Shadow Warrior:

The Outsourcing of the United States' Offensive Cyber Capabilities

---

July 2021

University of Glasgow: 2478010

Dublin City University: 19108796

Charles University in Prague: 42696365

Presented in partial fulfilment of the requirements for the degree of

International Masters

in

Security, Intelligence & Strategic Studies

Word Count: 22264

Written By: Ashley Jones

Supervisor: David Erkomashvili

Date of Submission: July 2021

Abstract

The cyberspace has emerged as a conscientious topic for military leaders and senior policymakers as they attempt to ensure critical national infrastructure is secured against cyberattacks. The previous decade has seen the re-emergence of the state actor as a primary threat actor; a large-scale threat actor that is heavily funded, well equipped, and has the ability to avoid legal ramifications for their actions. The cyberspace presented new opportunities of attack and manoeuvre below the threshold of armed response and has transformed the way conflicts are fought and disputes are resolved. This dissertation aims to analyse the effect that the private sector has on the United States' offensive cyber capabilities. Specifically, this research will answer the question of 'How does the private sector support the development of the United States offensive cyber capabilities?'

To meet the growing threat of cyber warfare, new organisational structures were rapidly devised and established within the U.S. Department of Defense. Literature on the two key themes, the cyberspace as a strategic capability and the cyberspace as an outsourced commodity, was reviewed to determine the factors contributing to the increase in outsourcing offensive cyber capabilities. Then a qualitative case study on the newest branch of the United States military, U.S. Cyber Command was conducted to investigate the use of private sector support within U.S. Cyber Command to identify the offensive cyber capabilities being outsourced. Subsequently, the discussion assessed and evaluated the effects that outsourcing has on the ability of the United States to conduct offensive cyber operations.

The result of the research indicates that the United States relies heavily on the private sector to contribute a vital role, not only in the development of the offensive cyber capabilities but also the overall cyber capabilities of the United States. The U.S. partners with multiple organisations to fulfil their needs, this research has shown how the U.S. Cyber Command relies heavily on these

industrial partners to meet the basic specification necessary to operate as a full unified command. This is indicative of a poorly funded, underequipped, and understaffed organisation that is incapable of defending its networks against adversaries. Moreover, the lack of norms within the cyberspace has contributed to an ethical dilemma that arose out of the blurred lines of operations and the unclear international legal status of contractors. The outcomes reached in this dissertation were qualitative and subjective to interpretation, however, it sets a precedence for similar future work to be conducted on other federal agencies, as well as, contrasted against similar research on other nations use of outsourcing.

Key Words: Cyberspace, Cyberspace Operations, Cyber Warfare, Offensive Cyber Capabilities, Defence Contractors, Outsourcing, Private Sector, United States Cyber Command

Acknowledgements

The author would like to thank his supervisor, David Erkomashvili, for the guidance provided during the proposal stage, for his monthly review of completed work, as well as, his feedback on the individual chapters. Thank you.

Table of Contents

Abstract ii
Acknowledgements iv
Table of Contents v
List of Illustrative Materials viii
List of Abbreviations ix

CHAPTER ONE: INTRODUCTION 1
Background 1
Statement of Problem 2
Research Aim and Objectives 4
Research Question 4
Purpose of the Research 5
Structure of Dissertation 5
Definition of Key Terminology 7

CHAPTER TWO: LITERATURE REVIEW 9
Introduction 9
The Cyberspace as a Strategic Capability 9
The Delineation of Cyber Warfare 9
The Adoption of Cyber Capabilities 12
The Strategic Thought Process of Cyber 14
The Cyberspace as an Outsourced Commodity 17
The History of Military Outsourcing 17
The Expansion of Cyber Outsourcing 19
The Ethical Dilemma of Outsourcing 21
Conclusion 23
Summary 24

CHAPTER THREE: RESEARCH DESIGN 27
Introduction 27
Rationale 27

Methodology 29
Significance 31
Limitations 32
Hypotheses 33
Conclusion 36
Summary 36

CHAPTER FOUR: FINDINGS 39
Introduction 39
Case Study: U.S. Cyber Command 39
Background 39
Full Operational Capabilities 43
Interagency Partnerships 46
Tendering of Contracts 47
Private-Sector Partnerships 49
Hypothesis Testing 54
Conclusion 56
Summary 57

CHAPTER FIVE: DISCUSSION AND RECOMMENDATIONS 60
Introduction 60
Discussion of Findings 60
Key Theme: The Insufficient Ethical and Legal Frameworks 61
Key Theme: The Blurred Lines of Operations 63
Key Theme: The Lack of Accountability and Oversight 65
Recommendations 67
Update International Agreements and Establish Norms 67
Implement Additional Instruments of Accountability 68
Enhance Cyber Education Offerings 68
Apply a Shift in Strategic Thinking 69
Areas of Future Research 69
Conclusion 70

Summary 71

CHAPTER SIX: CONCLUSION 73

Conclusion 73

BIBLIOGRAPHY 77

List of Illustrative Materials

Figure 1: U.S. Cyber Command Organisational Structure as of June 2018 40
Figure 2: Department of Defense Cyber Mission Force Relationships 43
Figure 3: The Conceptual Diagram of the Joint Cyber Warfighting Architecture Programme.....46

List of Abbreviations

AFCYBER	U.S. Air Force Cyber Command
APT	Advanced Persistent Threat
ARCYBER	U.S. Army Cyber Command
ARPA	Advanced Research Project Agency
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCMD	Combatant Command
CCMF	Cyber Combat Mission Force
CMF	Cyber Mission Force
CNMF	Cyber National Mission Force
CPT	Cyberspace Protection Team
DCO	Defensive Cyberspace Operations
DDOS	Distributed Denial of Service
DevSecOps	Software Development Security Operations
DHS	Department of Homeland Security
DIRNSA	Director of the National Security Agency
DISA	Defense Information Service Agency
DoD	U.S. Department of Defense
DoDIN	Department of Defense Information Network
ENISA	European Union Agency for Cybersecurity
FLTCYBER	U.S. Fleet Cyber Command
FY	Financial Year
FYDP	Future Years Defense Program
GAO	Government Accountability Office (U.S.)
GSA	General Service Administration
IDIQ	Indefinite Delivery / Indefinite Quantity
ISP	Internet Service Provider
JCWA	Joint Cyber Warfighting Architecture
JFCC-NW	Joint Functional Component Command – Network Warfare

JFHQ	Joint Force Headquarters
JTF	Joint Task Force
JTF-CND	Joint Task Force – Computer Network Defense
JTF-CNO	Joint Task Force – Computer Network Operations
JTF-GNO	Joint Task Force – Global Network Operations
MARFORCYBER	U.S. Marines Force Cyber Command
MoD	U.K. Ministry of Defence
NATO	North Atlantic Treaty Organisation
NMF	National Mission Force
NSA	National Security Agency
OCO	Offensive Cyberspace Operations
PCTE	Persistent Cyber Training Environment
PMC	Private Military Contractors
PMSC	Private Military and Security Companies
P-OTA	Production - Other Transaction Agreement
PPBE	Planning, Programming, Budgeting, and Execution
RCC	Regional Cyber Centres
RFI	Request for Information
RFP	Request for Proposals
SCC	Service Cyber Components
SPACECOM	U.S. Space Command
TRIDENT	Training, Readiness, Integration, Delivery, and Enterprise Technology
TTPs	Tools, Tactics, and Procedures
U.K.	United Kingdom
U.S.	United States
USCYBERCOM	U.S. Cyber Command
USSTRATCOM	U.S. Strategic Command

Chapter One: Introduction

Background

The future of warfare is changing as the cyberspace opens up new opportunities to challenge adversaries. The end of the Cold War saw the decline in threats originating from state-based threat actors, but within the last decade, the large-scale state actor has re-emerged as one of the most notable threat actors. A threat actor that will continue to grow in importance as society progresses into the future. Working collaboratively under a guise, nation-states provide a safe haven for hackers to comprise and disrupt official government and private sector partners networks in the search for valuable data. With the potential of plausible deniable for the nation-state and the hacker's lack of fear for legal reprisal, recently, the cyberspace has evolved into one of the most debated and important military trends.

The wide global reach of computer networks, the ability to highly tailor attacks, and the vast array of targets, has offered the cyberspace untold potential. Computer malware code has been executed on critical national infrastructure that had the ability to physically destroy nuclear centrifuges. Computers have been grouped together into a botnet that caused a distributed denial of service attack on an entire country's banking and e-government system. Moreover, adversaries have been able to operate inside restricted computer networks to secretly exfiltrate a huge amount of classified data. Industrial espionage, global mass surveillance, and state-sponsored clandestine operations are taking place on a scale never before seen. These are just some of the factors which have given rise to a new domain of warfare. A domain that faces difficulties in attributing the cyber-attack to an individual threat actor, where damage assessments cannot be fully realised until days after the attack is initially spotted, and in which geographical boundaries play no part in limiting the reach of adversaries. Since the turn of the millennia, in particular the last decade, the cyberspace has rapidly transformed the way conflicts are fought and disputes are resolved.

Statement of Problem

New and emergent technology presents a whole wrath of potential opportunities to provide benefits for citizens. The latest technological trends provide an opportunity that can either enhance or erode our society's cultural values. Cloud computing has transformed the provisioning of information technology infrastructure providing an opportunity for smaller organisations to leverage a larger company's networking power. As the number of devices increases due to the Internet of Things (IoT), organisations are moving their end points and security towards the edge of the network that if improperly cared for can increase security risks. The expansion of devices has risen sharply as more homes become smart and factories integrate more machine automation. The transformation in processes, practices, and procedures can be linked to industry 4.0, a new revolution powered through machine learning and artificial intelligence (Capdevielle, 2017). With the United States being one of the most technologically developed countries, it has become reliant on technology, and this has introduced a new vulnerability (McConnell, 2009; The World Bank, n.d.).

