory provide models and metrics already thoroughly researched. Bringing these into UCCS in a unified manner across the entire organization would standardize efforts and allow for proper measurements against the strategy to be performed for proper Feedback and improvements. Disruptive innovation theory combined with the adoption curve as presented by Nunes and Downes (2019) may provide an excellent hybrid model for product improvement and comparison to other nation states for R&D efforts and acquisition prioritization.

3. Develop an Integrated Cyberspace Systems Strategy

Industry best practices are to centralize management, monitoring, and assessment of systems. The DOD lacks a strategy to do so, emphasizing integration into operations, rather than systems. As a natural evolution, simultaneous strategies that integrate into operations, update legacy systems, integrate systems and centralize their control are the most important best practices recommendations from this research.

4. Increased Specificity

DOD/government cyberspace strategy aspires to integration between systems, not just operations, partnerships, innovation, agility, speed, and automation. But industry can contribute specificity to increase the strength and momentum of those strategies.

5. Iteration and Strategic Communications

The National Defense Strategy (2018) aspires to increase experimentation and calculated risk-taking (p. 7). More frequent and faster iteration of the strategy allows for Feedback to adjust the course and learn from less than optimal and risky decisions. This iteration must be then promulgated to the disparate and global force that applies these strategies to promote unification of effort. Iterations should demonstrate success and

improvement across an entire force, which would allow current status to be observed and would permit incorporation of lessons learned and encourage progress.

APPENDIX A. DATA SOURCES

Appendix A contains the sources utilized for the quantitative and qualitative analysis of this thesis. Citations that also appear in the text are re-referenced in the List of References.

Akamai Technologies Inc. (2019). *Akamai annual report 2019*. Investors Investor Relations | Akamai. <https://www.ir.akamai.com/static-files/569d1024-6d2c-4fdd-bfd5-9ae3d5c85eab>

Apple Inc. (2019, September). *Apple Inc. form 10-K*. SEC.gov. <https://www.sec.gov/Archives/edgar/data/320193/000032019319000119/a10-k20199282019.htm>

AT&T. (2020, February 20). *AT&T Inc. form 10-K*. Sec.gov. <https://otp.tools.investis.com/clients/us/atnt2/sec/sec-show.aspx?Type=page&FilingId=13936660-139387-206135&CIK=0000732717&Index=11100>

Bank of America. (2020). *Bank of America's strategy of responsible growth*. bankofamerica.com. Retrieved March 24, 2020, from <https://about.bankofamerica.com/en-us/who-we-are/our-strategy.html#fbid=Lmh6FmRAfD7>

BlackBerry Ltd. (2019). *BlackBerry analyst summit 2019*. BlackBerry Official Home Page – Security Software & Services. <https://www.blackberry.com/content/dam/blackberry-com/Documents/pdf/financial-reports/2019/q4fy2019/analyst-day-2019-strategic-and-financial-sessions.pdf>

Cisco. (2019, October). *2019 Annual report: Defining the future of the internet*. cisco.com. https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2019.pdf

Edgescan. (2020). *Effective, scalable, #fullstack vulnerability management* [Brochure]. BCC Risk Advisory Ltd.

FireEye, Inc. (2019, December 31). *FireEye, Inc. form 10-K*. Investor Relations | FireEye. <https://investors.fireeye.com/node/14176/html#sEBF126F99B3E578498E9DBDBC72EEF75>

General Electric Company. (2019). *GE 2019 annual report*. ge.com. https://www.ge.com/investor-relations/sites/default/files/GE_AR19_AnnualReport.pdf

- Intel Corporation. (2019). *Intel 2018 online annual report*. intel.com.
<https://intel2019or.q4web.com/Y2018/default.aspx#>
- Ixia. (2016, December 31). *Ixia form 10-K*. SEC.gov. <https://www.sec.gov/Archives/edgar/data/1120295/000112029517000006/a2016q4form10-k.htm>
- LookingGlass Cyber. (2020). *Intelligence-driven risk mitigation | understand, detect, and block cyber threats, in real-time* [Brochure].
- Marsh & McLennan Companies, Inc. (2018, December 31). *Marsh & McLennan Companies form 10-K*. SEC.gov. <https://www.sec.gov/Archives/edgar/data/62709/000006270919000010/mmc1231201810k.htm>
- McAfee LLC. (2020). *About McAfee*. McAfee | Security Solutions for Cloud, Endpoint, and Antivirus. Retrieved April 17, 2020, from <https://www.mcafee.com/enterprise/en-us/assets/fact-sheets/fs-mcafee-fact-sheet.pdf>
- Microsoft. (2019). *Microsoft 2019 annual report*. microsoft.com.
<https://www.microsoft.com/investor/reports/ar19/index.html>
- Optimal IDM. (2020). *Optimal IdM: Who we are*. optimalidm.com. Retrieved April 16, 2020, from <https://optimalidm.com/why-optimal/>
- Palo Alto Networks, Inc. (2019, July 31). *Palo Alto Networks, Inc. form 10-K*. investors.paloaltonetworks.com. <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001327567/6b9031d3-1bed-4db4-a694-aaa7811418a1.pdf>
- Pebble Beach Community Services District. (1997). *Pebble Beach Community Services District long-term goals and objectives*.
- Security Compass. (2020). *About SD elements: The solution to the development devil's choice. Go fast. Stay safe*. Retrieved April 14, 2020, from <https://securitycompass.com/sdelements>
- Splunk Inc. (2020). *FY2020 annual report and proxy statement*. Investor Relations | Splunk Inc. <https://investors.splunk.com/static-files/993ab50b-19d1-44b0-826b-071d82c77d87>
- Splunk Inc. (2020). *Splunk vision*. Splunk.com. Retrieved April 24, 2020, from https://www.splunk.com/en_us/about-us/business-strategy-and-vision.html
- Symantec Corporation. (2018, March 30). *Symantec Corporation form 10-K*. SEC.gov. https://www.sec.gov/Archives/edgar/data/849399/000119312518309091/d573170d10k.htm#osl573170_1
- Tesla. (2019). *Tesla impact report*. tesla.com. https://www.tesla.com/ns_videos/tesla-impact-report-2019.pdf

United States Department of Defense. (2018a). *Department of Defense cyber strategy summary 2018*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

United States Department of Defense. (2018b). *Summary of the 2018 national defense strategy of the United States of America: Sharpening the American military's competitive edge*. <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>

U.S. Cyber Command. (2018). *Achieve and maintain cyberspace superiority; Command vision for U.S. Cyber Command*. Home USCYBERCOM. <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>

The White House. (2018). *National cyber strategy of the United States of America*. Whitehouse.gov. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. DATA SPREADSHEETS

Appendix B includes the assessed and collated data used for analysis. The first tables break the Averages and Ratios used to collate data per sector. This is followed by the collated data tables, and finally the raw data tables per strategic section.

Analysis of the DoD/Government Strategy Table of Averages and Ratios												
Organization/ Document	Average action items per strategy	Average MOS/MOE	Average Timelines	Average Feedback	Average Budget Allocation	Average Empty elements per strategy	Ratio Action items to MOS/MOE	Ratio Action Items to Timelines	Ratio Action Items to Feedback	Ratio Action items to budget	Average Unpredictable Change	Ratio of Cyberspace Specific
National Defense Strategy	10.1081	4.7027	0.5135	0.1892	0.5676	2.32	46.52%	5.08%	1.87%	5.61%	3.89	40.54%
National Cyber Strategy	8.9286	3.1964	0.1786	0.2857	0.1091	2.66	35.80%	2.00%	3.20%	1.22%	3.1786	98.21%
The DoD Cyber Strategy	8.6087	3.7391	0.6957	0.3913	0.0435	2.22	43.43%	8.08%	4.55%	0.51%	4.1739	100.00%
USCYBERCOM Vision	18.6667	5.8889	1.3333	0.6667	0.0000	2.11	31.55%	7.14%	3.57%	0.00%	4.1111	100.00%

Analysis of the Industry Strategy Table of Averages and Ratios												
Organization/ Document	Average action items per strategy	Average MOS/MOE	Average Timelines	Average Feedback	Average Budget Allocation	Average Empty elements per strategy	Ratio Action items to MOS/MOE	Ratio Action Items to Timelines	Ratio Action Items to Feedback	Ratio Action items to budget	Average Unpredictable Change	Ratio of Cyberspace Specific
Del Monte Forest Conservancy Strategic Plan	6.1667	3.7500	2.0000	2.2500	0.1667	1.2500	60.81%	32.43%	36.49%	2.70%	2.25	16.67%
Ixia Annual Report 10K 2016	10.6154	4.0769	0.6923	0.7692	0.2308	2.2308	38.41%	6.52%	7.25%	2.17%	4.00	76.92%
Marsh & McLennan Companies, Inc. 10-K 2019	6.2500	1.5000	0.0625	0.0000	0.0000	3.4375	24.00%	1.00%	0.00%	0.00%	2.63	18.75%
Intel 2018 Annual Report	10.8235	5.1765	0.8824	1.8235	0.6471	1.4118	47.83%	8.15%	16.85%	5.98%	4.18	58.82%
Bank of America	8.0000	6.0000	0.8571	1.0000	0.2857	1.4286	75.00%	10.71%	12.50%	3.57%	1.43	14.29%
Lookingglass Cyber	5.3333	2.3333	0.3333	0.0000	0.0000	2.8333	43.75%	6.25%	0.00%	0.00%	4.00	100.00%
Cisco	6.6250	4.3750	1.5000	1.0000	0.0000	1.8750	66.04%	22.64%	15.09%	0.00%	3.63	62.50%
Tesla Impact Report 2018	5.5455	4.1818	1.0909	1.7273	0.2273	1.5000	75.41%	19.67%	31.15%	4.10%	2.32	9.09%
Blackberry/Cyalance Annual Report 2019	6.0000	3.2857	1.1429	0.0000	1.0000	1.1429	54.76%	19.05%	0.00%	16.67%	3.00	85.71%
Edgescan	4.1667	2.2500	0.5000	0.5000	0.0000	2.2500	54.00%	12.00%	12.00%	0.00%	3.00	100.00%
Security Compass	9.4000	6.8000	2.2000	4.2000	0.4000	0.6000	72.34%	23.40%	44.68%	4.26%	3.40	100.00%
Microsoft Annual Report/10K	23.6667	14.5000	0.8333	1.1667	0.8333	1.6667	61.27%	3.52%	4.93%	3.52%	4.17	100.00%
AT&T 10K	7.2857	6.8571	1.4286	0.4286	0.0000	1.7143	94.12%	19.61%	5.88%	0.00%	3.43	100.00%
Optimal IDM Website	4.3750	3.3750	0.7500	0.6250	0.0000	2.0000	77.14%	17.14%	14.29%	0.00%	2.88	100.00%
Palo Alto Networks Form 10-k	14.3750	8.5000	1.7500	2.0000	0.3750	1.5000	59.13%	12.17%	13.91%	2.61%	3.63	62.50%
Symantec Corporation Form 10-K	21.0909	9.0000	1.7273	1.4545	0.1818	1.9091	42.67%	8.19%	6.90%	0.86%	3.45	63.64%
McAfee corporate fact sheet	12.8333	10.5833	1.3333	0.9167	0.0000	1.5833	82.47%	10.39%	7.14%	0.00%	3.83	83.33%
Apple Inc Form 10-K	7.5385	2.9231	1.1538	0.2308	0.0769	2.2308	38.78%	15.31%	3.06%	1.02%	2.62	76.92%
GE Corporation annual report	12.3333	10.8889	2.7778	3.2222	2.0000	0.4444	88.29%	22.52%	26.13%	16.22%	3.56	55.56%
Akamai Form 10-K	22.3333	13.7500	2.7500	3.0833	0.2500	1.2500	61.57%	12.31%	13.81%	1.12%	4.42	75.00%
FireEye Inc Form 10-K	20.5385	6.8846	2.0385	2.8077	0.2308	1.3077	33.52%	9.93%	13.67%	1.12%	3.96	80.77%
Splunk Strategy and Growth strategy from Form	18.1842	8.5789	1.6053	1.2105	0.2895	1.7105	47.18%	8.83%	6.66%	1.59%	4.16	65.79%