The cyberspace has offered numerous benefits for societies through increasing connectivity and productivity, these benefits are now being eroded as the risks associated with technology begin to escalate. Because of this escalated risk, a new threat has been creeping up the Pentagon's list of concerns with the cyberspace has been adopted by the military as both a target and a weapon (Berkowitz, 1995; Shimeall, 2001). Adversaries are rapidly intensifying actions to challenge the military dominance of the United States. The Chinese technology industry has hastily broadened and enlarged almost to be comparable to the United States (Brown, 2020). Meanwhile, Russia, Iran, North Korea, and Israel have all proven adept through military operations that challenge and overcome the cyber defences of other countries (Jones, 2021). NATO military leaders and senior policy makers first collectively

acknowledged the cyberspace at the 2002 Prague Summit both as a concern and an opportunity, they later adopted their first cyber defence policy in 2008 (Brent, 2019). Around 2010, approximate six countries had offensive cyber capabilities but five years later that number had climbed to thirty (Maurer & Hoffman, 2019). These are capabilities that enable a method for adversaries to match or supersede the military capabilities of the United States (Arquilla & Ronfeldt, 1993). Militaries have sought to obtain offensive cyber capabilities to integrate into their force operational structure as a force multiplier to compete against the United States, contributing to the redistribution of power boundaries amongst a new hierarchy (Arquilla & Ronfeldt, 1993; Shimeall, 2001).

Cyberspace is becoming an ever more important warfighting domain. Currently, loose collectives of hackers, terrorist organisations, and state-sponsored threat actors have all presented challenges to the United States (McMurdo, 2015). A new threat emerged from the state-sponsored cyber warfare teams called the Advanced Persistent Threat (APT) who continually exploit computer networks with the latest technology and the economic and legal support of a nation-state behind them (Hutchins, et al., 2011; Citizenfour, 2014). As the United States continues to expand its capabilities while concurrently shifting its strategic focus to an offensive stance, it presents a dilemma in the use of private-sector contracting support (Nakasone, 2019). Often contractors have operated within a grey area of international law, neither as a civilian nor military personnel (Adams, 1999). Recent decades have seen the shift of military outsourcing from the outsourcing of products to the outsourcing of services (Makinson, 2004). This progression of warfare amplified by the cyberspace has blurred the boundaries between civilian and military targets, by using contractors the military is effectively utilising civilians to wage warfare. The problem of outsourcing is further exemplified by the niche and wide range of technical knowledge required to conduct cyber operations thus contributing to an insufficiently trained and developed cyber force within the military (Nielsen, 2012). Private sector organisations are able to fulfil this void of human capital

by providing short term support, whilst this method is suitable in the short term, longer-term educational establishments will have to be devised to reduce the shortfall in talent and reduce risk (Nielsen, 2012).

Research Aim and Objectives

As the cyberspace transitions into a new domain of warfare, private industrial partnerships have been formed between the private sector, military officials, and policy makers. These partnerships cover a breadth of topics including offensive cyber capabilities. This research aims to analyse the effect that the private sector has on the United States' offensive cyber capabilities. In order to achieve the aim, three research objectives have been established; (a) explore and determine the factors contributing to the increased outsourcing of offensive cyber capabilities; (b) investigate and identify the offensive cyber capabilities being outsourced by the United States; (c) assess and evaluate the effects that outsourcing has on the ability of the United States to conduct offensive cyber operations.

Research Question

This dissertation will answer the research question of 'How does the private sector support the development of the United States offensive cyber capabilities?'

To answer this question three supporting questions will be researched; (1) What are the reasons why offensive cyber capabilities are being outsourced rather than matured in-house? (2) What are the offensive cyber capabilities being outsourced by the United States? (3) What effect does the outsourcing of offensive cyber capabilities have on the United States' ability to conduct offensive cyber operations?

The hypothesis of this research is that the private sector plays an important and crucial role in providing support to and developing new offensive cyber

capabilities for the United States to enhance their strategic capabilities. This is because outsourcing tasks allows for costs to be converted into a regular monthly payment, it provides access to new technology and people, and will follow the trend of the United States Department of Defense in tendering new contracts for services rather than products.

Purpose of the Research

The purpose of this qualitative case study is to research the outsourcing of offensive cyber capabilities by the United States throughout the history of the militarised cyber domain. To complete the research required for this dissertation, the combination of a literature review and a case study was found to be the most appropriate research methods. The literature review is necessary to research the militarisation of the cyber domain and the historical uses of contractors. Vitally, this chapter is used to explore and determine the factors contributing to the increased outsourcing of offensive cyber capabilities. The case study examines in detail the use of private-sector contractors within the cyber domain by the United States. The case study investigates and identified the offensive cyber capabilities being outsourced by the United States. The discussion chapter will assess and evaluate the aforementioned factors and the effect that outsourcing has had on the ability of the United States to conduct offensive cyber operations. When the literature review, case study, and discussion are combined they will be used to answer the research question of 'How does the private sector support the development of the United States' offensive cyber capabilities?'

Structure of Dissertation

This dissertation is split into five chapters, each with multiple subchapters. The first chapter provides the necessary contextual information and introductory text of the dissertation. Identifying the background of the topic, stating the problem that has evolved out of this and led to this research being conducted. The research aims, objectives, and the research question are then formulated. The

purpose of this research is clarified and the structural outline of the chapters is then provided before the necessary key terms are defined.

Secondly, the literature review chapter studies the pre-existing literature surrounding the topic of outsourcing to private sector partners by the United States, and the larger cyber domain, as well as, the use of cyber capabilities by the United States. The chapter is categorised into two sections, beginning by reviewing cyber as a strategic capability and then reviewing cyber as an outsourced commodity. The research objective of the chapter is to explore and determine the factors contributing to the increased outsourcing of offensive cyber capabilities.

The third chapter focuses on the design and methodology associated with this research. To begin, a rationale is explained for the reasons why a case study methodology was chosen, followed by the significance of the research and its limitations. Three hypotheses are devised based on trends seen elsewhere that will later be tested against the research finding.

Chapter four contains the findings of the case study on the United States Cyber Command covering multiple aspects of the organisation. The findings of this research are then compared against the initial hypothesis before conclusions are made. This chapter specifically investigates and identifies the offensive cyber capabilities being outsourced by the United States.

Chapter five first discusses the key themes found throughout the course of this research paper, afterwards, recommending four appropriate courses of action that can be taken to mitigate any potential future risk away from the United States. The discussion synthesises the previous two research objectives to assess and evaluate the effect that outsourcing has on the ability of the United States to conduct offensive cyber operations.

Finally, the last chapter concludes on all of the information identified and studies throughout the previous chapters whilst relating the information back to the aims and objectives of the research, as well as, the research question.

Definition of Key Terminology

Throughout this dissertation, a number of terms are employed primarily relating to the cyberspace, some of these words and their terminology are more obscure. Therefore, a definition has been provided to strengthen understanding and enhance the clarity of meaning.

***Cyberspace**:* The global domain and information operating environment consisting of interdependent networks, information technology infrastructure, and the data contained within including platforms, the Internet, telecommunications networks, computer systems, as well as, embedded processors and controllers, that span physical, virtual, and cognitive domains (Joint Chiefs of Staff, 2021, p. 55; U.K. Military of Defence, 2019, p. 11; NATO, n.d.).

***Cyberspace Capability**:* "A device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace" (Joint Chiefs of Staff, 2021, p. 55).

***Cyberspace Operations**:* The planning, synchronisation, and employment of actions and activities in or through cyberspace where the primary purpose is to preserve and enable freedom of manoeuvre and to achieve military objectives (Joint Chiefs of Staff, 2021, p. 55; U.K. Military of Defence, 2019, p. 11; NATO, n.d.).

Cyberspace Security: The application of security measures taken to protect cyberspace and prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as, the

information that is stored, processed, or transmitted in these systems with respect to ensuring its availability, integrity, authentication, confidentiality, and nonrepudiation (Joint Chiefs of Staff, 2021, p. 55; NATO, n.d.).

Defence Contractor: "Any individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the DoD to furnish services, supplies, or construction … The word can describe the private companies with which DOD contracts to provide goods and services. It can also describe individuals hired by DOD" (Congressional Research Service, 2021, p. 1).

Defensive Cyberspace Operations*:* Missions that utilize active and passive measures to preserve the ability to use cyberspace and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating ongoing or imminent malicious cyberspace activity (Joint Chiefs of Staff, 2021, p. 60; U.K. Military of Defence, 2019, p. 13).

Offensive Cyberspace Operations*:* Missions intended to project power to achieve military objectives in, and through cyberspace. (Joint Chiefs of Staff, 2021, p. 158; U.K. Military of Defence, 2019, p. 41).

Private Sector*:* "An umbrella term that may be applied to any or all of the non-public or commercial individuals and businesses, specified non-profit organizations, most of academia and other scholastic institutions, and selected nongovernmental organizations" (Joint Chiefs of Staff, 2021, p. 172).

Note: The term 'cyber warfare' is not defined by the United States Department of Defense or NATO who instead use the term 'cyberspace operations' to denote military actions taken within the cyberspace.

Chapter Two: Literature Review

Introduction

This literature review draws attention to two key aspects from which further research has been drawn; the cyberspace as a strategic capability and cyber as an outsourced commodity. From these two initial start points, three additional sub-topics were categorised and assessed on both points. Examining these two aspects is critical for this piece of research to achieve its objectives. The first topic, the cyberspace as a strategic capability, will provide a contextual understanding for the reader towards the cyber domain. The second topic, cyber as an outsourced commodity, will look at the evolution of contractors and private sector support. This chapter begins to answer the research objective of exploring and determining the factors contributing to the increased outsourcing of offensive cyber capabilities.

The Cyberspace as a Strategic Capability

To provide a contextual understanding of the cyber domain, this section reviews the literature on cyberspace as a strategic capability. Beginning by delineating between the perceived benefits of cyber warfare against conventional warfare tactics and doctrine, then facilitating the reader through the adoption of cyber as a strategic capability by state actors, afterwards, researching the strategic thought process applied within the cyber domain by military officials and policy makers.

The Delineation of Cyber Warfare

Alan Turing was one of the first individuals to develop an electronic computing machine (BBC, n.d.). This machine was devised at Bletchley Park during World War II and was capable of breaking the strong cryptography of the German Navy's Enigma Encryption (BBC, n.d.). After a series of advances in electronic computing after the end of the second world war, the U.S. Department of Defense' research organisation, Advanced Research Projects Agency (ARPA)

created a communication network which became the predecessor to the Internet called ARPANET in the late 1960s (DARPA, n.d.). The use of computers had humble beginnings primarily being used by academics, researchers, and businesses used for the computation and analysis of numbers (Computer History Museum, n.d.). But by the 1990s that changed fundamentally. In 1991, the World Wide Web was created by Sir Berners-Lee, this spurred the increase of home computing and increased the amount of time spent on home computers (Guimaraes & Ramanujam, 1986; Roser, et al., n.d.). As the number of individuals using an electronic computer began to rise, not just at their workplace, but also within their homes, the number of threats increased too (The Secret History of Hacking, 2001). By the turn of the 2nd millennia, society had entered the information age with electronic technology and the connectivity it provided rapidly becoming an integral part of daily life (Tabansky, 2011; Leiner, et al., 2009).