Analysis of the DoD/Government Strategy Table of Combined Averages and Ratios

Combined Average action items per strategy section	Combined Average MOS/MOE	Combined Average Timelines	Combined Average Feedback	Combined Average Budget Allocation	Combined Average Empty Elements	Combined Average Unpredictable Change	Combined Ratio of Cyberspace Specific	Combined Minimum Cyberspace Specific Ratio	Combined Ratio MOS/MOE over Action Items	Combined Ratio Timelines over Action Items	Combined Ratio Feedback over Action Items	Combined Ratio Budget over Action Items
11.58	4.38	0.68	0.38	0.18	2.33	3.84	84.69%	40.54%	39.33%	5.58%	3.30%	1.84%

Analysis of the Industry Strategy Table of Combined Averages and Ratios

Combined Average action items per strategy section	Combined Average MOS/MOE	Combined Average Timelines	Combined Average Feedback	Combined Average Budget Allocation	Combined Average Empty Elements	Combined Average Unpredictable Change	Combined Ratio of Cyberspace Specific	Combined Minimum Cyberspace Specific Ratio	Combined Ratio MOS/MOE over Action Items	Combined Ratio Timelines over Action Items	Combined Ratio Feedback over Action Items	Combined Ratio Budget over Action Items
11.07	6.34	1.34	1.38	0.33	1.69	3.36	68.47%	9.09%	59.02%	13.72%	13.29%	3.07%

Analysis of the DoD/Government Strategy Coding

Document	Strategy	Number of Strategic Sections	Unpredictable change +0-5	Cyberspace specific *(+1 or -1)	Action Items + 0.01x#	MOS/MOE + 0.01x#	Timelines + 0.01x#	Feedback + 0.01x#	Budget Allocated + 0.01x#	Total
National Defense Strategy	Strategic Approach	1 of 37	5	1	0.17	0	0	0	0	5.17, 1 of 37
National Defense Strategy	Be strategically predictable, but operationally unpredictable	1 of 37	5	-1	0.1	0.07	0	0.01	0	-5.18, 1 of 37
National Defense Strategy	Integrate with U.S. interagency	1 of 37	4	-1	0.17	0.06	0	0.01	0	-4.24, 1 of 37
National Defense Strategy	Counter coercion and subversion.	1 of 37	4	-1	0.06	0.02	0	0	0	-4.08, 1 of 37
National Defense Strategy	Foster a competitive mindset.	1 of 37	5	-1	0.13	0.03	0	0	0	-5.16, 1 of 37
National Defense Strategy	Build a More Lethal Force	1 of 37	4	-1	0.12	0.06	0.01	0	0	-4.19, 1 of 37
National Defense Strategy	Prioritize Preparedness for War	1 of 37	4	1	0.19	0.17	0.01	0	0	4.37, 1 of 37
National Defense Strategy	Modernize Key Capabilities	1 of 37	3	1	0.1	0.05	0.02	0	0.01	3.18, 1 of 37
National Defense Strategy	Nuclear Forces	1 of 37	2	1	0.06	0.01	0	0	0	2.07, 1 of 37
National Defense Strategy	Space and Cyberspace as a warfighting domain	1 of 37	5	1	0.06	0.01	0	0	0.01	5.08, 1 of 37
National Defense Strategy	Command, control, communications, computers and intelligence	1 of 37	5	1	0.13	0.07	0.01	0	0.02	5.23, 1 of 37
National Defense Strategy	missile defense	1 of 37	3	1	0.04	0	0	0	0.01	3.05, 1 of 37
National Defense Strategy	joint lethality in contested environments	1 of 37	5	1	0.04	0.01	0	0	0	5.05, 1 of 37
National Defense Strategy	forward force maneuver and posture resilience	1 of 37	4	1	0.14	0.12	0	0	0.02	4.28, 1 of 37
National Defense Strategy	advanced autonomous systems	1 of 37	5	1	0.04	0.01	0	0	0.01	5.06, 1 of 37
National Defense Strategy	resilient and agile logistics	1 of 37	3	-1	0.07	0.01	0	0	0.1	-3.18, 1 of 37
National Defense Strategy	Evolve innovative operational concepts.	1 of 37	5	1	0.08	0.02	0.02	0.01	0	5.13, 1 of 37
National Defense Strategy	Develop a lethal, agile, and resilient force posture and doctrine	1 of 37	4	-1	0.35	0.2	0.03	0	0.01	-4.59, 1 of 37
National Defense Strategy	Cultivate workforce talent	1 of 37	3	-1	0.07	0.02	0	0	0	-3.09, 1 of 37
National Defense Strategy	Professional Military Education	1 of 37	3	-1	0.14	0.05	0	0	0	-3.19, 1 of 37
National Defense Strategy	Talent Management	1 of 37	3	-1	0.06	0.01	0	0	0	-3.07, 1 of 37
National Defense Strategy	Civilian Workforce Expertise	1 of 37	5	-1	0.13	0.06	0	0	0	-5.19, 1 of 37
National Defense Strategy	Strengthen Alliances and Attract New Partners	1 of 37	1	-1	0.05	0	0	0	0	-1.05, 1 of 37
National Defense Strategy	Uphold a foundation of mutual respect, responsibility, and trust	1 of 37	4	-1	0.06	0.04	0	0	0	-4.1, 1 of 37
National Defense Strategy	Expand regional consultative mechanisms and collaboration	1 of 37	3	-1	0.06	0.05	0	0	0	-3.11, 1 of 37
National Defense Strategy	Deepen interoperability	1 of 37	4	-1	0.06	0	0.01	0	0	-4.07, 1 of 37
National Defense Strategy	Expand Indo-Pacific alliances and partnerships	1 of 37	5	-1	0.09	0.05	0	0	0	-5.14, 1 of 37
National Defense Strategy	Fortify the Trans-Atlantic NATO Alliance	1 of 37	4	1	0.07	0.02	0.01	0	0	4.1, 1 of 37
National Defense Strategy	Form enduring coalitions in the Middle East.	1 of 37	4	-1	0.12	0.05	0	0	0	-4.17, 1 of 37
National Defense Strategy	Sustain advantages in the Western Hemisphere	1 of 37	2	1	0.01	0.01	0	0	0	-2.02, 1 of 37
National Defense Strategy	Support relationships to address significant terrorist threats	1 of 37	4	-1	0.13	0.09	0	0	0	-4.22, 1 of 37
National Defense Strategy	Reform the Department for Greater Performance and Accountability	1 of 37	4	-1	0.06	0.06	0	0.01	0	-4.13, 1 of 37
National Defense Strategy	Deliver performance at the speed of relevance	1 of 37	5	1	0.09	0.05	0.01	0	0	5.15, 1 of 37
National Defense Strategy	Organize for innovation	1 of 37	5	-1	0.08	0.04	0.01	0.01	0	-5.14, 1 of 37
National Defense Strategy	Drive budget discipline and affordability to achieve strategic goals	1 of 37	4	-1	0.24	0.08	0	0.01	0	-4.33, 1 of 37
National Defense Strategy	Streamline rapid, iterative approaches from development to deployment	1 of 37	5	1	0.1	0.06	0.04	0.01	0.01	5.22, 1 of 37
National Defense Strategy	Harness and protect the national security innovation base	1 of 37	1	1	0.07	0.08	0.01	0	0.01	1.17, 1 of 37
The DoD Cyber Strategy	Strategic competition in cyberspace	1 of 23	4	1	0.09	0	0	0	0	4.09, 1 of 23
The DoD Cyber Strategy	ensure US Military ability to fight and win wars in any domain	1 of 23	5	1	0.19	0.07	0	0	0	5.26, 1 of 23
The DoD Cyber Strategy	preempt, defeat, or deter malicious cyber activity targeting US interests	1 of 23	3	1	0.08	0.02	0.01	0.01	0	3.12, 1 of 23
The DoD Cyber Strategy	strengthen cyber capacity, expand combined cyberspace capabilities	1 of 23	4	1	0.03	0.04	0	0	0	4.07, 1 of 23
The DoD Cyber Strategy	defending civilian assets that enable US Military advantage	1 of 23	4	1	0.13	0.04	0.03	0	0	4.2, 1 of 23
The DoD Cyber Strategy	Accelerate cyber capability development	1 of 23	5	1	0.1	0.02	0.02	0	0	5.14, 1 of 23
The DoD Cyber Strategy	innovate to foster agility	1 of 23	5	1	0.08	0.05	0.02	0.01	0	5.16, 1 of 23
The DoD Cyber Strategy	leverage automation and data analysis to improve effectiveness	1 of 23	5	1	0.07	0.06	0.02	0	0	5.15, 1 of 23
The DoD Cyber Strategy	employ COTs cyber capabilities	1 of 23	5	1	0.01	0.01	0	0.01	0	5.03, 1 of 23
The DoD Cyber Strategy	deter malicious cyber activities	1 of 23	5	1	0.09	0.01	0	0.01	0	5.11, 1 of 23
The DoD Cyber Strategy	persistently contest malicious cyber activity in day-to-day operations	1 of 23	4	1	0.1	0.04	0	0	0	4.14, 1 of 23
The DoD Cyber Strategy	increase resilience of US Critical infrastructure	1 of 23	3	1	0.08	0.02	0.01	0.01	0	3.12, 1 of 23
The DoD Cyber Strategy	build trusted private sector partnerships	1 of 23	4	1	0.04	0.02	0	0	0	4.06, 1 of 23
The DoD Cyber Strategy	operationalize international partnerships	1 of 23	4	1	0.06	0.06	0	0	0	4.12, 1 of 23
The DoD Cyber Strategy	reinforce norms of responsible State behavior in cyberspace	1 of 23	5	1	0.12	0.04	0.01	0.01	0	5.18, 1 of 23
The DoD Cyber Strategy	incorporate cyber awareness into DoD institutional culture	1 of 23	2	1	0.08	0.07	0.01	0	0	2.16, 1 of 23
The DoD Cyber Strategy	increase cybersecurity accountability	1 of 23	2	1	0.04	0	0	0	0	2.04, 1 of 23
The DoD Cyber Strategy	seek material solutions that are affordable, flexible, and scalable	1 of 23	4	1	0.09	0.07	0.02	0	0	4.18, 1 of 23
The DoD Cyber Strategy	expand crowd-sourced vulnerability identification	1 of 23	5	1	0.04	0.03	0	0.01	0	5.08, 1 of 23
The DoD Cyber Strategy	sustain a ready cyber workforce	1 of 23	4	1	0.15	0.05	0.01	0.01	0.01	4.23, 1 of 23
The DoD Cyber Strategy	enhances the nation's cyber talent	1 of 23	4	1	0.13	0.06	0	0.01	0	4.2, 1 of 23
The DoD Cyber Strategy	embed software and hardware expertise as a core DoD capability	1 of 23	5	1	0.09	0.04	0	0	0	5.13, 1 of 23
The DoD Cyber Strategy	establish a cyber top talent management program	1 of 23	5	1	0.09	0.04	0	0	0	5.13, 1 of 23
USCYBERCOM Vision	Superiority through persistence	1 of 9	4	1	0.42	0.29	0.04	0.01	0	4.76, 1 of 9
USCYBERCOM Vision	commander's intent	1 of 9	5	1	0.36	0.1	0.01	0	0	5.47, 1 of 9
USCYBERCOM Vision	Achieve and sustain overmatch of adversary capabilities	1 of 9	5	1	0.09	0.05	0.01	0	0	5.15, 1 of 9
USCYBERCOM Vision	create cyberspace advantages to enhance operations in cyberspace	1 of 9	5	1	0.07	0.03	0.02	0	0	5.12, 1 of 9
USCYBERCOM Vision	create information advantages to support operational and strategic goals	1 of 9	3	1	0.09	0.02	0	0	0	3.11, 1 of 9
USCYBERCOM Vision	operationalize the battlespace for agile and responsive operations	1 of 9	4	1	0.08	0	0.01	0	0	4.09, 1 of 9
USCYBERCOM Vision	expand, deepen, and operationalize partnerships	1 of 9	4	1	0.17	0	0.01	0	0	4.18, 1 of 9
USCYBERCOM Vision	Risk mitigation	1 of 9	4	1	0.18	0.01	0	0.01	0	4.2, 1 of 9
USCYBERCOM Vision	Implementation	1 of 9	3	1	0.22	0.03	0.02	0.04	0	3.31, 1 of 9