As academics debated the rise of computing and the connectivity it offered, three early academic papers on the topics noted the potential for this threat to become militarized. These researchers attempted to establish a name for this threat. The first of these papers defined two terms; 'net war' was defined as "information-related conflict at a grand level between nations or society" (Arquilla & Ronfeldt, 1993, p. 28); and 'cyber war' as "conducting, and preparing to conduct, military operations according to information-related principles" (Arquilla & Ronfeldt, 1993, p. 30). Nowadays, these two terms would be considered interrelated and synonymous with cyber war likely to be the more commonly used. The authors recognised that the potential of cyber warfare might not just be used to achieve the military objectives but also to alter the minds of individuals through disinformation campaigns. The second journal article defined 'information warfare' as "the actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information system and, in the process, achieving information

advantage in the application of force" (Rothrock, 1994, p. 218). Rothrock's definition was particularly influential as it includes a number of different methods to conduct operations with the ultimate objective of gaining an advantage through the application of force, implying that information warfare may be fought alongside traditional methods of warfare. The third paper was published by Berkowitz (1995, p. 59) who defined the term as 'information warfare' as "the use of information systems – computers, communication networks, databases – for military advantage, either by the United States or by a variety of unfriendly parties". The issue with this definition is that it specifically denotes the use of the military and negates the potential for civilian or non-military misuse.

Cyber warfare is fundamentally different to conventional kinetic warfare and there are multiple reasons for this. Cyber warfare removes the geographic limitations with difficult to define international boundaries (Lampson, 2001; Conti & Surdu, 2009; Maurer & Hoffman, 2019), it lower barriers of entry (Berkowitz, 1995; Maurer & Hoffman, 2019), anonymizes the adversary whilst making subsequent attribution activities difficult (Berkowitz, 1995; Hoffman, 2019; Conti & Surdu, 2009; Hayden, 2011), currently, states have inadequate response options for cyber-attacks below the threshold of armed response (Berkowitz, 1995), the number of exploits is diverse with attacks that can be highly tailored (Berkowitz, 1995; Hoffman, 2019; Butler, 2001), it provides a dual-use platform for civilians and military purposes (Maurer & Hoffman, 2019), as well as, providing a platform to organise and coordinate efforts to respond to the requirements of warfare (Rothrock, 1994). These factors have all accumulated into the new domain of warfare, the cyberspace, with most advanced militaries beginning to implement new armed forces branches or integrate new regiments in existing armed force branches.

The end objectives of cyber operations can easily be obfuscated. Usually, there are several options. Cyber can be used to disrupt the adversary by interrupting

their ability to make decisions, to generate intelligence by conducting espionage missions, and to inflict significant destruction on connected systems by degrading networks (Hoffman, 2019). As more state actors begin to devise new strategies for conducting cyber operations, a new dimension of war and peace has arisen. Cyber operations are often conducted below the threshold of armed response, as new methods of attack are generated, and operations are increasingly being directed by private actors, ultimately hindering the ability to accurately attribute attacks thus reducing the fear of reprisals (Hoffman, 2019). Clausewitzian thinking states the defender has the upper hand, that it is easier to defend than it is to acquire (Clausewitz, 1873). Cyber-attacks can be crafted through numerous methods by state-sponsored actors or even lone individuals. The defenders have a large number of avenues for a potential attack that must be defended against, whereas, attackers need only to exploit a single vulnerability (Conti & Surdu, 2009). In the case of cyber operations, it is those on the offensive that have the upper hand. Further cementing the importance of developing new cyber capabilities.

The Adoption of Cyber Capabilities

Militaries around the world have spearheaded and devised new technologies, embracing them with open arms to find a new way to challenge their adversaries thus gaining an advantage. Cyber is more than a new technology, it is a new domain of fighting. Within the domain of cyberspace, there are a multitude of tools, tactics, and procedures (TTPs), that can be utilised by the force structure to enhance their operational capabilities and impose challenges on their adversaries. Recognising the emerging potential of cyber operations, the United States Department of Defense (DoD) was one of the first to begin its expansion into the fifth domain with small cyber units first being created in the late 1990s (Warner, 2015). Meanwhile, other nations took longer to declare it as a domain of operations. The cyberspace only gained full recognition as a domain of operations by the North Atlantic Treaty Organisation (NATO) in 2016 after the Warsaw conference (NATO, 2016). Despite this, the Cooperative Cyber

Defence Centre of Excellence (CCDCOE) was established in Tallinn, Estonia by six member states in 2008, gaining NATO accreditation later in the same year (NATO, n.d.). The CCDCOE released a paper in 2013 entitled the *'Tallinn Manual'* that represented the first attempt to collectively define levels of attacks and appropriate use of force (Boeke & Broeders, 2018).

Harknett and Smeet (2020) noted that the behaviour of actors in the cyberspace has veered in a direction not predicted by the literature. Academics have spent time debating whether a cyber-attack can be equivalent to an armed attack or whether a large scale unexpected military attack could take place. The then U.S. Secretary of Defence even made mention of a scenario called 'Cyber Pearl Harbour' in response to growing threats in the cyberspace (BBC, 2012). Instead, methods of attack have been focused on small scale attacks below the response of armed response in order to achieve their strategic outcomes and conducted through persistent low-intensity attacks. Cyber campaigns are have rapidly adopted as they do not suffer as they expand beyond their geographical point. The 'loss-of-strength gradient' as defined by Kenneth Boulding (1962) results in the decrease of military force as expansion occurs. In the cyberspace, this rule does not apply, resulting in the actor having a wide range of targets to enact cyber operations (Harknett & Smeet, 2020). The types of tools used by cyber operators normally consist of software but can include hardware. Offensive weaponry includes malware and Distributed Denial of Service (DDOS) attacks whilst defensive technology includes firewall and disaster recovery tools (Tabansky, 2011). But Tabansky (2011) continues to highlight that most of the technology will be for dual-use purposes, that is for private corporations as well as public sector agencies, such as network monitoring, penetration testing, and encryption. However, having advanced weaponry and tools available for use will also require new doctrines, strategies, and planning in order to gain the full effectiveness of these (Arquilla & Ronfeldt, 1993).

The current commander of the United States Cyber Command, General Paul Nakasone (2019, p. 11), writes that the cyberspace provides countries with "the means to augment their power, degrade or usurp the powers of others, and gain a strategic advantage" without triggering an armed response. The United States enjoyed a military superiority in the cyberspace due to its advanced technology base and its large military-industrial complex, but recently adversaries have rapidly developed and acquired effective resources in niche areas that challenge the hegemony that the U.S. had previously enjoyed (Nakasone, 2019). The United States must take further action to prepare itself against attacks. Cyberspace offer exploits for militaries to target military infrastructure but also critical national infrastructure. Critical national infrastructure includes the financial sector, energy resources, and other important functions of society, however, often this infrastructure is run by the private sector. Therefore, as Rothrock (1994, p. 72) asks rhetorically, "does the military have an appropriate role in helping the society deal with such non-military requirements and implications? If so, what is that role". Nearly three decades after this question was asked, there is no clear-cut answer. Typically, the military does not play a role in the protection of critical national infrastructure, it is unclear whether the defence of critical infrastructure against a cyber-attack should be left to the military.

The Strategic Thought Process of Cyber

Introducing the fifth domain, the cyberspace, into warfighting caused a new strategic thought process to emerge within military leadership. The military and government bodies have been challenged on a new threat vector that changes the traditional dynamic and tactics deployed by military officers. Each country has used this new aspect of warfighting differently, each embracing the concepts and adding their own understanding and methodology for the integration of cyber into their procedures. This thought process has led many senior policymakers and military officials to integrate cyber warfighting capabilities into their existing force structure rather than devising a new operational branch

of the armed forces focused purely on cyber capabilities. As Hoffman (2019, p. 137) states cyber "cannot conquer territory or overthrow a rival". Instead, cyber has been utilised as a force multiplier and to provide operational enhancements for existing forces. As advanced militaries increasing rely on technological and networking capabilities to project their force, either having the ability to remove the adversaries use of networking capabilities or merely having superior capabilities will provide the advantage on the battlefield (Hoffman, 2019).

Some critics have stated that cyber isn't a new way of conducting warfare, but rather using traditional methods through new means. The tactics afforded through the means of the cyberspace is the natural progression and sophisticated version of classical military and intelligence capabilities such as subversion, espionage, sabotage, signals, cryptography, disinformation, and propaganda (Berkowitz, 1995; Harknett & Smeet, 2020). Rid (2011) even goes as far as suggesting that a cyber war has not occurred and will not occur, this is because cyber operations are unlikely to meet the three Clausewitzian criteria for war, violent, instrumental, and political. Within cyberspace, the lines between offence and defence become blurred. McMurdo (2015, p. 2) stated that "the best defense [sic] is a good offense [sic]". Cyber warfare requires a team to continuously search and seek for exploits in an adversary's network so that when the order is given to attack, the order can be executed swiftly. However, the tactics used between searching exploits and conducting offensive operations are closely intertwined (Stanford, 2014). In an article written by the former NSA director, Michael Hayden (2011, p. 3) notes that "the doctrinal, policy, and legal dilemmas" remain unresolved. The progression and adoption of cyberspace capabilities has increased faster than the military can effectively implement its new doctrine and much quicker than policymakers can debate the legality of searching for exploits or conducting offensive cyber operations. Hayden (2011) concludes on a rhetorical question in which the advantages of cyber operations is skewed towards the attackers so rather than focusing on how to defend against

a cyber-attack, it might be best to focus on how to recover from the inevitable attack.

Conti and Surdu (2009) argue that the existing cultures that have been nurtured through the three traditional branches of the armed forces, the Army, the Navy, and the Air Force are incompatible with the requirements of conducting cyber operations. Simply, the duo state that the "existing services operate in the kinetic arena, the directed application of physical force, whereas cyber warfare exists in the non-kinetic world of information flows, network protocols, and hardware, and software vulnerabilities" (Conti & Surdu, 2009, p. 15). Over 15 years earlier, Arquilla and Ronfeldt (1993) predicted that the organisation of the cyber forces would be as important as the technical abilities. Conti and Surdu (2009) emphasised a new branch of the military should be established as traditional soldier skills such as physical endurance and marksmanship were less important for cyber operations who require problem-solving skills, the ability to act under pressure, and critical thinking.

To combat the new threats, new methods of response are needed. Berkowitz (1995, p. 66) states that countermeasures "are likely to be political, economic, and cultural" and new concepts are needed as traditional military response measures will not work. This is because attacks will likely be below the threshold of armed response. Hayden (2011, pp. 3-4) also emphasised that "applying well-known concepts from physical space like deterrence, where attribution is assumed, to cyberspace where attribution is frequently the problem, is a recipe for failure". On the contrary, General Paul Nakasone (2019, p. 13), Commander of U.S. Cyber Command, emphasises that "cyberspace represents a new strategic environment through which relative power can be challenged without resorting to armed conflict". Whilst the first two authors based their attitude towards cyber from the defenders' point of view, General Nakasone based his on the view of the attacker, signalling a shifting in U.S. strategic policy and thought. Regardless of belief about the future of cyber

warfare, military forces around the world are a transformational moment in strategy attempting to shape the future of warfare. Bound by no established norms of operations, each actor races to develop novel methods of operations to challenge the previously established hegemony of the United States and its allies.

The Cyberspace as an Outsourced Commodity

As the cyberspace becomes an increasingly outsourced commodity by militaries, this section will begin to explore and determine the factors contributing to the increased outsourcing. Doing so by categorising the history of military outsourcing from mercenaries to contractors, then highlighting significant factors contributing to the private sector's expansion to the cyber domain, and examining ethical dilemma that arises from using private organisations in support of strategic national objectives.

The History of Military Outsourcing

Arguably one of the oldest aspects of warfare is the use of mercenaries, also commonly known as a soldier of fortune, history has documented the countless times that these warriors have fought for factions pledging their allegiance in return for income (Maurer, 2017). Since the inception of the Geneva convention that defined the laws of warfare, mercenaries were not recognised as lawful combatants and are not afforded the same protections as lawful combatants under the prisoner of war regulations (Adams, 1999). As state actors began to impose enhanced rules and enact new laws that effectively banned individuals from becoming mercenaries, the use of mercenaries has dwindled especially amongst the developed countries (Adams, 1999; Maurer, 2017). Instead, a fundamental change occurred that caused mercenaries to become known as contractors. The modern mercenary, or as they are known, private security and military contractor, has evolved out of the need for the governments to reduce their military spending budget but at the same time leveraging new technologies whilst increasing their agility to respond to a diverse range of threats. This

research paper will categorise the successive evolution of contractors into five sections; governmental, traditional, security, service, and consumer.

The ‘governmental’ contractor is either the government of another country or a public governmental department that bills another country or public governmental department for its services. Examples of governmental contractors include the Government of Canada, Japan, and Germany with funding for these contractors is primarily used for the upkeep of U.S. bases located within these countries (Makinson, 2004). As this type of contractor is considered a public body, it is out of the scope of this research to further investigate the governmental contractor.

The ‘traditional’ contractors are large international defence corporations the likes of Lockheed Martin, The Boeing Company, Raytheon Technologies, and General Dynamics Corporation. These corporations began to see a rise in the 1950s, defence budgets were decreasing and outsourcing was increasingly being normalised. These companies are often collectively known as the ‘military-industrial complex’ a term first recognised by President Eisenhower (Apgar & Keane, 2004). In his farewell speech to the nation, Eisenhower recommends applying caution against the defence industry or risking the potential of power to be misplaced (NPR, 2011).

The ‘security’ contractors are smaller yet the most notorious companies that often hire experienced individuals directly from the military, examples of these contractors are Academi formerly known as Blackwater, Executive Outcomes, Triple Canopy, and Aegis Defence Services. The 1990s gave rise to a new type of contract that primarily focused on security, protection, and escort services. These organisations won a diverse range of contracts from overthrowing governments, securing diamond mines that had been overrun with rebel factions, and protecting oil fields in the Gulf War (Adams, 1999). The saying ‘Guns-for-Hire’ became synonymous terminology with these groups. Their

notoriety peaked during the War on Terrorism in 2007 when some Blackwater employees escorting U.S. diplomatic staff engaged in the unlawful killing of Iraqi citizens in an event known as the Nisour Square Massacre (BBC News, 2008; Johnston & Broder, 2007).

The 'service' contractors consist of a vast array of organisations big and small that provide support services to militaries, this includes Booz Allen Hamilton, Leidos formerly known as Science Application International Corporation, Serco Inc, and The Mitre Corporation. These companies provide support services to the U.S. military from cleaning, catering, recruiting, and information technology capabilities. Far less infamous than the governmental or traditional contractor, these organisations often keep a quiet profile in the background, the 'tail', of the larger U.S. military presence, the 'tooth', but continue to play a vital role (Apgar & Keane, 2004).

The 'consumer' contractors are the next generation of contractors that is currently emerging within the United States. These are not defence specialists but rather multinational corporations that some examples are Microsoft Corporation, John Hopkins University, AT&T, and GlaxoSmithKline plc. The United States will require new technological services, research, healthcare support and services, or pharmaceuticals from the companies. With the application of civilian infrastructure and dual-use of technology, these contractors will be more difficult to regulate and potentially more dangerous (Adams, 1999).

The Expansion of Cyber Outsourcing

Technology is changing the battlefield. Modern militaries are constantly seeking to exploit new technologies to gain an advantage over their adversaries. And, cyber is no different. With the militaries adopting dual-use technologies leveraged from the private sector, the requirements are then tailored towards the Department of Defense. The private sector was ready to utilise their skills and

abilities to bid on the new contracts being tendered as cyber rapidly climbed up the Pentagon's list of priorities. One vital difference with cyber technologies in comparison to conventional weaponry is the larger list of potential customers. Aircraft, tank, and missile manufacturers are limited to a small number of potential customers, whereas, cloud computing capabilities, intrusion detection software, and software development support services have a much larger breath of customers across the public sector and private organisations. A journal article written two decades ago concludes with the statement that "information warfare, in fact, may well become dominated by mercenaries" (Adams, 1999, p. 110).

Between 1984 and 2003, the United States' Department of Defense has transformed its contracting budget from spending almost two-thirds on products to spending 56 percent on services (Makinson, 2004). The DoD works with a multitude of suppliers from large enterprises to small-medium enterprises and the average contract size was $1.1 million with 92% of the contracts were for less than $1 million (Apgar & Keane, 2004). One of the primary reasons that support the governments business case for outsourcing is that the use of contractors converts the initially large capital requirements costs into annual payments (Apgar & Keane, 2004). To meet the demand in cyber capabilities required by the DoD, large multinational firms are expanding through the acquisition of smaller companies that specialise in cyber tools and services to leverage their knowledge and working practices (Maurer & Hoffman, 2019). McMurdo (2015) suggests that smaller firms can specialise and innovate whilst providing employees with greater autonomy and less accountability. These smaller firms were unable to compete in the U.S. defence market where the top 50 biggest contractors obtained more than 50 percent of the procurement budget (Makinson, 2004). Organisations who have won over $100 million in contractors can be called defence primes, these prime defence contractors are responsible for 80% of the DoD's procurement budget with the top 10 collecting 38% (Makinson, 2004). This has caused a top-heavy structure that has increases the barriers for entry for smaller companies. Consequently, these prime

organisations have gained access to favourable contracts and closed-door bidding (Makinson, 2004). Many of these organisations will count ex-government employees within their staff as it is vital to understand the governmental way of working (Maurer & Hoffman, 2019; Hedahl, 2005). These factors can easily amount to the private sector company having greater access to technology and knowledge than the government agency.

Recent years has seen cyber security rise amongst importance in international security requirements (Information Telecommunication Union, 2018). With an estimated "85 percent of the nation's critical infrastructure is owned by the private sector", the government is unable to implement all the security requirements on its own (Healey, 2017, p. 120). A report by the DoD's Defense Science Board (2018, p. 1) opens with "the degree to which U.S. civilian and military infrastructure depend on cyber-enabled technologies, U.S. risks in the cyber domain present a serious and growing challenge to the Nation's ability to defend itself at home and advance its interests abroad". The inability of the government to exert its control over the use of computer systems has caused a rise in the misuse of computers and unauthorised access to data. Measures are being implemented across the United States in the private sector and within the government to address the potential risks associated with cyber technologies, especially within the critical national infrastructure sector.

The Ethical Dilemma of Outsourcing

The use mercenaries in combat have been reduced since the inception of the Geneva convention and as more countries enact new laws that prevent their citizens from fighting as a mercenary (Adams, 1999). The laws and regulations surrounding the use of mercenaries are clearly defined, however, the laws around the use of contractors remain vague or non-existent. Contractors operate within a grey area of international law in which they are able to operate with minimal restrictions, especially those contractors deployed overseas (McMurdo, 2015). Cyber firms often use remote access to conduct hacking operations

resulting in the contractors being far removed from the scene, this makes ascertaining jurisdiction on compliance, accountability, and monitoring over the cyber activities difficult (Maurer & Hoffman, 2019).

Private Military and Security Companies (PMSC) are a vital part of the military operations, some much so that the U.S. military would be unlikely able to mobilise its troops without them. Despite this, international law does not make distinctions for their role. “Contractors are not quite civilians, given that they often carry and use weapons, interrogate prisoners, load bombs, and fulfil other critical military roles. Yet they are not quite soldier, either” (Singer, 2005, p. 126). Contractors can fulfil a wide number of roles alongside the United States military, notable examples include protection and escort services, and interrogation services, but they also provide important support roles such as cleaning, cooking, and administration. In an early effort conducted by the Pentagon to manage the influx of contractors, they “even hired contractors to advise it on hiring contractors” (Makinson, 2004, p. 4). For military staff operating overseas, they are subject to the laws of their home country and military tribunals. However, contractors are not subject to these laws. Singer (2005, p. 127) writes that “contractors have a murky legal status, undefined by international law” as they do not meet the definition of military personnel, mercenary, or civilian.