Analysis of the DoD/Government Strategy Coding

Document	Strategy	Number of Strategic Sections	Unpredictable change +0-5	Cyberspace specific *(+1 or -1)	Action Items + 0.01x#	MOS/MOE + 0.01x#	Timelines + 0.01x#	Feedback + 0.01x#	Budget Allocated + 0.01x#	Total
National Cyber Strategy	Protect the American people, the homeland and the an	1 of 56	1	1	0.11	0	0.01	0	0	1.12, 1 of 56
National Cyber Strategy	secure Federal Networks and information	1 of 56	2	1	0.1	0	0	0	0	2.1, 1 of 56
National Cyber Strategy	Further centralize management and oversight of fede	1 of 56	3	1	0.15	0.04	0	0.01	0.01	3.21, 1 of 56
National Cyber Strategy	align risk management and information technology ac	1 of 56	3	1	0.11	0.07	0	0.03	0.03	3.24, 1 of 56
National Cyber Strategy	improve federal supply chain risk management	1 of 56	4	1	0.1	0.05	0	0.01	0	4.16, 1 of 56
National Cyber Strategy	strengthen federal contractor cybersecurity	1 of 56	4	1	0.1	0.04	0	0.03	0	4.17, 1 of 56
National Cyber Strategy	ensure government leads in best and innovative practic	1 of 56	5	1	0.13	0.03	0.01	0	0	5.17, 1 of 56
National Cyber Strategy	secure critical infrastrucutre	1 of 56	4	1	0.05	0.03	0	0.01	0	4.09, 1 of 56
National Cyber Strategy	refine roles and responsibilities	1 of 56	3	1	0.08	0.04	0	0	0	3.12, 1 of 56
National Cyber Strategy	prioritize actions according to identified national risk	1 of 56	4	1	0.06	0.01	0	0.01	0	4.08, 1 of 56
National Cyber Strategy	leverage information and communications technology	1 of 56	5	1	0.17	0.08	0	0.01	0	5.26, 1 of 56
National Cyber Strategy	protect our democracy	1 of 56	3	1	0.11	0.04	0.01	0.01	0	3.17, 1 of 56
National Cyber Strategy	incentivize cybersecurity investments	1 of 56	3	1	0.05	0.04	0	0	0	3.09, 1 of 56
National Cyber Strategy	prioritize national research and development investme	1 of 56	4	1	0.07	0.03	0	0	0.01	4.11, 1 of 56
National Cyber Strategy	improve transportation and maritime cybersecurity	1 of 56	4	1	0.04	0.04	0.01	0	0	4.09, 1 of 56
National Cyber Strategy	improve space cybersecurity	1 of 56	4	1	0.05	0.04	0.01	0	0	4.1, 1 of 56
National Cyber Strategy	combat cybercrime and improve incident reporting	1 of 56	3	1	0.1	0.04	0.01	0	0	3.15, 1 of 56
National Cyber Strategy	improve incident reporting and response	1 of 56	3	1	0.01	0.01	0	0.01	0	3.03, 1 of 56
National Cyber Strategy	modernize electronic surveillance and computer crim	1 of 56	2	1	0.05	0.03	0	0	0	2.08, 1 of 56
National Cyber Strategy	reduce threats from transnational criminal organizatio	1 of 56	2	1	0.03	0.01	0	0	0	2.04, 1 of 56
National Cyber Strategy	improve apprehension of criminals located abroad	1 of 56	3	1	0.08	0.03	0	0	0	3.11, 1 of 56
National Cyber Strategy	strengthen partner nations' law enforcement capacity	1 of 56	4	1	0.12	0.03	0	0	0	4.15, 1 of 56
National Cyber Strategy	Promote American prosperity	1 of 56	1	1	0.06	0	0	0	0	1.06, 1 of 56
National Cyber Strategy	foster a vibrant and resilient digital economy	1 of 56	2	1	0.04	0.03	0	0	0	2.07, 1 of 56
National Cyber Strategy	incentivize on adaptable and secure technology marke	1 of 56	4	1	0.13	0.04	0	0.01	0	4.18, 1 of 56
National Cyber Strategy	prioritize innovation	1 of 56	5	1	0.09	0.01	0	0	0	5.1, 1 of 56
National Cyber Strategy	invest in next generation infrastructure	1 of 56	5	1	0.14	0.07	0.01	0.01	0	5.23, 1 of 56
National Cyber Strategy	promote the free flow of data across borders	1 of 56	4	1	0.08	0.03	0	0	0	4.11, 1 of 56
National Cyber Strategy	maintain US leadership in emerging technologies	1 of 56	5	1	0.09	0.06	0	0	0	5.15, 1 of 56
National Cyber Strategy	promote full-lifecycle cybersecurity	1 of 56	5	1	0.2	0.04	0	0	0	5.24, 1 of 56
National Cyber Strategy	foster and protect US ingenuity	1 of 56	4	1	0.09	0.03	0	0	0	4.12, 1 of 56
National Cyber Strategy	update mechanisms to review foreign investment and	1 of 56	2	1	0.03	0.01	0.01	0	0	2.05, 1 of 56
National Cyber Strategy	maintain a strong and balanced intellectual property pr	1 of 56	3	-1	0.06	0	0	0	0	-3.06, 1 of 56
National Cyber Strategy	protect the confidentiality and integrity of american ic	1 of 56	1	1	0.02	0	0	0.01	0	1.03, 1 of 56
National Cyber Strategy	develop a superior cybersecurity workforce	1 of 56	1	1	0.02	0	0	0	0	1.02, 1 of 56
National Cyber Strategy	build and sustain the talent pipeline	1 of 56	2	1	0.05	0.01	0	0	0	2.06, 1 of 56
National Cyber Strategy	expand re-skilling and educational opportunities for A	1 of 56	2	1	0.08	0.01	0	0	0	2.09, 1 of 56
National Cyber Strategy	enhance the Federal Cybersecurity workforce	1 of 56	2	1	0.15	0.02	0	0	0.01	2.18, 1 of 56
National Cyber Strategy	use executive authority to highlight and reward talent	1 of 56	2	1	0.09	0.02	0	0	0	2.11, 1 of 56
National Cyber Strategy	Preserve Peace through strength	1 of 56	4	1	0.13	0.01	0	0	0	4.14, 1 of 56
National Cyber Strategy	enhance cyber stability through Norms of responsible	1 of 56	0	1	0.04	0.02	0	0	0	0.06, 1 of 56
National Cyber Strategy	encourage Universal adherence to cyber norms	1 of 56	1	1	0.03	0.08	0	0	0	1.11, 1 of 56
National Cyber Strategy	attribute and deter unacceptable behavior in cyberspac	1 of 56	5	1	0.19	0.05	0.01	0	0	5.25, 1 of 56
National Cyber Strategy	lead with objective collaboration intelligence	1 of 56	5	1	0.13	0.09	0	0	0	5.22, 1 of 56
National Cyber Strategy	impose consequences	1 of 56	4	1	0.09	0.03	0.01	0	0	4.13, 1 of 56
National Cyber Strategy	build a cyber deterrence initiative	1 of 56	4	1	0.09	0.02	0	0	0	4.11, 1 of 56
National Cyber Strategy	counter malign cyber influence and information opera	1 of 56	4	1	0.15	0.07	0	0	0	4.22, 1 of 56
National Cyber Strategy	Advance American influence	1 of 56	1	1	0.12	0	0	0	0	1.12, 1 of 56
National Cyber Strategy	promote an open, interoperable, reliable and secure in	1 of 56	4	1	0.07	0.01	0	0	0	4.08, 1 of 56
National Cyber Strategy	protect and promote internet freedom	1 of 56	1	1	0.01	0	0	0	0	1.01, 1 of 56
National Cyber Strategy	work with like-minded countries, industry, academia,	1 of 56	1	1	0.11	0.01	0	0	0	1.12, 1 of 56
National Cyber Strategy	promote a multi-stakeholder model of internet govern	1 of 56	4	1	0.13	0.04	0	0	0	4.17, 1 of 56
National Cyber Strategy	promote interoperable and reliable communications in	1 of 56	4	1	0.06	0.04	0	0	0	4.1, 1 of 56
National Cyber Strategy	promote and maintain markets for US ingenuity world	1 of 56	4	1	0.17	0.06	0	0	0	4.23, 1 of 56
National Cyber Strategy	build international cyber capacity	1 of 56	4	1	0.01	0.1	0	0	0	4.11, 1 of 56
National Cyber Strategy	enhance cyber capacity building efforts	1 of 56	5	1	0.18	0.05	0	0	0	5.23, 1 of 56