Military contractors working alongside the United States have often taken the role of support and defence. Cyber introduces a new paradigm, contractors taking part in offensive operations. It seems unlikely that the United States would hire a contracting force to fight large-scale battles in kinetic warfare, however, offensive cyber operations are being outsourced to these organisations. “No cyber offense [sic] has ever caused the loss of human life. No cyber offense [sic] has ever injured a person. No cyber-attack has ever damaged a building” (Rid, 2011, p. 11). It becomes apparent that offensive cyber operations are considered by senior policymakers and officials as less

dangerous than offensive kinetic operations. The unique characteristics of the cyberspace "blur traditional distinctions critical to the foundation of governance of private actors, including between offensive and defensive capabilities, between legitimate commercial as well as law enforcement activities and illegitimate ones, abusive behaviour by governments, and even between peace and armed conflict" (Maurer & Hoffman, 2019, p. 10). These characteristics have given rise to the cyberspace as a new domain of operations, however, they present a new ethical dilemma that has heavily been debated by rarely acted on. Two critical aspects of military forces are the loyalty and the discipline of its personnel, but mercenaries "have no allegiance except to the highest bidder and the mighty dollar" (da Cruz & Pedron, 2020, p. 23).

Conclusion

The information age is powering the fourth industrial revolution. Individuals have become more connected and more accessible. As society reaps the benefits gained from innovative uses of technology that better our livelihood, a risk of cyber warfare emerges. Powered by the widespread and sheer scale of the attack vector, the anonymization of actors, and the removal of geographical limitations, modern militaries have begun to incorporate offensive and defensive cyber operations into their warfighting capabilities. Whether incorporated as a force multiplier or a strategically utilized weapon that reduces an adversary's capability, the use of cyber technology is currently being heavily invested in. The United States in particular is seeking to expand its cyber forces rapidly. But on the road to integrate new capabilities, it has faced struggles and sought assistance from the private sector. Facing challenges in the development, operation, and maintenance of rapid technological innovation, industrial partners are being used by the military to achieve their goals and objectives. As more cyber technologies are outsourced including offensive weaponry, the role of the contractor is transformed into neither civilian nor military personnel, operating in a legal grey area outside of established international rules and

regulations. Currently, the literature reviewed through this section notes that knowledge is lacking in regard to offensive cyber weaponry, instead, primarily focusing on the defensive. Furthermore, as more industrial partners are embedded in conducting offensive operations, an ethical dilemma arises towards the legality of their participation as a non-combatant and citizens under international law, this issue is further cemented with a lack of accountability regarding the actions of these individuals. The use of contractors and offensive weaponry in blurring the lines of operations that would have previously made clear distinctions between offence and defence and civilian and military. These aforementioned factors raise the question of how does the private sector support the development of the United States' offensive cyber capabilities.

Summary

Cyber is contributing to the evolution of warfare. With cyberspace now being considered a strategic capability by state governments, each are looking to expand their existing capabilities, turning the cyberspace into an outsourced commodity. Military operations conducted in the cyberspace are fundamentally different to conventional kinetic operations as it takes places in a virtual environment. Drawbacks such as geographical limitation, the expense of weaponry, and ease of attribution have now been removed. These advantages make for an alluring marketplace for smaller countries to challenge the military dominance of the United States. Despite this, NATO was slow in recognising the cyberspace as a domain of operation, only doing so in 2016. Meanwhile, governments, military, lone individuals, and collective groups have applied a new method of thinking to the cyberspace. Some consider cyber to be an advanced version of classical military capabilities whilst others see it as a domain of operation offering untold advantages. Cyber is being implemented in different ways, either integrating it into existing armed forces branches or establishing new branches. With the cyberspace, there may be compatibility

issues with integration as often existing procedures or doctrines can be seen as unsuitable for the domain.

To meet the growing demands placed on each armed force branch and rapidly develop new technology and procedures, the military is turning to the private sector. The cyberspace has become an outsourced commodity. Mercenaries have been around for centuries but many states began to implement laws that outright banned mercenary activities, this gave birth to a new status as a contractor. This research has categorised the five different types of contractors as governmental, traditional, security, service, and consumer. Each has had its impact on the international order, each with its own controversies. Warfare is changing and militaries are adapting. As cyber climbed up the Pentagon priority list, the private sector contractors were ready to assist. Utilising civilian infrastructure, critical national infrastructure is particularly at risk due to the government's inability to reduce risks like compliance, accountability, and monitoring. International law does not make a distinction between contractor and civilian meaning that contractors are not afforded the same rights as military personnel. It is an unlikely expectation that the military would outsource offensive kinetic operations, however, for offensive cyber operations they do. This gives rise to a new ethical dilemma that blurs the line between peace and war, civilian and contractor, and defence and offence.

The information age has powered the fourth industrial revolution. New technological innovation, enhanced connectivity, and automation are just some of the ways that society will change. This will bring new exploits for adversaries to attack and new ways for the U.S. dominance to be challenged. Contractors operate in a legal grey area outside of international law, more so, within the cyberspace, they are now conducting offensive operations. Resulting in a new ethical dilemma about the role of civilians in warfighting situations, this has also caused a blurring of lines between offence and defence and civilian and military.

These aforementioned factors raise the question of how does the private sector support the development of a state's offensive cyber capabilities.

Chapter Three: Research Design

Introduction

This chapter consists of information relating to the design of the research and methodological structure. This chapter begins by outlining the rationale for choosing this specific case and the methodology for analysing the data, afterwards, explaining the significance of the study and providing details on the limitations faced during the course of the research, as well as, discussing the data that led to the formulation of the three hypotheses. At last, the conclusion and summary of the chapter are provided at the end.

Rationale

In order to investigate and assess the research question, how does the private sector support the development of the United States' offensive cyber capabilities, a case study on the United States Cyber Command was chosen. By utilising a methodology design comprised of a qualitative approach towards the single case study, this dissertation was able to conduct a detailed investigation into the key events and actors thus revealing the relationships between them (Tellis, 1997). This research was solely centred around one of the newest branches of the United States armed forces, the U.S. Cyber Command, in particular focusing on the objective of describing and furthering understanding of the organisation's use of outsourcing aspects of operations and development to the private sector. The narrative case study utilized an exploratory and inductive structure to approach the interpretive topic with a wider depth of research allowing for the observation of the phenomenon's elements and relationships (Baxter & Jack, 2008; Levy, 2008). The perceived outcome of the case study was to understand the U.S. Cyber Command perspectives and experience with outsourcing through logically devising a sequence of events over time.

There are three reasons why the United States Cyber Command was chosen as the specific in-depth research case study for this dissertation. The first is that the establishment of the command represents the 21st-century shift in military capabilities to the fifth domain, the cyberspace. At the turn of the millennia, many nations began to become gradually more concerned with the threats originating from the adoption of technological capabilities and societies increasing reliance on digital technology. Near the end of the first decade of the 2000s, these threats were beginning to become sophisticated and sponsored by states thus accelerating the need for a proportionate military warfighting capability to defend and deter adversaries; the U.S. Cyber Command was the United States' answer to reducing this risk to national security.

Secondly, the United States has one of the most mature and segregated armed forces branches with an organisation whose specific focus is on cyber operations, U.S. Cyber Command. Only two other countries have a branch of the armed forces that is specifically responsible for cyber warfare; the Norwegian Cyber Defence Force *[Norwegian: Cyberforsvaret]* and Germany's Cyber and Information Domain Service *[German: Cyber- und Informationsraum]* (Forsvaret, n.d.; Bundeswehr, n.d.); whilst the United Kingdom is currently in the process of establishing the National Cyber Force (GCHQ, 2020). Many other armed forces across the world have the ability to conduct cyber warfare, however, often this is either integrated into one of their existing branches of the armed forces such as the Army, Navy, or Air Force and will often involve a regiment who authority has been expanded from signals intelligence or electronic warfare to include cyber warfare. Worldwide, there is a limited number of suitable alternatives that could be compared to U.S. Cyber Command, most of which are not anywhere near the same size and scale of the organisation and lack access to a similar amount of funding.

Finally, the United States has a public contract database where all federal contracts over a specific amount are listed. As U.S. Cyber Command falls under

the Department of Defense, a federal agency, all of the tendering contracts over a specific amount are made available on the federal procurement website. The segregation between the branches of the armed forces is crucial as it allows for budgets and contracts to be analysed easier as U.S. Cyber Command and its major projects will appear as a line item in the overall budget for the Department of Defense; without this segregation, the expenditure would be absorbed and obfuscated by another branch of the armed forces. After applying consideration to the three aforementioned factors, it was deemed more appropriate to analyse the effects of outsourcing within one specific armed force organisation rather than expanding the scope of the study to conduct a comparative case study.

Methodology

A single case study using a post-positivism theoretical perspective was chosen as the primary research method to facilitate a detailed, in-depth, and investigative mode of analysis focusing on a specific issue using multiple sources of information (Noor, 2008). Yin (2003) stated four indications for when the case study research method should be used; when the focus is on how and why; the inability to control or influence the behaviours of the subject; to provide relevant contextual factual information; and when the boundary between the phenomenon and context is obscure. Hence, a qualitative approach that seeks to describe rather than a quantitative approach was taken to explore the phenomenon of outsourcing within U.S. Cyber Command (Baxter & Jack, 2008; Meyer, 2001). The post-positivism perspective facilitated a subtle yet intricate socially constructed but subjective viewpoint towards the research question from the relevant literature and surrounding content (Mills, et al., 2010). The narrative case study on U.S. Cyber Command was enriched with literature concerning the background of events that led to the creation of the organisation, as well as, how and why the organisation uses outsourcing to further its capabilities (Dumez, 2015). The lack of clear and predictable outcomes at the initiation of the case study and the need to provide insights into

the issue indicates the exploratory and instrumental nature of this case study (Yin, 2003; Stake, 1995). The findings from studying this data would be subjective, therefore, the research followed a chronologically structured, multi-perspective analysis to conduct process tracing to identify the potential causal mechanisms that factored into the establishment of the hypotheses (Levy, 2008; Tellis, 1997).

A variety of sources were used to explore the outsourcing phenomenon from the perspective of the multiple actors involved such as the U.S. Cyber Command, the private organisations who won the government support contracts, the U.S. Government Accountability Office, and other third-party media agencies. The bulk of the data collected for this research was published between 2009 and 2020, this date range selected was as it begins in the year that the U.S. Cyber Command was established and ends at the commencement of this dissertation. To conduct this research, several primary sources were instrumental, notably the United States implementation of an e-government system that resulted in the wide publication and ease of access to official government documents vastly expedited the research process. This meant that budget requests, military doctrines, oversight advisory board reports, fact sheets, presentations, and contract tenders were all available online to the public. Another crucial primary source for information came from the press release published by the private organisation working alongside the USCYBERCOM that announced that contracts had been won to investors, often these provided further contextual clues surrounding the inner-workings of the organisation. To triangulate all of this data, additional supplementary information was gathered from secondary sources including peer-reviewed journals and third-party media reports on specific topics to fill any missing gaps in the government or business literature.