Analysis of the Industry Strategy Coding

Document	Strategy	Number of Discrete Strategies	Unpredictable change +0-5	Cyberspace specific *(+1 or -1)	Action Items + 0.01x#	MOS/MOE + 0.01x#	Timelines + 0.01x#	Feedback + 0.01x#	Budget Allocated + 0.01x#	Total
Del Monte Forest Conservancy Strategic Plan	Provide general governance and management direction IAW I	1 of 12	2	-1	0.03	0.01	0.01	0.03	0	-2.08, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Implement and oversee open space conservation... etc.	1 of 12	2	-1	0.07	0.07	0.03	0.05	0	-2.22, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Assist Budget and Finance Committee to achieve fiscal stabil	1 of 12	2	-1	0.04	0.03	0.01	0.02	0.01	-2.11, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Actively participate in development of future DMFS managen	1 of 12	4	-1	0.1	0.01	0.01	0.02	0	-4.14, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Develop plans and programs to obtain financial support for D	1 of 12	2	1	0.09	0.03	0.03	0.01	0	2.16, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Develop DM Forest education plans and programs	1 of 12	2	1	0.09	0.04	0	0.02	0	2.15, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Support scientific forest and environmental research program	1 of 12	0	-1	0.01	0.05	0	0	0.01	-0.07, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Provide oversight for management of DMFC's financial resou	1 of 12	3	-1	0.13	0.07	0.05	0.07	0	-3.32, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Serve as a resource for election and retention of directors w/	1 of 12	2	-1	0.03	0.01	0.02	0	0	-2.06, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Develop a plan to create a smooth transition for newly appoin	1 of 12	3	-1	0.02	0.03	0.01	0	0	-3.06, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Coordinate independent audits or reviews of DMFC's financ	1 of 12	2	-1	0.07	0.01	0.04	0.03	0	-2.15, 1 of 12
Del Monte Forest Conservancy Strategic Plan	Plan of Management and Professional Organization	1 of 12	3	-1	0.06	0.09	0.03	0.02	0	-3.2, 1 of 12
Ixia Annual Report 10K 2016	Our Business Strategy	1 of 13	4	1	0.03	0.03	0	0	0	4.06, 1 of 13
Ixia Annual Report 10K 2016	Continue to expand our addressable markets	1 of 13	4	1	0.05	0	0	0	0	4.05, 1 of 13
Ixia Annual Report 10K 2016	Maintain focus on technology leadership	1 of 13	5	1	0.08	0.03	0.02	0.01	0	5.14, 1 of 13
Ixia Annual Report 10K 2016	Expand and further penetrate customer base	1 of 13	5	1	0.14	0.05	0	0	0	5.19, 1 of 13
Ixia Annual Report 10K 2016	Expand international Market Presence	1 of 13	5	-1	0.07	0	0	0	0	-5.07, 1 of 13
Ixia Annual Report 10K 2016	License and acquire new products	1 of 13	5	1	0.04	0.03	0	0	0	5.07, 1 of 13
Ixia Annual Report 10K 2016	Our Solutions (product strategy)	1 of 13	4	1	0.08	0.07	0.01	0.06	0	4.22, 1 of 13
Ixia Annual Report 10K 2016	Competition <strategy>	1 of 13	4	1	0.1	0.08	0.01	0	0	4.19, 1 of 13
Ixia Annual Report 10K 2016	Sales, Marketing and Technical Support <strategy>	1 of 13	1	-1	0.27	0.1	0.02	0	0	-1.39, 1 of 13
Ixia Annual Report 10K 2016	Manufacturing and Supply Ops	1 of 13	4	1	0.23	0.03	0.02	0.01	0	4.29, 1 of 13
Ixia Annual Report 10K 2016	Research and Development	1 of 13	5	1	0.12	0.02	0.01	0.01	0.03	5.19, 1 of 13
Ixia Annual Report 10K 2016	Intellectual property and proprietary rights	1 of 13	5	1	0.15	0.08	0	0.01	0	5.24, 1 of 13
Ixia Annual Report 10K 2016	Employees	1 of 13	1	-1	0.02	0.01	0	0	0	-1.03, 1 of 13
Marsh & McLennan Companies, Inc. 10-K 2019	Insurance Broking and Risk Consulting	1 of 16	3	-1	0.16	0.02	0	0	0	-3.38, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2019	Risk Management	1 of 16	3	-1	0.05	0.02	0	0	0	-3.07, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2019	Corporate	1 of 16	2	-1	0.09	0.01	0	0	0	-2.1, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2019	Commercial & Consumer	1 of 16	2	-1	0.08	0.01	0.01	0	0	-2.1, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2020	High Net Worth	1 of 16	2	-1	0.04	0	0	0	0	-2.04, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2022	health	1 of 16	2	-1	0.05	0	0	0	0	-2.05, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2023	wealth	1 of 16	1	-1	0.07	0	0	0	0	-1.07, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2024	Career	1 of 16	2	-1	0.08	0.04	0	0	0	-2.12, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2026	Risk and Insurance Services	1 of 16	1	-1	0.03	0	0	0	0	-1.03, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2027	Consulting	1 of 16	1	-1	0	0	0	0	0	-1, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2028	Risks relating to the company generally	1 of 16	4	-1	0.02	0.03	0	0	0	-4.05, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2029	Competitive Risks - technology change	1 of 16	3	1	0.08	0.04	0	0	0	3.12, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2030	Competitive Risks - Culture and reputation	1 of 16	3	-1	0.11	0.05	0	0	0	-3.16, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2031	Competitive Risks - Talent management	1 of 16	5	-1	0.05	0.02	0	0	0	-5.07, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2032	cybersecurity and data protection risks	1 of 16	4	1	0.05	0	0	0	0	4.05, 1 of 16
Marsh & McLennan Companies, Inc. 10-K 2033	Business Resiliency Risk	1 of 16	4	1	0.04	0	0	0	0	4.04, 1 of 16
Intel 2018 Annual Report	Our Strategy	1 of 17	5	1	0.07	0.02	0.02	0.01	0	5.12, 1 of 17
Intel 2018 Annual Report	Make the World's Best semiconductors	1 of 17	5	1	0.19	0.11	0.01	0	0	5.31, 1 of 17
Intel 2018 Annual Report	Lead the AI and Autonomous Revolution	1 of 17	5	1	0.09	0.06	0	0.09	0	5.24, 1 of 17
Intel 2018 Annual Report	Be the leading end-to-end platform provider for the new data	1 of 17	5	1	0.29	0.1	0	0.02	0	5.41, 1 of 17
Intel 2018 Annual Report	relentless focus on operational excellence and efficiency	1 of 17	3	-1	0.13	0.07	0	0	0	-3.2, 1 of 17
Intel 2018 Annual Report	Continue to hire, develop and retain the best, most diverse an	1 of 17	4	-1	0.12	0.09	0.01	0	0	-4.22, 1 of 17
Intel 2018 Annual Report	Our Capital	1 of 17	4	1	0.19	0.14	0	0.01	0	4.34, 1 of 17
Intel 2018 Annual Report	Financial capital	1 of 17	5	1	0.06	0.01	0	0.01	0	5.08, 1 of 17
Intel 2018 Annual Report	Invest in the business	1 of 17	5	1	0.03	0	0.01	0.01	0.03	5.08, 1 of 17
Intel 2018 Annual Report	Acquire and integrate	1 of 17	4	-1	0.03	0.04	0.01	0	0.02	-4.1, 1 of 17
Intel 2018 Annual Report	Return cash to stockholders	1 of 17	3	-1	0.03	0.04	0.01	0	0.04	-3.12, 1 of 17
Intel 2018 Annual Report	intellectual capital	1 of 17	4	1	0.12	0.03	0.01	0.02	0	4.18, 1 of 17
Intel 2018 Annual Report	Product technology (6 areas)	1 of 17	4	1	0.08	0.01	0.01	0	0	4.1, 1 of 17
Intel 2018 Annual Report	manufactured capital	1 of 17	5	1	0.07	0.03	0.02	0.02	0.01	5.15, 1 of 17
Intel 2018 Annual Report	human capital	1 of 17	5	-1	0.07	0.03	0.01	0.05	0	-5.16, 1 of 17
Intel 2018 Annual Report	social and relationship capital	1 of 17	4	-1	0.14	0.03	0.01	0.05	0	-4.23, 1 of 17
Intel 2018 Annual Report	natural capital	1 of 17	1	-1	0.13	0.07	0.02	0.02	0.01	-1.25, 1 of 17
Bank of America	we must grow and win in the market - no excuses	1 of 7	1	-1	0.03	0.05	0.01	0	0	-1.09, 1 of 7
Bank of America	we must grow with out customer-focused strategy	1 of 7	2	1	0.18	0.15	0	0	0.02	2.35, 1 of 7
Bank of America	we must grow within our risk framework	1 of 7	3	-1	0.19	0.1	0.01	0.02	0	-3.32, 1 of 7
Bank of America	we must grow in a sustainable manner	1 of 7	2	-1	0.04	0.01	0.01	0	0	-2.06, 1 of 7
Bank of America	sharing success with the communities we serve	1 of 7	0	-1	0.05	0.03	0.01	0.01	0	-0.1, 1 of 7
Bank of America	being a great place to work	1 of 7	1	-1	0.06	0.02	0.01	0.02	0	-1.11, 1 of 7
Bank of America	driving operational excellence	1 of 7	1	-1	0.01	0.06	0.01	0.02	0	-1.1, 1 of 7
Lookingglass Cyber	intelligence tradecraft	1 of 6	3	1	0.03	0.01	0	0	0	3.04, 1 of 6
Lookingglass Cyber	best-in-class threat intelligence	1 of 6	5	1	0.04	0.01	0	0	0	5.05, 1 of 6
Lookingglass Cyber	experienced security & threat analysts	1 of 6	4	1	0.04	0.03	0	0	0	4.07, 1 of 6
Lookingglass Cyber	timely, relevant, actionable intelligence	1 of 6	5	1	0.04	0.01	0.01	0	0	5.06, 1 of 6
Lookingglass Cyber	robust portfolio with choice of delivery model	1 of 6	2	1	0.02	0	0	0	0	2.02, 1 of 6
Lookingglass Cyber	about lookingglass cyber solutions	1 of 6	5	1	0.15	0.08	0.01	0	0	5.24, 1 of 6

Analysis of the Industry Strategy Coding

Document	Strategy	Number of Discrete Strategies	Unpredictable change +0-5	Cyberspace specific *(+1 or -1)	Action Items + 0.01x#	MOS/MOE + 0.01x#	Timelines + 0.01x#	Feedback + 0.01x#	Budget Allocated + 0.01x#	Total
Cisco	enabling network automation	1 of 8	3	1	0.11	0.03	0.01	0	0	3.15, 1 of 8
Cisco	powering a multicloud world	1 of 8	4	1	0.11	0.02	0	0	0	4.13, 1 of 8
Cisco	security is foundational	1 of 8	3	1	0.04	0.07	0.01	0	0	3.12, 1 of 8
Cisco	unlocking the power of data	1 of 8	4	1	0.01	0.03	0.01	0	0	4.05, 1 of 8
Cisco	transforming our business model	1 of 8	4	1	0.04	0.03	0	0.01	0	4.08, 1 of 8
Cisco	Diverse leadership	1 of 8	4	-1	0.07	0.06	0.01	0	0	-4.14, 1 of 8
Cisco	shareholder engagement	1 of 8	3	-1	0.02	0.01	0.02	0.01	0	-3.06, 1 of 8
Cisco	risk management approach	1 of 8	4	-1	0.13	0.1	0.06	0.06	0	-4.35, 1 of 8
Tesla Impact Report 2018	sustainable and superior products for everyone	1 of 22	0	-1	0.07	0.08	0	0	0	-0.15, 1 of 22
Tesla Impact Report 2018	environmental impact	1 of 22	5	-1	0.06	0.14	0.03	0	0	-5.23, 1 of 22
Tesla Impact Report 2018	resilience of the grid	1 of 22	4	-1	0.05	0.1	0.02	0	0	-4.17, 1 of 22
Tesla Impact Report 2018	access to sustainable energy	1 of 22	2	-1	0.01	0.01	0.01	0.01	0.01	-2.05, 1 of 22
Tesla Impact Report 2018	building the safest cars from the ground up	1 of 22	3	1	0.14	0.09	0.02	0.02	0	3.27, 1 of 22
Tesla Impact Report 2018	building a sustainable future in a sustainable way	1 of 22	2	-1	0.06	0.03	0.01	0	0.01	-2.11, 1 of 22
Tesla Impact Report 2018	greenhouse gas inventory	1 of 22	2	-1	0.01	0.02	0.01	0.01	0	-2.05, 1 of 22
Tesla Impact Report 2018	energy efficiency	1 of 22	2	-1	0.03	0.02	0.02	0.01	0	-2.08, 1 of 22
Tesla Impact Report 2018	sustainable energy	1 of 22	2	-1	0.01	0.01	0	0	0	-2.02, 1 of 22
Tesla Impact Report 2018	superchargers	1 of 22	3	-1	0.04	0.04	0	0.02	0	-3.1, 1 of 22
Tesla Impact Report 2018	responsible sourcing	1 of 22	2	-1	0.05	0.03	0	0.02	0	-2.1, 1 of 22
Tesla Impact Report 2018	conflict minerals	1 of 22	2	-1	0.01	0.01	0	0.01	0	-2.03, 1 of 22
Tesla Impact Report 2018	supplier diversity	1 of 22	2	-1	0.02	0.02	0	0	0	-2.04, 1 of 22
Tesla Impact Report 2018	becoming the safest car factory in the world	1 of 22	3	-1	0.07	0.05	0.02	0.04	0	-3.18, 1 of 22
Tesla Impact Report 2018	the safest cars for customers and employees	1 of 22	2	-1	0.02	0.02	0	0.05	0	-2.09, 1 of 22
Tesla Impact Report 2018	rewarding the individual	1 of 22	2	-1	0.09	0.05	0.04	0.07	0.01	-2.26, 1 of 22
Tesla Impact Report 2018	diversity and inclusion	1 of 22	2	-1	0.03	0.01	0	0	0	-2.04, 1 of 22
Tesla Impact Report 2018	excellence - the passing grade	1 of 22	2	-1	0.08	0.06	0.01	0.02	0	-2.17, 1 of 22
Tesla Impact Report 2018	employee mobility and transportation programs	1 of 22	2	-1	0.03	0.02	0.01	0.01	0.01	-2.08, 1 of 22
Tesla Impact Report 2018	education	1 of 22	4	1	0.1	0.02	0.01	0	0.01	4.14, 1 of 22
Tesla Impact Report 2018	corporate governance	1 of 22	0	-1	0.16	0.04	0.02	0.08	0	-0.3, 1 of 22
Tesla Impact Report 2018	driven by sustainability	1 of 22	3	-1	0.08	0.05	0.01	0.01	0	-3.15, 1 of 22
Blackberry/Cylance	IoT	1 of 7	4	1	0.05	0.04	0.01	0	0.01	4.11, 1 of 7
Blackberry/Cylance	Licensing	1 of 7	3	1	0.02	0.01	0.01	0	0.01	3.05, 1 of 7
Blackberry/Cylance	enterprise software and services	1 of 7	3	1	0.08	0.04	0.01	0	0.01	3.14, 1 of 7
Blackberry/Cylance	BlackbBerry Technology solutions	1 of 7	3	1	0.08	0.04	0.01	0	0.01	3.14, 1 of 7
Blackberry/Cylance	Licensing	1 of 7	2	1	0.04	0.02	0.01	0	0.01	2.08, 1 of 7
Blackberry/Cylance	BlackBerry Cylance (2nd strategy)	1 of 7	3	1	0.07	0.05	0.01	0	0.02	3.15, 1 of 7
Blackberry/Cylance	Opportunity for long term growth	1 of 7	3	-1	0.08	0.03	0.02	0	0	-3.13, 1 of 7
Edgescan	SaaS	1 of 12	2	1	0.02	0.03	0.01	0	0	2.06, 1 of 12
Edgescan	Hybrid Scalable Assessments	1 of 12	3	1	0.02	0.02	0	0	0	3.04, 1 of 12
Edgescan	Analytics & Depth	1 of 12	4	1	0.07	0.02	0.02	0.02	0	4.13, 1 of 12
Edgescan	Coverage	1 of 12	4	1	0.06	0.01	0	0	0	4.07, 1 of 12
Edgescan	support	1 of 12	3	1	0.04	0.02	0	0.01	0	3.07, 1 of 12
Edgescan	Vulnerability intelligence	1 of 12	3	1	0.06	0.02	0	0.01	0	3.09, 1 of 12
Edgescan	Rich API integration	1 of 12	2	1	0.06	0.06	0	0	0	2.12, 1 of 12
Edgescan	One-click WAF	1 of 12	3	1	0.01	0.01	0	0	0	3.02, 1 of 12
Edgescan	Alerting	1 of 12	4	1	0.05	0.02	0	0.01	0	4.08, 1 of 12
Edgescan	Continuous Asset Profiling	1 of 12	3	1	0.03	0.02	0.01	0	0	3.06, 1 of 12
Edgescan	Scale	1 of 12	3	1	0.04	0.01	0.02	0.01	0	3.08, 1 of 12
Edgescan	Compliance	1 of 12	2	1	0.04	0.03	0	0	0	2.07, 1 of 12
Security Compass	SD Elements	1 of 5	3	1	0.05	0.03	0.01	0.01	0	3.1, 1 of 5
Security Compass	Threat Modeling	1 of 5	3	1	0.11	0.05	0.03	0.04	0.01	3.24, 1 of 5
Security Compass	Secure Development	1 of 5	3	1	0.1	0.07	0.03	0.04	0.01	3.25, 1 of 5
Security Compass	Risk Assessments	1 of 5	4	1	0.07	0.11	0.03	0.05	0	4.26, 1 of 5
Security Compass	Compliance	1 of 5	4	1	0.14	0.08	0.01	0.07	0	4.3, 1 of 5
Microsoft Annual Report/10K	Embracing our future	1 of 6	4	1	0.16	0.08	0	0	0	4.24, 1 of 6
Microsoft Annual Report/10K	what we offer	1 of 6	4	1	0.2	0.01	0	0	0	4.21, 1 of 6
Microsoft Annual Report/10K	reinvent productivity and business processes	1 of 6	4	1	0.23	0.2	0.01	0	0	4.44, 1 of 6
Microsoft Annual Report/10K	build the intelligent cloud and intelligent edge platform	1 of 6	4	1	0.21	0.26	0.01	0.02	0	4.5, 1 of 6
Microsoft Annual Report/10K	create more personal computing	1 of 6	4	1	0.29	0.14	0.01	0.04	0	4.48, 1 of 6
Microsoft Annual Report/10K	our future opportunity	1 of 6	5	1	0.33	0.18	0.02	0.01	0.05	5.59, 1 of 6
AT&T 10K	Areas of Focus	1 of 7	4	1	0.07	0.07	0.01	0	0	4.15, 1 of 7
AT&T 10K	Communications	1 of 7	3	1	0.07	0.06	0.01	0	0	3.14, 1 of 7
AT&T 10K	wireless service	1 of 7	3	1	0.14	0.18	0.04	0.01	0	3.37, 1 of 7
AT&T 10K	broadband technology	1 of 7	4	1	0.04	0.05	0.01	0	0	4.1, 1 of 7
AT&T 10K	Media	1 of 7	4	1	0.12	0.04	0.02	0.01	0	4.19, 1 of 7
AT&T 10K	Advertising	1 of 7	3	1	0.04	0.04	0.01	0.01	0	3.1, 1 of 7
AT&T 10K	Latin America	1 of 7	3	1	0.03	0.04	0	0	0	3.07, 1 of 7
Optimal IDM Website	Customizable solutions	1 of 8	4	1	0.12	0.06	0.01	0.01	0	4.2, 1 of 8
Optimal IDM Website	superior customer service & support	1 of 8	4	1	0.05	0.04	0.03	0.02	0	4.14, 1 of 8
Optimal IDM Website	security is foundational	1 of 8	3	1	0.05	0.06	0	0	0	3.11, 1 of 8
Optimal IDM Website	scalability	1 of 8	2	1	0.01	0.01	0	0	0	2.02, 1 of 8
Optimal IDM Website	savings	1 of 8	2	1	0.01	0.02	0	0.01	0	2.04, 1 of 8
Optimal IDM Website	managed services	1 of 8	3	1	0.05	0.02	0	0.01	0	3.08, 1 of 8
Optimal IDM Website	speed	1 of 8	3	1	0.05	0.04	0.01	0	0	3.1, 1 of 8
Optimal IDM Website	stability	1 of 8	2	1	0.01	0.02	0.01	0	0	2.04, 1 of 8

Analysis of the Industry Strategy Coding

Document	Strategy	Number of Discrete Strategies	Unpredictable change +0-5	Cyberspace specific *(+1 or -1)	Action Items + 0.01x#	MOS/MOE + 0.01x#	Timelines + 0.01x#	Feedback + 0.01x#	Budget Allocated + 0.01x#	Total
Palo Alto Networks Form 10-k	general	1 of 8	3	1	0.27	0.21	0	0	0	3.48, 1 of 8
Palo Alto Networks Form 10-k	product, subscription and support offerings	1 of 8	4	1	0.43	0.08	0.03	0	0	4.54, 1 of 8
Palo Alto Networks Form 10-k	technology	1 of 8	3	1	0.06	0.07	0	0	0	3.13, 1 of 8
Palo Alto Networks Form 10-k	Research and Development	1 of 8	5	1	0.1	0.07	0.02	0.07	0.01	5.27, 1 of 8
Palo Alto Networks Form 10-k	intellectual property	1 of 8	4	-1	0.13	0.1	0.01	0.02	0	-4.26, 1 of 8
Palo Alto Networks Form 10-k	sales, customer support and marketing	1 of 8	4	-1	0.08	0.08	0.05	0.04	0.02	-4.27, 1 of 8
Palo Alto Networks Form 10-k	manufacturing	1 of 8	3	1	0.05	0.06	0.02	0.03	0	3.16, 1 of 8
Palo Alto Networks Form 10-k	employees	1 of 8	3	-1	0.03	0.01	0.01	0	0	-3.05, 1 of 8
Symantec Corporation Form 10-K	business Strategy	1 of 11	3	1	0.2	0.2	0.01	0	0	3.41, 1 of 11
Symantec Corporation Form 10-K	enterprise security portfolio: integrated cyber defense	1 of 11	2	1	0.11	0.01	0	0	0	2.12, 1 of 11
Symantec Corporation Form 10-K	core services	1 of 11	3	1	0.09	0.07	0	0.02	0	3.18, 1 of 11
Symantec Corporation Form 10-K	control points	1 of 11	3	1	0.2	0.15	0	0.01	0	3.36, 1 of 11
Symantec Corporation Form 10-K	foundation	1 of 11	4	1	0.33	0.18	0.04	0.06	0	4.61, 1 of 11
Symantec Corporation Form 10-K	consumer digital safety portfolio	1 of 11	4	1	0.26	0.17	0.01	0.03	0	4.47, 1 of 11
Symantec Corporation Form 10-K	sales and go-to-market strategy	1 of 11	4	-1	0.44	0	0	0	0	-4.44, 1 of 11
Symantec Corporation Form 10-K	Research and Development	1 of 11	5	1	0.19	0.06	0.05	0	0.02	5.32, 1 of 11
Symantec Corporation Form 10-K	product and technical support	1 of 11	3	-1	0.17	0.02	0.04	0.04	0	-3.27, 1 of 11
Symantec Corporation Form 10-K	intellectual property: protective measures	1 of 11	3	-1	0.2	0.05	0.02	0	0	-3.27, 1 of 11
Symantec Corporation Form 10-K	intellectual property: trademarks, patents, copyrights and licenses	1 of 11	4	-1	0.13	0.08	0.02	0	0	-4.23, 1 of 11
McAfee corporate fact sheet	about mcafee	1 of 12	3	1	0.11	0.16	0.01	0	0	3.28, 1 of 12
McAfee corporate fact sheet	customers	1 of 12	4	-1	0.12	0.17	0.01	0.01	0	-4.31, 1 of 12
McAfee corporate fact sheet	home	1 of 12	3	1	0.13	0.05	0.01	0.01	0	3.2, 1 of 12
McAfee corporate fact sheet	small business	1 of 12	3	1	0.08	0.06	0.02	0.01	0	3.17, 1 of 12
McAfee corporate fact sheet	Commercial & Consumer	1 of 12	3	1	0.05	0.05	0	0	0	3.1, 1 of 12
McAfee corporate fact sheet	enterprise	1 of 12	3	1	0.12	0.1	0.01	0.01	0	3.24, 1 of 12
McAfee corporate fact sheet	mobile	1 of 12	3	1	0.1	0.07	0	0	0	3.17, 1 of 12
McAfee corporate fact sheet	cloud	1 of 12	5	1	0.24	0.13	0	0.02	0	5.39, 1 of 12
McAfee corporate fact sheet	integrated, simple-to-manage solutions	1 of 12	5	1	0.21	0.1	0.05	0.01	0	5.37, 1 of 12
McAfee corporate fact sheet	professional services and support	1 of 12	4	-1	0.1	0.07	0.02	0.03	0	-4.22, 1 of 12
McAfee corporate fact sheet	research	1 of 12	5	1	0.13	0.07	0.01	0	0	5.21, 1 of 12
McAfee corporate fact sheet	innovation	1 of 12	5	1	0.15	0.24	0.02	0.01	0	5.42, 1 of 12
Apple Inc Form 10-K	iphone	1 of 13	2	1	0.03	0.03	0.01	0	0	2.07, 1 of 13
Apple Inc Form 10-K	Mac	1 of 13	2	1	0.03	0.03	0.01	0	0	2.07, 1 of 13
Apple Inc Form 10-K	iPad	1 of 13	2	1	0.04	0.04	0.01	0	0	2.09, 1 of 13
Apple Inc Form 10-K	wearables, home and accessories	1 of 13	3	1	0.08	0.02	0.02	0	0	3.12, 1 of 13
Apple Inc Form 10-K	digital content stores and streaming services	1 of 13	3	1	0.11	0.04	0.01	0	0	3.16, 1 of 13
Apple Inc Form 10-K	AppleCare	1 of 13	2	1	0.05	0	0	0	0	2.05, 1 of 13
Apple Inc Form 10-K	iCloud	1 of 13	3	1	0.03	0.03	0.01	0	0	3.07, 1 of 13
Apple Inc Form 10-K	licensing	1 of 13	1	-1	0.02	0	0	0	0	-1.02, 1 of 13
Apple Inc Form 10-K	other services	1 of 13	2	1	0.04	0	0	0	0	2.04, 1 of 13
Apple Inc Form 10-K	Markets and distribution	1 of 13	3	-1	0.1	0.02	0.01	0.02	0.01	-3.16, 1 of 13
Apple Inc Form 10-K	supply of components	1 of 13	3	1	0.12	0.05	0.01	0	0	3.18, 1 of 13
Apple Inc Form 10-K	Research and Development	1 of 13	5	1	0.1	0.04	0.02	0	0	5.16, 1 of 13
Apple Inc Form 10-K	intellectual property	1 of 13	3	-1	0.23	0.08	0.04	0.01	0	-3.36, 1 of 13
GE Corporation annual report	improve our financial position	1 of 9	2	-1	0.18	0.18	0.04	0.02	0.13	-2.55, 1 of 9
GE Corporation annual report	strengthen our businesses	1 of 9	3	-1	0.13	0.09	0.01	0.02	0	-3.25, 1 of 9
GE Corporation annual report	lean management	1 of 9	4	-1	0.11	0.11	0.03	0.05	0	-4.3, 1 of 9
GE Corporation annual report	potential opportunities	1 of 9	4	-1	0.18	0.17	0.02	0.04	0.02	-4.43, 1 of 9
GE Corporation annual report	power	1 of 9	4	1	0.11	0.14	0.03	0.02	0	4.3, 1 of 9
GE Corporation annual report	renewable energy	1 of 9	4	1	0.09	0.08	0.04	0.04	0	4.25, 1 of 9
GE Corporation annual report	aviation	1 of 9	3	1	0.08	0.09	0.03	0.04	0.01	3.25, 1 of 9
GE Corporation annual report	healthcare	1 of 9	3	1	0.11	0.08	0.02	0.03	0.01	3.25, 1 of 9
GE Corporation annual report	path to growth	1 of 9	5	1	0.12	0.04	0.03	0.03	0.01	5.23, 1 of 9
Akamai Form 10-K	our strategy	1 of 12	5	1	0.35	0.3	0.02	0.05	0	5.72, 1 of 12
Akamai Form 10-K	our solutions	1 of 12	5	1	0.08	0.04	0.02	0	0	5.14, 1 of 12
Akamai Form 10-K	cloud security solutions	1 of 12	5	1	0.3	0.14	0.01	0.01	0	5.46, 1 of 12
Akamai Form 10-K	enterprise security solutions	1 of 12	5	1	0.12	0.09	0.02	0	0	5.23, 1 of 12
Akamai Form 10-K	web and mobile performance solutions	1 of 12	5	1	0.3	0.27	0.08	0.12	0	5.77, 1 of 12
Akamai Form 10-K	media delivery solutions	1 of 12	3	1	0.22	0.2	0.04	0.05	0	3.51, 1 of 12
Akamai Form 10-K	carrier solutions	1 of 12	5	1	0.38	0.14	0.01	0.01	0	5.54, 1 of 12
Akamai Form 10-K	services and support solutions	1 of 12	4	1	0.17	0.14	0.04	0.06	0	4.41, 1 of 12
Akamai Form 10-K	our technology and network	1 of 12	5	1	0.3	0.24	0.02	0.06	0	5.62, 1 of 12
Akamai Form 10-K	customers	1 of 12	3	-1	0.05	0.03	0.03	0.01	0.03	-3.15, 1 of 12
Akamai Form 10-K	sales, services and marketing	1 of 12	4	-1	0.25	0.03	0.01	0	0	-4.29, 1 of 12
Akamai Form 10-K	proprietary rights and licensing	1 of 12	4	-1	0.16	0.03	0.03	0	0	-4.22, 1 of 12