Using multiple types of data sources from both primary and secondary provided a well-rounded and contextual view into the United States Cyber Command. In order to manage this information with as much efficacy as possible, different

tools and techniques were used. Primarily, to assist in the aid of managing the flow of information, a data array table was developed in the spreadsheet software Microsoft Excel. By taking the key elements from the original data source such as date of publication, title, award amount, project name, year of the award, contract tendering organisation, and awarding organisation, it helped to store the data in a structured and chronological order for reporting purposes. Overall, this data array table facilitated the multiple-perspective analysis to ensure that consideration had been applied to the multitude of actors involved, the interaction between the actors, and the relationships of all those involved with the operation of U.S. Cyber Command.

The proposed methodological approach outlined in this dissertation is not subject to approval from the University of Glasgow's ethical review policy as the research does not involve human subjects.

Significance

This dissertation devises a method of qualitative research that analyses the phenomenon of outsourcing offensive cyber capabilities within a state's cyber warfare branch of the armed forces. Currently, there is a limited amount of literature focusing on the outsourcing of offensive cyber capabilities. Existing literature which is closely related fixates on several potential aspects such as general outsourcing in the military, the ethics of private military and security companies, or more recently, outsourcing of defensive cyber capabilities. This case study concentrates research efforts primarily on the offensive capabilities outsourced to the private sector from the U.S. Cyber Command. By being selective and probing this sole aspect of the USCYBERCOM will highlight how the private sector is aiding the military in providing defence to the United States.

The significance of this case study is that it elucidates a conscientious topic of outsourcing within the military through harnessing multiple sources of data to provide evidence on the private sector's ability to design, develop, implement,

operate, and support the military's cyber capabilities in aid of strategic national security endeavours. The expansion of technology has contributed to a rise in threats originating from a variety of threat actors within the cyberspace, new partnerships between hackers and nation-states have been formed, and adversaries have rapidly developed their capabilities. Increasingly the United States has turned to private-sector contractors to provide services rather than products including the participation in offensive cyber operations. Private military and security contractors operate in a grey area of international law neither as a civilian nor military personnel, what was once civilian infrastructure could now be seen as a military target. By examining the use of government outsourcing in an organisation like the military will provide insights into how private industry is encroaching its grasp on the traditionally public workforce thus influencing the country's high-level strategic decision-making abilities.

Limitations

One of the primary limitations of this case study was the lack of information accessible to the researcher through open-source research methods. The classified nature of the armed forces restricts the publications of detailed information, only information relating to private-sector partnerships that had been publicized through the federal business opportunities website, through the press release of the private sector companies announcing contract awards, and the U.S. Government Accountability Office were analysed. As U.S. Cyber Command is a public governmental organisation, unlike private-sector organisations, it is not accountable to shareholders, and therefore, is not required to produce publicly accessible annual reports on the operational performance of its endeavours and financial expenditure for these projects. Thus, unlike a business that has to publish its profit / loss statement, it is difficult to assess the true account of the benefits gained from the outcomes of a project conducted within the organisation. However, the U.S. Congress has an investigative oversight agency, the U.S. Government Accountability Office, that ensures that

public funds are being dispersed in a responsible manner that benefits the American people (United States House of Representatives, n.d.). USCYBERCOM is accountable to the American public and the DoD has to publish public annual budget requests that can be utilised to provide a high-level financial overview on the major ongoing projects. Additionally, freedom of information requests can be requested and once approved allows for previously classified information to be published in the public domain, often in a reduced and redacted format. These freedom of information requests were vital to gain an understanding of the inner workings of the classified organisation.

With this research taking a qualitative approach, the conclusions reached are open to subjectivity, to mitigate this, multiple perspectives had to be triangulated to assess the consistency of the data and validate the findings. The cyber security industry, similar to the technology industry, is a rapidly developing sector that is currently experiencing a period of huge growth and as a result, it often sees literature, as well as, the technological and procedural capabilities become quickly outdated. With U.S. Cyber Command being a newly established military command branch, the vast amount of non-technical information made publicly available was still suitable and beneficial for this research. Although this research briefly mentions USCYBERCOM partnerships with other federal agencies, it was deemed beyond the scope of this study to examine these relationships. Furthermore, whilst the U.S. Marine and Navy Cyber Commands form part of USCYBERCOM, limited information was readily available on the private-sector partnerships of these two commands; the largest of U.S. Cyber Command projects was initiated centrally or under the U.S. Army or Air Force Cyber Command.

Hypotheses

This case study will aim to identify any possible relationship between the following hypotheses

H1: United States Cyber Command and its Service Cyber Components are understaffed.

Cyber-attacks and cyber-based crimes are increasing rapidly, reaching all-time highs, this has resulted in the demand for cyber security professionals increasing faster than the supply (Perhach, 2018). A survey conducted on IT decision-makers found the vast majority, 82%, reported a shortage of cyber security skills, with the United States cyber security job market having over 40% shortfall in employees, that is 314,000 unfilled jobs out of a workforce of 716,000 (Crumpler & Lewis, 2019). This has led to one of the senior officials at the Department for Homeland Security describing the lack of cyber security talent as a risk to national security (Shieber, 2019). This phenomenon is not just unique to the United States of America, nearly every country is realising their potential risk to a future cyber-attack; the United Kingdom's Department for Digital, Culture, Media, & Sport (2020, p. 3) estimated that "approximately 653,000 businesses (48%) have a basic skills gap"; the European Union lacks specific data on the cyber security skills shortage across all member states, but estimates that the shortage of cyber security professionals had increased from 142,000 in 2018 to 291,000 in 2019 (European Union Agency for Cybersecurity, 2019). A further report commissioned by the cyber security company McAfee on the study of eight countries including the United States concludes that "the lack of trained personnel exacerbates the already difficult task of managing cybersecurity risks" (McAfee, 2016, p. 3). Therefore, it is probable that the United States Cyber Command will likely experience the same issues with recruiting cyber security professionals.

H2: United States Cyber Command lacks the technological capabilities to project force.

For a long time, the United States military dominance has rested on its technological superiority, however, as other nations and the commercial sector

advance their cyber capabilities, it erodes the traditional advantages of the United States (Congressional Research Service, 2020). A bipartisan governmental body called the Cyberspace Solarium Commission was created under the National Defense Authorization Act; their final report acknowledged the benefits that digital connectivity has enabled society with, but also states that neither the government nor the private sector is able to provide the level of data security, resilience, trustworthiness, or expertise required by the United States to manage its technological infrastructure and services (Cyberspace Solarium Commission, 2020). Adversaries with fewer resources have been devising new methods so that they can challenge the capabilities of the U.S., developing cyber capabilities represents that possibility as Congress and U.S. military officials have often seen cyber as an afterthought in comparison to conventional weaponry (Donnelly & Ratnam, 2019). Consequently, the rapid advancement of technology and the reluctance of the United States to adapt to new methods of fighting will likely result in the United States Cyber Command lacking the technological capability to project force.

H3: United States Cyber Command is increasing the number of projects being outsourced.

The United States has a history of partnering with private sector organisations to provide and supplement its resources with a significant portion of its budget, $131 billion, going towards research, development, acquisition of products, and procurement of services (Mahony, 2020). There are several reasons why an organisation outsourcing including reducing risk, gaining talent, adopting new technology, and minimizing overheads (Buck-Lew, 1992). The Iraq War of 2003 – 2011 brought additional notoriety to outsourcing through the use of Private Military and Security Companies (PMSC), this was due to the contractors from these organisations outnumbering the American soldiers they were deployed alongside, 200,000 vs 165,000 (Wechsler, 2019). The domain of cyberspace bypasses traditional limitations of warfare such as geographic

borders and national jurisdiction, as well as, decreases the barriers of entry whilst minimizes risks for adversaries (Tabansky, 2011). These factors have accumulated into the development of a domain that is a breeding ground for commercial entities to reshape the military landscape by leveraging their commercial-off-the-shelf products for dual-use purposes (U.S. Department of Homeland Security, 2019). Henceforth, the United States Cyber Command is highly likely to follow the trend of the U.S. Department of Defense by increasing the number of projects being outsourced.

Conclusion

The cyberspace is becoming increasingly militarised as organisational structures are implemented and the units obtain full operational capability. Threat actors are beginning to normal engaging in an offensive manner through non-kinetic means. The time has arisen for a thorough analysis to be orchestrated on the capabilities of these new operational forces. A qualitative research design consisting of a case study on the United States Cyber Command will address the use of private sector contracted support on the capabilities of this organisation. The case study will be limited to open-source data and undertaken through a qualitative method, ultimately opening the findings to subjectivity. Three hypotheses of expected results were devised prior to commencing the research and were based on the well-established trends being seen outside of the organisation. This research will be significant as it is expected to highlight the lack of technological power internally within the United States Department of Defence and their necessity to rely on third-party entities to achieve their strategic objectives.

Summary

This chapter has noted the research strategy undertaken to assess the dissertation's central aim of identifying how the private sector supports the development of the United States' offensive cyber capabilities. To do this, a qualitative approach was taken and a narrative case study was selected as the

research method to explore in-depth and identify the potential relationships between the instrumental events and actors that contributed to the organisation's reasons for outsourcing. The United States Cyber Command (USCYBERCOM) was chosen as the specific case study for three key reasons; first, is that the organisation represents the 21st-century warfighting shift that has occurred resulted in the creation of a new domain of battle; secondly, USCYBERCOM is a segregated branch of the armed forces of the United States, it is one of the few in the world with this structure; third, as the organisation is a federal agency of the United States, this means that all business contracts must be published on the federal business opportunities website. These three factors accumulate into making the United States Cyber Command the most suitable candidate for the case study.

The perceived outcome of conducting research was to test the hypotheses by devising a logical sequence of events over time based on the perspectives and experiences of USCYBERCOM. Utilising a case study as the research method facilitated the analysis of the phenomenon of outsourcing by enriching the research with background information, testing hypotheses, and understanding the multiple perspectives of the instrumental events and actors. To gain the information needed for this research, many different sources, both primary and second, were analysed to provide a well-rounded view. The majority of this data was captured from 2009 onwards through official U.S. government sources such as governmental websites, freedom of information requests, and official documents released in the public domain. To triangulate the information studied, additional information was gathered from the investor and press releases of the private organisations announcing their contract win, furthermore, media reports and peer-reviewed journals were studied to fill gaps in the information.

The significance of this research is that previously there has been limited other research into the effects of outsourcing of offensive cyber capabilities and will

provide insights into the numerous activities outsourced by the United States as they have limited capability to do so in-house. As a new and emergent threat facing the United States, other countries will likely face similar threats in the future. This research was hindered by the classified nature of the topic and of USCYBERCOM, this risk was mitigated by the cross-referencing information through multiple sources of data, authors, and varying perspectives to gain an understanding of the inner workings of the organisation. Overall, the research strategy took a qualitative approach which resulted in the findings being subjective and open to interpretation. Additionally, this research also deemed it out-of-scope to study the effects of partnerships between intergovernmental agencies and focused primarily on the private sector. Before researching the case study, three hypotheses were devised that could be tested throughout; (H1) United States Cyber Command and its Service Cyber Components are understaffed; (H2) United States Cyber Command lacks the technological capabilities to project force; (H3) United States Cyber Command is increasing the number of projects being outsourced.

Chapter Four: Findings

Introduction

This chapter will investigate and explore an interpretive case study conducted on the United States Cyber Command (USCYBERCOM) with the central objective of identifying the offensive cyber capabilities being outsourced by the United States. The case study begins by determining the events that led to the creation of USCYBERCOM and its roadmap to full operational capabilities followed by the organisation's partnerships with other federal agencies. To truly understand how a private-sector partnership works, a short section will outline the key information required to understand how defence contracts are tendered, before diving deep into the U.S. Cyber Command use of private third-party contractor support, with the penultimate section comparing the hypotheses against the findings of this case study. The chapter will then use this information to reach its conclusions before summarising the chapter.

Case Study: U.S. Cyber Command

Background

United States Cyber Command (USCYBERCOM) was established under the directive order given by the then Secretary of Defense, Robert Gates on 23rd June 2009 that U.S. Strategic Command (USSTRATCOM) should establish a subordinate unified for military cyberspace operations (Gates, 2009). The U.S. Cyber Command was to be "headquartered with the National Security Agency at Fort George G. Meade, Maryland" (U.S. Cyber Command, n.d., p. 1), furthermore, the commander was to be the Director of the National Security Agency, as well as, the Commander of the U.S. Cyber Command (U.S. Cyber Command, n.d.). The military command was designed to consists of operational intelligence and information technology capabilities to operate against global adversaries in the domain of cyberspace whilst reducing the overtly complicated procedures between the previous organisations (U.S. Cyber Command, n.d.; Warner, 2015). The work of U.S. Cyber Command is achieved through its

Service cyberspace components of; "Army Cyber Command (ARCYBER), Fleet Cyber Command (FLTCYBER), Air Force Cyber Command (AFCYBER), and Marines Corps Forces Cyberspace Command (MARFORCYBER)" (Rogers, 2015, p. 1). Figure 1 below provides an overview of the command structure of the United States Cyber Command.

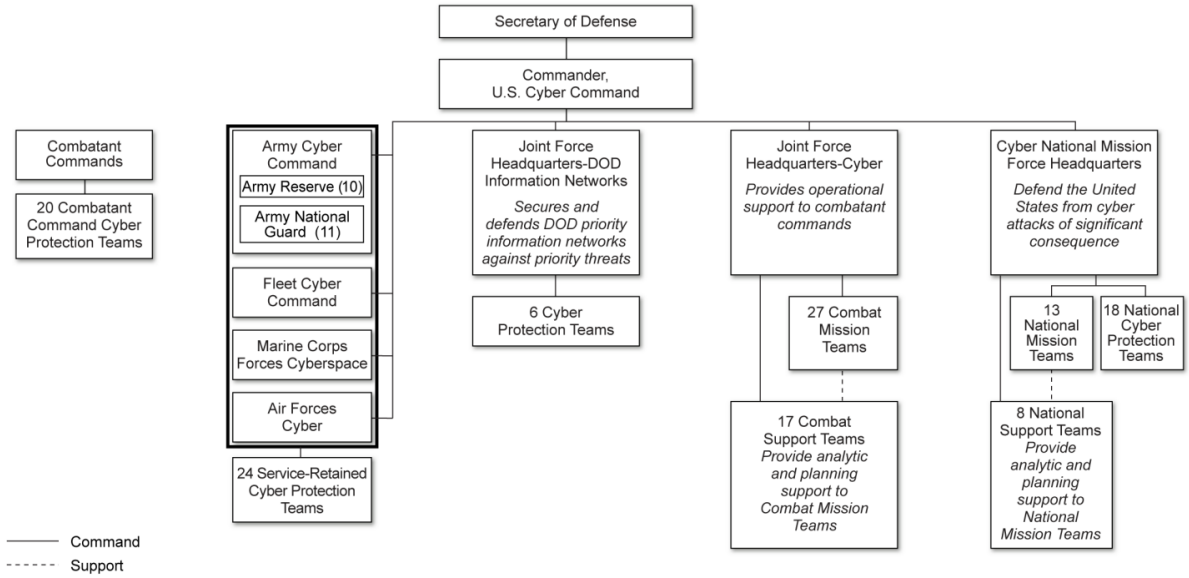

Figure 1: U.S. Cyber Command Organisational Structure as of June 2018 (U.S. Government Accountability Office, 2019)

The DoD was an avid adoption of technological solutions for the networking and command and control of its forces throughout the world; the mid-90s represented a shift in military thinking as senior DoD leaders publicly acknowledged the risk and vulnerabilities of its computer networks (U.S. Cyber Command, n.d.). A small organisation called the Joint Task Force – Computer Network Defense (JTF-CND) was chartered by the Secretary of Defense in 1998, the Joint Task Force (JTF) would report directly to him, but by 1999 the directing responsibilities were transferred to U.S. Space Command (SPACECOM) (Warner, 2015). SPACECOM took over the DoD's offensive network attack planning in 2000, subsequentially in 2001, the JTF-CND was renamed Joint Task Force – Computer Network Operations (JTF-CNO)

(Warner, 2015). SPACECOM was dissolved in 2002 and JTF-CNO was transferred over to USSTRATCOM, at this point the organisation was staffed by 122 personnel and managed a budget of $26 million (Warner, 2015). In 2004, a new organisation was established by USSTRATCOM and the Defense Information Systems Agency (DISA) called the Joint Task Force – Global Network Operations (JTF-GNO). Just a year later, JTF-CNO was dissolved and a new command was established between the National Security Agency (NSA) and USSTRATCOM called the Joint Functional Component Command for Network Warfare (JFCC-NW), they would then absorb JTF-CNO offensive responsibilities (Warner, 2015). By 2008, the current organisation of cyber forces was deemed inefficient and a review was arranged that accumulated in the merger of the offensive capabilities of JFCC-NW and the defensive capabilities of JTF-CNO (Warner, 2015). As the new President, Obama, took office in 2009, he was told that USTRATCOM had too many responsibilities and its responsibilities should be shared with other organisations; ultimately, this concluded with the creation of U.S. Cyber Command (Warner, 2015).

As the U.S. reliance on cyberspace increased, it added a new element of risk to national security, thus the Department of Defense required a command who had the required technical capability and the ability to synchronize the Pentagon's warfighting ability across the technological security environment (Gates, 2009). "The Joint Chiefs of Staff in their 2004 National Military Strategy declared cyberspace a 'domain' of conflict alongside the air, land, sea, and space domain" (U.S. Cyber Command, n.d., p. 1). The original mission of USCYBERCOM was to defend the Department of Defense Information Network (DoDIN), to "conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S. / Allied freedom of action in cyberspace and deny the same to adversaries" (Rogers, 2015, p. 1). The initial focus of USCYBERCOM was to design "the cyber force structure, training requirements and certification standards that will enable the Services to build the cyber force required to execute assigned missions" (Rogers, 2015). After the

directive to establish a military command for cyberspace operations was given, the JFCC-NW and JTF-GNO were reorganized into the U.S. Cyber Command in May 2010 (U.S. Cyber Command, n.d.). The unique structure of the command which sees it being staffed by the Service cyber components resulted in nearly every senior leader across the Department of Defense providing guidance and input during the roadmap for USCYBERCOM to attain its initial operational capability (Warner, 2015).