Analysis of the Industry Strategy Coding

Document	Strategy	Number of Discrete Strategies	Unpredictable change +0-5	Cyberspace specific *(+1 or -1)	Action Items + 0.01x#	MOS/MOE + 0.01x#	Timelines + 0.01x#	Feedback + 0.01x#	Budget Allocated + 0.01x#	Total
FireEye Inc Form 10-K	General	1 of 26	5	1	0.22	0.08	0.03	0.08	0.01	5.42, 1 of 26
FireEye Inc Form 10-K	our cybersecurity solutions and services	1 of 26	4	1	0.29	0.03	0.07	0	0	4.39, 1 of 26
FireEye Inc Form 10-K	threat detection and prevention solutions	1 of 26	4	1	0.25	0.1	0	0.01	0	4.36, 1 of 26
FireEye Inc Form 10-K	network security and network forensics solutions	1 of 26	3	1	0.17	0.1	0.02	0.01	0	3.3, 1 of 26
FireEye Inc Form 10-K	email security solutions	1 of 26	3	1	0.28	0.06	0	0.01	0	3.35, 1 of 26
FireEye Inc Form 10-K	endpoint security solutions	1 of 26	3	1	0.19	0.07	0.03	0.01	0	3.3, 1 of 26
FireEye Inc Form 10-K	cloud security solutions	1 of 26	3	1	0.1	0.07	0	0.01	0	3.18, 1 of 26
FireEye Inc Form 10-K	customer support and maintenance services	1 of 26	4	1	0.1	0.05	0.01	0.05	0	4.21, 1 of 26
FireEye Inc Form 10-K	helix security platform	1 of 26	5	1	0.23	0.11	0.01	0.03	0	5.38, 1 of 26
FireEye Inc Form 10-K	security validation platform	1 of 26	3	1	0.19	0.04	0.01	0.02	0	3.26, 1 of 26
FireEye Inc Form 10-K	threat intelligence solutions	1 of 26	4	1	0.18	0.01	0.01	0.01	0	4.21, 1 of 26
FireEye Inc Form 10-K	on-demand and managed service-as-a-service solutions	1 of 26	5	1	0.2	0.08	0.03	0.03	0	5.34, 1 of 26
FireEye Inc Form 10-K	professional services	1 of 26	3	1	0.23	0	0	0.12	0	3.35, 1 of 26
FireEye Inc Form 10-K	our technologies	1 of 26	5	1	0.13	0.04	0	0.01	0	5.18, 1 of 26
FireEye Inc Form 10-K	advanced threat detection and prevention technologies	1 of 26	5	1	0.18	0.03	0	0	0	5.21, 1 of 26
FireEye Inc Form 10-K	advanced endpoint validation and containment	1 of 26	4	1	0.13	0	0.02	0.01	0	4.16, 1 of 26
FireEye Inc Form 10-K	security validation	1 of 26	3	1	0.01	0.01	0.01	0.01	0	3.04, 1 of 26
FireEye Inc Form 10-K	evolved security architecture and security orchestration	1 of 26	5	1	0.26	0.11	0.01	0.02	0	5.4, 1 of 26
FireEye Inc Form 10-K	customers	1 of 26	3	-1	0.1	0.06	0.05	0.05	0.03	-3.29, 1 of 26
FireEye Inc Form 10-K	sales	1 of 26	4	-1	0.44	0.19	0.03	0.05	0	-4.71, 1 of 26
FireEye Inc Form 10-K	marketing	1 of 26	3	-1	0.28	0.01	0.01	0.01	0	-3.31, 1 of 26
FireEye Inc Form 10-K	technology alliance partners	1 of 26	5	1	0.18	0.1	0.01	0.01	0	5.3, 1 of 26
FireEye Inc Form 10-K	government affairs	1 of 26	5	-1	0.15	0.07	0.02	0.03	0	-5.27, 1 of 26
FireEye Inc Form 10-K	manufacturing	1 of 26	3	1	0.17	0.05	0.1	0.03	0	3.35, 1 of 26
FireEye Inc Form 10-K	Research and Development	1 of 26	5	1	0.43	0.26	0.03	0.11	0.02	5.85, 1 of 26
FireEye Inc Form 10-K	intellectual property	1 of 26	4	-1	0.25	0.06	0.02	0	0	-4.33, 1 of 26
Splunk Strategy and Growth strategy from Form	AIOPS: Artificial Intelligence for IT operations	1 of 38	5	1	0.2	0.1	0.04	0.01	0	5.35, 1 of 38
Splunk Strategy and Growth strategy from Form	The Splunk Analytics-Driven Solution	1 of 38	5	1	0.31	0.24	0.02	0	0	5.57, 1 of 38
Splunk Strategy and Growth strategy from Form	Security Nerve Center	1 of 38	5	1	0.38	0.26	0.05	0.02	0	5.71, 1 of 38
Splunk Strategy and Growth strategy from Form	Get the value out of AI and Machine Learning	1 of 38	5	1	0.32	0.28	0.04	0	0	5.64, 1 of 38
Splunk Strategy and Growth strategy from Form	Real-Time Enterprise Log Managmeent to Search, Diagnose,	1 of 38	5	1	0.39	0.32	0.04	0.05	0	5.8, 1 of 38
Splunk Strategy and Growth strategy from Form	Platform for Big Data Analytics	1 of 38	5	1	0.19	0.06	0.02	0.03	0	5.3, 1 of 38
Splunk Strategy and Growth strategy from Form	extend our technological capabilities	1 of 38	4	1	0.2	0.1	0	0	0.02	4.32, 1 of 38
Splunk Strategy and Growth strategy from Form	continue to expand our direct and indirect sales organization.	1 of 38	4	-1	0.12	0.04	0	0	0.03	-4.19, 1 of 38
Splunk Strategy and Growth strategy from Form	further penetrate our existing customer base and drive enterpri	1 of 38	3	-1	0.15	0.03	0.03	0.03	0	-3.24, 1 of 38
Splunk Strategy and Growth strategy from Form	enhance our value proposition through a focus on solutions w	1 of 38	4	1	0.11	0.03	0.01	0	0.01	4.16, 1 of 38
Splunk Strategy and Growth strategy from Form	Grow our user communities and partner ecosystem to increas	1 of 38	3	-1	0.08	0.07	0.01	0.01	0.01	-3.18, 1 of 38
Splunk Strategy and Growth strategy from Form	continue to deliver a rich developer environment...	1 of 38	5	1	0.07	0.04	0	0	0.01	5.12, 1 of 38
Splunk Strategy and Growth strategy from Form	Pricing	1 of 38	3	-1	0.1	0.02	0.03	0	0	-3.15, 1 of 38
Splunk Strategy and Growth strategy from Form	key technologies	1 of 38	1	1	0.07	0.02	0	0	0.01	1.1, 1 of 38
Splunk Strategy and Growth strategy from Form	schema-on-the-fly	1 of 38	5	-1	0.12	0.03	0.02	0	0	-5.17, 1 of 38
Splunk Strategy and Growth strategy from Form	machine data platform	1 of 38	5	1	0.11	0.05	0.01	0.01	0	5.18, 1 of 38
Splunk Strategy and Growth strategy from Form	search processing language	1 of 38	5	1	0.13	0.05	0.02	0.01	0	5.21, 1 of 38
Splunk Strategy and Growth strategy from Form	machine learning	1 of 38	5	1	0.09	0.08	0.01	0	0	5.18, 1 of 38
Splunk Strategy and Growth strategy from Form	splunk enterprise and splunk cloud	1 of 38	5	1	0.61	0.24	0.09	0.03	0	5.97, 1 of 38
Splunk Strategy and Growth strategy from Form	Technology architecture collection	1 of 38	3	1	0.21	0.05	0	0	0	3.26, 1 of 38
Splunk Strategy and Growth strategy from Form	Technology architecture indexing	1 of 38	5	1	0.14	0.06	0.01	0	0	5.21, 1 of 38
Splunk Strategy and Growth strategy from Form	Technology architecture search	1 of 38	5	1	0.13	0.06	0	0	0	5.19, 1 of 38
Splunk Strategy and Growth strategy from Form	Technology architecture core functions	1 of 38	5	1	0.13	0.06	0	0	0	5.19, 1 of 38
Splunk Strategy and Growth strategy from Form	Technology architecture archive to hadoop and amazon S3	1 of 38	5	1	0.05	0.03	0.01	0	0	5.09, 1 of 38
Splunk Strategy and Growth strategy from Form	Technology architecture SDKs and APIs	1 of 38	5	1	0.04	0	0	0	0	5.04, 1 of 38
Splunk Strategy and Growth strategy from Form	Technology architecture App development environment	1 of 38	5	1	0.09	0.04	0	0	0	5.13, 1 of 38
Splunk Strategy and Growth strategy from Form	splunk product deployments	1 of 38	4	1	0.32	0.24	0.01	0	0	4.57, 1 of 38
Splunk Strategy and Growth strategy from Form	services	1 of 38	3	-1	0.08	0.02	0.02	0	0	-3.12, 1 of 38
Splunk Strategy and Growth strategy from Form	maintenance and customer support	1 of 38	3	-1	0.19	0.05	0.03	0.02	0	-3.29, 1 of 38
Splunk Strategy and Growth strategy from Form	training services	1 of 38	2	-1	0.05	0.01	0	0	0	-2.06, 1 of 38
Splunk Strategy and Growth strategy from Form	professional services	1 of 38	3	-1	0.06	0.02	0.01	0.01	0	-3.1, 1 of 38
Splunk Strategy and Growth strategy from Form	partner and developer ecosystem	1 of 38	5	1	0.25	0.14	0.02	0.03	0	5.44, 1 of 38
Splunk Strategy and Growth strategy from Form	splunk communities	1 of 38	5	1	0.23	0.06	0.01	0.1	0	5.4, 1 of 38
Splunk Strategy and Growth strategy from Form	sales	1 of 38	4	-1	0.52	0.08	0.01	0.08	0.01	-4.7, 1 of 38
Splunk Strategy and Growth strategy from Form	marketing	1 of 38	3	-1	0.23	0.14	0.01	0	0	-3.38, 1 of 38
Splunk Strategy and Growth strategy from Form	Research and Development	1 of 38	5	1	0.11	0.1	0.01	0.02	0.01	5.25, 1 of 38
Splunk Strategy and Growth strategy from Form	intellectual property	1 of 38	3	-1	0.16	0.01	0	0	0	-3.17, 1 of 38
Splunk Strategy and Growth strategy from Form	customers	1 of 38	3	-1	0.17	0.03	0.02	0	0	-3.22, 1 of 38

LIST OF REFERENCES

- A&E Television Networks. (2018, August). 9 *Groundbreaking early submarines*. History.com. <https://www.history.com/news/9-groundbreaking-early-submarines>
- Akamai Technologies Inc. (2019). *Akamai annual report 2019*. <https://www.ir.akamai.com/static-files/569d1024-6d2c-4fdd-bfd5-9ae3d5c85eab>
- Alford, J., & Greve, C. (2017). Strategy in the public and private sectors: Similarities, differences and changes. *Administrative Sciences; Basel*, 7(4), 35. <https://www.mdpi.com/2076-3387/7/4/35/htm>
- Appelbaum, S. H., Habashy, S., Malo, J.-L., & Shafiq, H. (2012). Back to the future: Revisiting Kotter's 1996 change model. *The Journal of Management Development; Bradford*, 31(8), 764–782. doi:10.1108/02621711211253231
- Apple Inc. (2019, September). *Apple Inc. form 10-K*. SEC.gov. <https://www.sec.gov/Archives/edgar/data/320193/000032019319000119/a10-k20199282019.htm>
- Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12(2), 141–165. https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf
- Aten, K., & Thomas, G. F. (2016). Crowdsourcing strategizing: Communication technology affordances and the communicative constitution of organizational strategy. *International Journal of Business Communication*, 1–33. <https://calhoun.nps.edu/handle/10945/48658>
- Aucsmith, D. (2016). Disintermediation, counterinsurgency, and cyber defense. In H. Lin and A. Zegart (Eds.), *Bytes, bombs, and spies: The strategic dimensions of offensive cyber operations* (pp. 343–56). Brookings Institution Press.
- Bank of America. (2020). *Bank of America's strategy of responsible growth*. <https://about.bankofamerica.com/en-us/who-we-are/our-strategy.html#fbid=Lmh6FmRAfD7>
- Bry, N. (2018, April 11). A manager's guide to disruptive innovation by Philippe Silberzahn (2/2). *Rapid Innovation in Digital Time*. <https://nbry.wordpress.com/2018/04/11/a-managers-guide-to-disruptive-innovation-by-philippe-silberzahn-2-2/>
- Bryson, J. M., & Roering, W. D. (2007). Applying private-sector strategic planning in the public sector. *Journal of the American Planning Association*. doi:10.1080/01944368708976631

- Bunker, K., Gechman, A., & Rush, J. (2012). Learning to lead in a volatile and uncertain world: Making experience really matter. *Business Strategy Series*; Northampton, 13(6), 288–294. doi:10.1108/17515631211286137
- Congressional Research Service. (2019). *Critical infrastructure: Emerging trends and policy considerations for Congress*. FAS.org. <https://fas.org/sgp/crs/homesecc/R45809.pdf>
- Christensen, C. M. (2001). The past and future of competitive advantage. *MIT Sloan Management Review*; Cambridge, 42(2), 105–109. <https://search.proquest.com/docview/224968687/abstract/786A7AF8765C4F88PQ/1>
- Christensen, C. M. (2002). The opportunity and threat of disruptive technologies. *MRS Bulletin*, 27(4), 278–282. doi:10.1557/mrs2002.81
- Christensen, C. M., & Bower, J. L. (1996). Customer power, strategic investment, and the failure of leading firms. *Strategic Management Journal (1986-1998)*, 17(3), 197.
- Christensen, C. M., Hang, C.-C., Chai, K.-H., & Subramanian, A. M. (2010). Editorial managing innovation in emerging economies: An introduction to the special issue. *IEEE Transactions on Engineering Management*, 57(1), 4–8. doi:10.1109/TEM.2009.2036601
- Christensen, C. M., McDonald, R., Altman, E. J., & Palmer, J. E. (2018). Disruptive innovation: An intellectual history and directions for future research. *Journal of Management Studies*, 55(7), 1043–1078. doi:10.1111/joms.12349
- Christensen, C. M., Suarez, F. F., & Utterback, J. M. (1998). Strategies for survival in fast-changing industries. *Management Science*; Linthicum, 44(12), S207–S220. <https://search.proquest.com/docview/213238823/abstract/FC582E77F804484EPQ/1>
- Cisco. (2019, October). *2019 Annual report: Defining the future of the internet*. https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2019.pdf
- Clinton, L. (2015). Best practices for operating government-industry partnerships in cyber security. *Journal of Strategic Security*; San Jose, 8(4), 53–68. doi:10.5038/1944-0472.8.4.1456
- Computer Crime and Intellectual Property Section Criminal Division. (2015). *Prosecuting computer crimes*. Office of Legal Education Executive Office for United States Attorneys. <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>
- Deal, K. (2013). *Strategy and investment planning*, DRM-2013-U-006208. CNA Analysis & Solutions.

- Defense Advanced Research Projects Agency. (n.d.). *Paving the way to the modern internet*. Retrieved May 18, 2020, from <https://www.darpa.mil/about-us/timeline/modern-internet>
- Demchak, C. C. (2012). Resilience and cyberspace: recognizing the challenges of a global socio-cyber infrastructure (GSCI). *Journal of Comparative Policy Analysis: Research and Practice*, 14(3), 254–269. doi:10.1080/13876988.2012.687619
- Edgescan. (2020). *Effective, scalable, #fullstack vulnerability management* [Brochure]. BCC Risk Advisory Ltd.
- Edmonds, J. (2011). Managing successful change. *Industrial and Commercial Training; Guildsborough*, 43(6), 349–353. doi:10.1108/00197851111160478
- Emmott, S., (2006), *Towards 2020 science*. Microsoft. https://code.org/curriculum/science/files/CS_in_Science_Background_papers.pdf
- FireEye, Inc. (2019, December 31). *FireEye, Inc. form 10-K*. <https://investors.fireeye.com/node/14176/html#sEBF126F99B3E578498E9DBDBC72EEF75>
- First Research. (2017). Surveillance, investigation & security consulting services - quarterly update 10/23/2017. *First Research Industry Profiles*. <http://libproxy.nps.edu/login?url=https://search-proquest-com.libproxy.nps.edu/docview/1957763857?accountid=12702>
- Gartzke, E. (2013). The myth of cyberwar: bringing war on the internet back down to earth. *International Security*, 38(2), 41–73. doi:10.1162/ISEC_a_00136
- General Electric Company. (2019). *GE 2019 annual report*. https://www.ge.com/investor-relations/sites/default/files/GE_AR19_AnnualReport.pdf
- Gillentine, A. (2010). Cyber operations require government, industry collaboration. *Colorado Springs Business Journal (CO)*.
- Gilliland, D. (2019). America's cyber blind spot. *The Hill*. <https://thehill.com/opinion/cybersecurity/461452-americas-cyber-blind-spot>
- Giniat, E. J., Benton, B., Biegansky, E., & Grossman, R. (2012). People and change management in an uncertain environment. *Healthcare Financial Management; Westchester*, 66(10), 84–89. <https://search.proquest.com/docview/1266005971/abstract/8D2FCD63711A44B1PQ/1>
- Horney, N., Eckenrod, M., McKinney, G., & Prescott, R. (2014). From change projects to change agility. *People and Strategy*, 37(1), 40–45. <https://search.proquest.com/docview/1753212722/abstract/2B8CCA8F85F74136PQ/1>

- Hechanova, M. R. M., Caringal-Go, J. F., & Magsaysay, J. F. (2018). Implicit change leadership, change management, and affective commitment to change. *Leadership & Organization Development Journal; Bradford*, 39(7), 914–925. doi:10.1108/LODJ-01-2018-0013
- Intel Corporation. (2019). *Intel 2018 online annual report*. <https://intel2019or.q4web.com/Y2018/default.aspx#>
- International Encyclopedia of the First World War. (2017, July). *Submarines and submarine warfare*. https://encyclopedia.1914-1918-online.net/article/submarines_and_submarine_warfare
- Ixia. (2016, December 31). *Ixia form 10-K*. SEC.gov. <https://www.sec.gov/Archives/edgar/data/1120295/000112029517000006/a2016q4form10-k.htm>
- Johnson, B. D. B. (2019). *For U.S. Government, cybersecurity is becoming a team sport*. FCW. <https://fcw.com/articles/2019/08/02/cyber-team-sport-johnson.aspx>
- Joint Chiefs of Staff. (2017, June 16). *JP 5-0, Joint Planning*. <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/5-0-Planning-Series/>
- Joint Chiefs of Staff. (2020). *DOD Dictionary of Military and Associated Terms*. <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-01-24-100230-123>
- Kallberg, J., & Cook, T. S. (2017). The unfitness of traditional military thinking in cyber. *IEEE Access*, 5, 8126–8130. doi:10.1109/ACCESS.2017.2693260
- Kane, G. C. (2017). *Digital disruption is a people problem*. MIT Sloan Management Review. <https://sloanreview.mit.edu/article/digital-disruption-is-a-people-problem/>
- Keller, C., & Widger, D. (2019). *On war, by General Carl von Clausewitz*. Project Gutenberg EBook. <https://www.gutenberg.org/files/1946/1946-h/1946-h.htm>
- Kettinger, W. J., Teng, J. T. C., & Guha, S. (1997). Business process change: A study of methodologies, techniques, and tools. *MIS Quarterly; Minneapolis*, 21(1), 55–80. <https://search.proquest.com/docview/218130935/abstract/77A2F2AF85C54DD3PQ/1>
- King, A. A., & Baatartogtokh, B. (2015). How useful is the theory of disruptive innovation? *MIT Sloan Management Review; Cambridge*, 57(1), 77–90. <http://search.proquest.com/docview/1719426267/abstract/4BB73271C85549ABPQ/1>

- King, A., & Gallagher, M. (2020). *United States of America Cyberspace Solarium Commission executive summary*. U.S. Cyberspace Solarium Commission. <https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view>
- Kotter, J. (1978). *Organizational dynamics: diagnosis and intervention*. Reading, Mass: Addison-Wesley Pub. Co.
- Kotter, J. (1979). *Power in management*. AMACOM.
- Kotter, J. (1988). *The leadership factor*. Free Press.
- Kotter, J. (1999). *John P. Kotter on what leaders really do*. Harvard Business School Press.
- Lee, S., Trimi, S., & Kim, C. (2013). Innovation and imitation effects' dynamics in technology adoption. *Industrial Management & Data Systems*, 113(6), 772–799. doi:10.1108/IMDS-02-2013-0065
- Liedtka, J., & Kaplan, S. (2019). How design thinking opens new frontiers for strategy development. *Strategy & Leadership*. doi:10.1108/SL-01-2019-0007
- Liedtka, J. M., & Rosenblum, J. W. (1996). Shaping conversations: Making strategy, managing change. *California Management Review*, 39(1), 141–157. <https://search.proquest.com/docview/216134602/abstract/49B8413DE0A5495CPQ/1>
- Lindsay, J., & Hopkins, M. (2010). From experience: Disruptive innovation and the need for disruptive intellectual asset strategy. *Journal of Product Innovation Management*, 27(2), 283–290. doi:10.1111/j.1540-5885.2010.00715
- Leavy, B. (2014). Strategy, organization and leadership in a new “transient-advantage” world. *Strategy & Leadership*, 42(4), 3–13. doi:10.1108/SL-05-2014-0038
- Maroney, T. (2017). Opinion: The boring life of a private investigator. *New York Times*. <https://www.nytimes.com/2015/03/07/opinion/the-boring-life-of-a-private-investigator.html>
- Mayer, P., & Vambery, R. G. (2008). Aligning global business strategy planning models with accelerating change. *Journal of Global Business and Technology; Huntington Station*, 4(1), 31–48. <https://search.proquest.com/docview/216934164/abstract/44DE7EDAC5B44829PQ/1>
- McAfee LLC. (2020). *About McAfee*. <https://www.mcafee.com/enterprise/en-us/assets/fact-sheets/fs-mcafee-fact-sheet.pdf>

- McFarland, W. (2015). Mastering change management. *Public Manager*, 44(1), 23–24. <https://search.proquest.com/docview/1688353781/citation/B29538B7705E4CE9PQ/1>
- McMillan, C., & Overall, J. (2016). Wicked problems: Turning strategic management upside down. *The Journal of Business Strategy*, 37(1), 34–43. doi:10.1108/JBS-11-2014-0129
- Merali, Y., Papadopoulos, T., & Nadkarni, T. (2012). Information systems strategy: Past, present, future? *Journal of Strategic Information Systems*, 21, 125–153. doi:10.1016/j.jsis.2012.04.002
- Microsoft. (2019). *Microsoft 2019 annual report*. <https://www.microsoft.com/investor/reports/ar19/index.html>
- Mireles, J. D., Ficke, E., Cho, J., Hurley, P., & Xu, S. (2019). Metrics towards measuring cyber agility. *IEEE Transactions on Information Forensics and Security*, 14(12), 3217–3232. doi:10.1109/TIFS.2019.2912551
- Murphy, L. (2011, October). *5 Companies that are using big data & gamification to disrupt market research*. GreenBook. <https://greenbookblog.org/2011/10/16/5-companies-that-are-using-big-data-gamification-to-disrupt-market-research/>
- National Conference of State Legislatures. (2019, February 8). *Cybersecurity legislation 2018*. <http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx>
- Norton. (2018). *2017 Norton cyber security insights report*. <https://us.norton.com/cyber-security-insights-2017>
- Nunes, P. F., & Downes, L. (2019). *Big bang disruption: The innovator's disaster*. Accenture Outlook. <https://www.accenture.com/us-en/insight-outlook-big-bang-disruption-innovators-disaster>
- Optimal IDM. (2020). *Optimal IdM: Who we are*. <https://optimalidm.com/why-optimal/>
- Palo Alto Networks, Inc. (2019, July 31). *Palo Alto Networks, Inc. form 10-K*. <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001327567/6b9031d3-1bed-4db4-a694-aaa7811418a1.pdf>
- Perry, J. L., & Rainey, H. G. (1988). The public-private distinction in organization theory: A Cr. Academy of Management. *The Academy of Management Review*, 13(2), 182. <https://search.proquest.com/docview/210938313/abstract/E3CF261C1A6E473APQ/1>

- Petrack, I. J., & Martinelli, R. (2012). Driving disruptive innovation: Problem finding and strategy setting in an uncertain world. *Research Technology Management*, 55(6), 49–57. <https://search.proquest.com/docview/1247867503/abstract/E2A6A1A2345F4138PQ/1>
- Poister, T. H. (2010). The future of strategic planning in the public sector: Linking strategic management and performance. *Public Administration Review*, 70(S1), S246–S254. doi:10.1111/j.1540-6210.2010.02284
- Prosci. (n.d.). *The history and future of change management*. Retrieved June 9, 2020, from <https://www.prosci.com/resources/articles/change-management-history-and-future>
- Rick, T. (2020, February). *How and why organizational culture eats strategy for breakfast, lunch and dinner*. SupplyChain 24/7. https://www.supplychain247.com/article/organizational_culture_eats_strategy_for_breakfast_lunch_and_dinner/legacy_supply_chain_services
- Rogers, E. M. (1999). Anatomy of the two subdisciplines of communication study. *Human Communication Research*, 25(4), 618–631. doi:10.1111/j.1468-2958.1999.tb00465
- Rogers, E. M. (2002). Diffusion of preventive innovations. *Addictive Behaviors*, 27(6), 989–993. doi:10.1016/s0306-4603(02)00300-3
- Rogers, E. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- Rogers, E., & Agarwala-Rogers, R. (1976). *Communication in organizations*. Free Press.
- Security Compass. (2020). *About SD elements: The solution to the development devil's choice. Go fast. Stay safe*. <https://securitycompass.com/sdelements>
- Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
- Sood, A., & Tellis, G. (2011). Demystifying disruption: A new model for understanding and predicting disruptive technologies. *Marketing Science*, 30(2), 339–354. <https://www.jstor.org/stable/23012004>
- Splunk Inc. (2020). *FY2020 annual report and proxy statement*. <https://investors.splunk.com/static-files/993ab50b-19d1-44b0-826b-071d82c77d87>
- Splunk Inc. (2020). *Splunk vision*. https://www.splunk.com/en_us/about-us/business-strategy-and-vision.html

- Strawn, G., & Strawn, C. (2015). Moore's Law at fifty. *IT Professional*, 17(6), 69–72. doi:10.1109/MITP.2015.109
- Symantec Corporation. (2018, March 30). *Symantec Corporation form 10-K* https://www.sec.gov/Archives/edgar/data/849399/000119312518309091/d573170d10k.htm#osl573170_1
- Symantec Corporation. (2019). *How do cybercriminals get caught?* Norton. <https://us.norton.com/internetsecurity-emerging-threats-how-do-cybercriminals-get-caught.html>
- Tamilarasu, V. (2012). Change management. *International Journal of Management Prudence*, 4(2), 26–31. <https://search.proquest.com/docview/1490677206/abstract/BF8CAA718A7342D1PQ/1>
- Tesla. (2019). *Tesla impact report*. https://www.tesla.com/ns_videos/tesla-impact-report-2019.pdf
- TOP500.org. (2019). *Performance development*. <https://www.top500.org/statistics/perfdevel/>
- United States Department of Defense. (2018a). *Department of Defense cyber strategy summary 2018*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
- United States Department of Defense. (2018b). *Summary of the 2018 national defense strategy of the United States of America: Sharpening the American military's competitive edge*. <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>
- United States Government Accountability Office. (2013). *GAO-13-462T, Cyberspace a better defined and implemented national strategy is needed to address persistent challenges* (Testimony GAO-13-462T). <https://www.gao.gov/assets/660/652817.pdf>
- United States Government Accountability Office. (2017). *GAO-686347, DOD's monitoring of progress in implementing cyber strategies can be strengthened* (Testimony GAO-17-512). <https://www.gao.gov/products/GAO-17-512>
- U.S. Cyber Command. (2018). *Achieve and maintain cyberspace superiority; Command vision for U.S. Cyber Command*. <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>
- U.S. Cyber Command. (2019). *Command history*. <https://www.cybercom.mil/About/History/>

- Van Der Wal, Z., De Graaf, G., & Lasthuizen, K. (2008). What's valued most? Similarities and differences between the organizational values of the public and private sector. *Public Administration*, 86(2), 465–482. doi:10.1111/j.1467-9299.2008.00719
- Van Rensburg, D. J. (2015). In-sourcing disruptive brands as a corporate entrepreneurship strategy. *International Entrepreneurship and Management Journal*, 11(4), 769–792. doi:10.1007/s11365-014-0309-4
- Vergun, D. (2020, March 16). *Submarine warfare played major role in World War II victory*. U.S. Department of Defense. <https://www.defense.gov/Explore/Features/Story/Article/2114035/submarine-warfare-played-major-role-in-world-war-ii-victory/>
- White House. (2016). *Fact sheet: Cybersecurity national action plan*. <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>
- White House. (2018). *National cyber strategy of the United States of America*. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
- Wiltbank, R., Dew, N., Read, S., & Sarasvathy, S. D. (2006). What to do next? The case for non-predictive strategy. *Strategic Management Journal*, 27(10), 981–998. <https://www.jstor.org/stable/20142390>
- Woahika. (2018, March 15). *The shark-fin effect: The alternative adoption process for digital disruptive products*. Bocconi Students for Digital Consulting. <https://bsdigitalconsulting.wordpress.com/2018/03/15/the-shark-fin-effect-the-alternative-adoption-process-for-digital-disruptive-products/>
- Worley, C. G., Williams, T., & Lawler, E. E. (2016). Creating management processes Built for Change. *MIT Sloan Management Review*, 58(1), 77–82. <https://search.proquest.com/docview/1832180675/abstract/57E9B3CF1A0F4F6EPQ/1>
- Walsh, S. T., Kirchhoff, B. A., & Newbert, S. (2002). Differentiating market strategies for disruptive technologies. *IEEE Transactions on Engineering Management*, 49(4), 341–351. doi:10.1109/TEM.2002.806718
- Yang, Q., & Zhang, Y. (2013). Research of disruptive diversification strategy and the synergy effect. *Applied Mechanics and Materials*, 409–410, 1587. doi:10.4028/www.scientific.net/amm.409-410.1587
- Zeng, Y., Dong, P., Shi, Y., & Li, Y. (2018). On the disruptive innovation strategy of renewable energy technology diffusion: An agent-based model. *Energies*, 11(11), 3217. doi:10.3390/en11113217

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California