Full Operational Capabilities

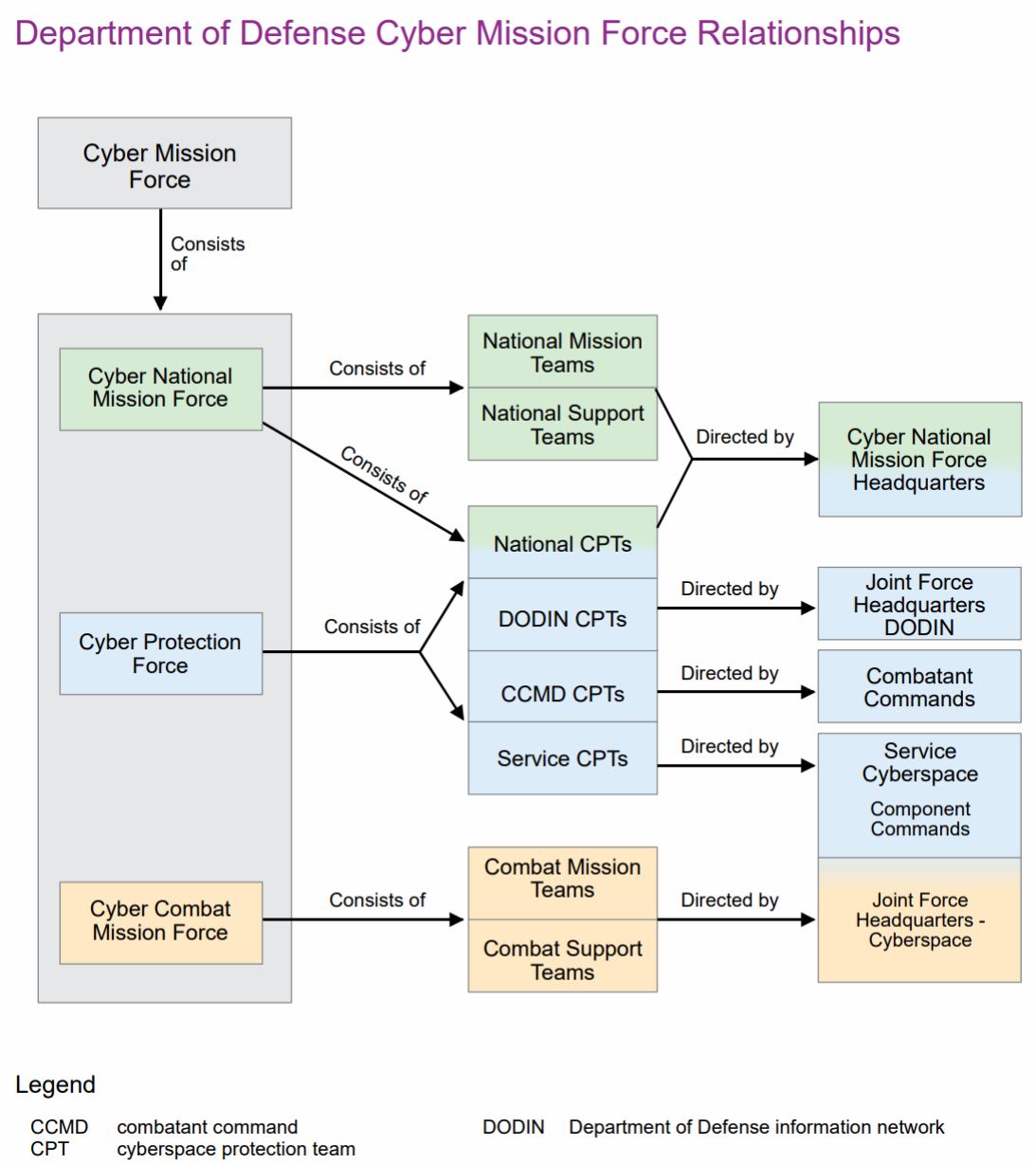

Figure 2: Department of Defense Cyber Mission Force Relationships (Joint Chiefs of Staff, 2018, pp. I-10)

After being established in late June 2009, the new command was instructed to reach its "initial operational capability by October 2009, with full operational capability following in October 2010" (Warner, 2015, p. 126). A number of

problems existed throughout USCYBERCOM progression to full operational capability, but the organisation received praise from the senior leaders for its situational awareness; consequentially this caused debates over whether the command was rushed to reach full operational capabilities and declared it too early (Warner, 2015). Increased authorization was given to USCYBERCOM in 2012 to establish a Cyber Mission Force (CMF) that would act as the operational arm of the command. The Cyber Mission Force consists of; the National Mission Force, who defend against adversary attacks; the Combat Mission Force who conduct military operations in support of the Service forces; and, the Cyber Protection Teams, who are responsible for the defence of the DoD Information Network (U.S. Cyber Command, n.d.). At the time of the Cyber Mission Force reaching full operational capabilities in 2018, the Cyber Mission Force was staffed by approximately 6,000 military and civilian personnel across 133 teams (U.S. Cyber Command, n.d.). Figure 2 above provides a high-level organisational chart of how the Cyber Mission Force is structured.

The President of the United States of America released a memorandum on August 15th 2017 which resulted in the "elevation of U.S. Cyber Command to a Unified Combatant Command" (Trump, 2017, p. 39953). As a result of the enduring threats faced within the domain of cyberspace, the strategic vision of the command had to be adapted to "persistent engagement with a persistent force" noting the ongoing and ever-evolving engagement with adversaries (U.S. Cyber Command, 2019, p. 3). The persistent engagement operational approach is aligned to the DoD Cyber Strategy's 'Defend Forward' concept that "extends [USCYBERCOM] reach to expose adversaries' weaknesses, learn their intentions and capabilities, and [conducts] counter attacks close to their origins. Continuous engagement imposes tactical friction and strategic costs on adversaries, compelling them to shift resources to defense [sic] and reduce attacks" (U.S. Cyber Command, n.d., pp. 2-3). Working with the geographical combatant commands to grow partnerships internationally, USCYBERCOM is attempting to discover adversary activity and then learn from the data collected

(U.S. Cyber Command, 2019). As the organisation has matured in its development and furthered its capabilities, the vision was changed to persistent engagement with "defensive teams [moved] forward to be able to operate in foreign networks; the purpose of that was to go where our adversaries are operating" (U.S. Cyber Command, 2019, p. 9). Ultimately, the geographical combatant commands are providing a really "good way for [USCYBERCOM] at low costs to gain a deep understanding of how our adversaries are operating, but also to just raise costs for them" (U.S. Cyber Command, 2019, p. 9).

During the Fiscal Year '20 of the President's budget request, USCYBERCOM requested a budget for $592 million, this was approximately 6% of the budget out of the overall $9.6 billion for DoD cyberspace activities (U.S. Cyber Command, 2019). The $9.6 billion requested for cyberspace operations is only a small fraction of the overall $705.4 billion requested by the DoD in Financial Year (FY) 2021 (U.S. Department of Defense, 2020). The DoD's "cyber-related budget is nearly 25 percent higher than the total going to all civilian [cyber] departments, including the departments of Homeland Security, Treasury, and Energy … ($9.6 billion compared to $7.8 billion)" (Healey, 2020, p. 2). Moreover, budget plans indicate the shift from defence to offence with the U.S. Air Force "spending 2.4 times as much on cyber offense [sic] research as on cyber defense [sic]" (Healey, 2020, p. 2). The Joint Cyber Warfighting Architecture (JCWA) was created by the DoD to better link its cyber operators together, the U.S. Air Force Cyber Command on behalf of USCYBERCOM released the programme 'Unified Platform' to connect the underlying information architecture to provides access for the tools required for the cyber operators, enabling command and control, data management, and a training environment all within an overarching secured system (U.S. Cyber Command, 2019). Figure 3 below graphically highlights the conceptual diagram of the Joint Cyber Warfighting Architecture and its integration of functions.

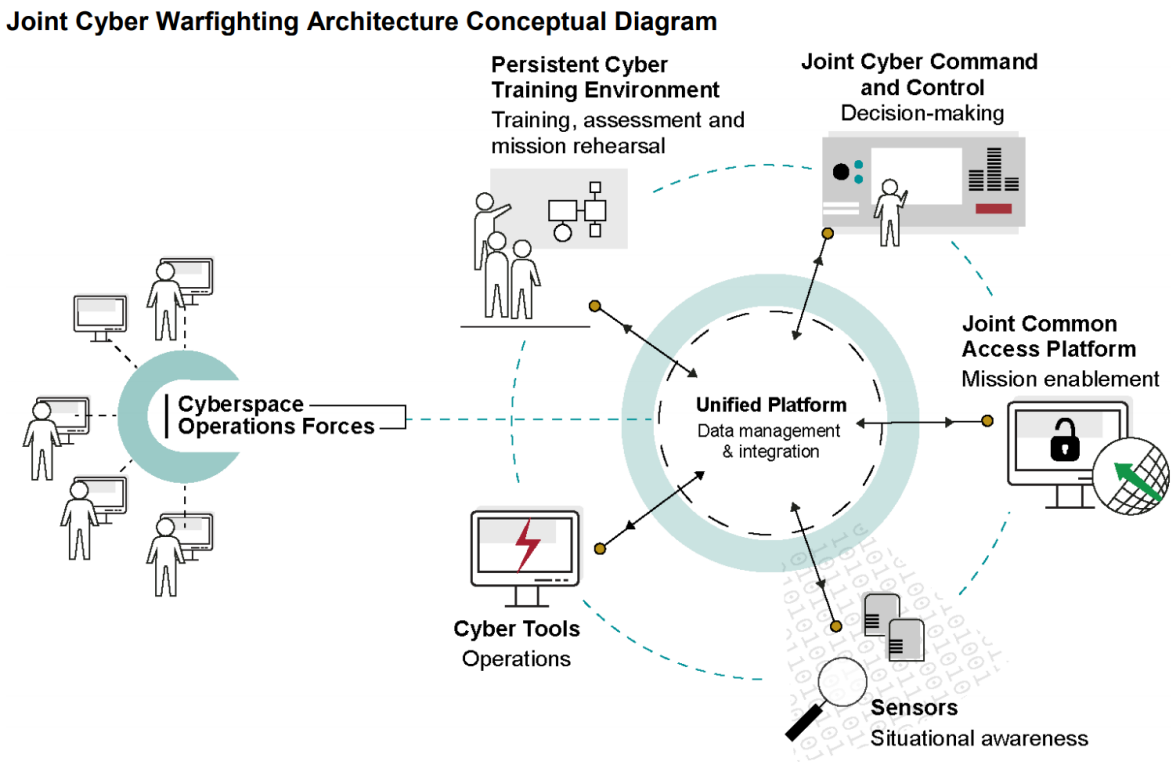

Figure 3: The Conceptual Diagram of the Joint Cyber Warfighting Architecture Programme (U.S. Government Accountability Office, 2020, p. 8)

Interagency Partnerships

The National Security Agency is one of the critical partners of U.S. Cyber Command by providing "world-class expertise, technical capabilities, and accesses that are crucial to United States Cyber Command's success" (U.S. Cyber Command, 2019, p. 5). Collaboration with the intelligence community within the United States and coalition partners is vital in gaining an asymmetric advantage in the complex and ever-changing domain (U.S. Cyber Command, 2019). Concerns have been raised over the ability to safeguard the tools, tactics, and procedures (TTP) used by U.S. Cyber Command from adversaries, however, one of the benefits of a partnership with the NSA, is that the best practices on securing data and tools can be shared (U.S. Cyber Command, 2019). In 2017, a memorandum of agreement was signed between the DoD and Department of Homeland Security (DHS) regarding establishing a stronger and

collaborative relationship between the two agencies due to the U.S. Coast Guard utilising the Department of Defense Information Network (DoDIN) despite being part of DHS (Department of Defense & Department of Homeland Security, 2017). In recent years, as adversaries have become more advanced and sophisticated in the method of attacks targeting critical national infrastructure, this caused a task force within USCYBERCOM to be established called the Cyber National Mission Force (CNMF) who partnered with the Department of Homeland Security (DHS) (U.S. Cyber Command, 2019). A further memorandum of agreement was signed in 2018 between the two agencies to counter malicious threats; one of the areas of critical national infrastructure was financial services, in this partnership DHS, the Treasury, and industrial leaders were responsible for the safeguarding of the network, while USCYBERCOM was tasked with identifying threats that are originating from outside the United States (U.S. Cyber Command, 2019). The Joint Force Headquarters (JFHQ) Department of Defense Information Network was created in cooperation with the Defense Information Systems Agency (DISA) as a task force who are responsible for managing the defence of the network on a day-to-day basis, with U.S. Cyber Command acting as a support if the Department of Defense is targeted (U.S. Cyber Command, 2019; Craft, 2019).

Tendering of Contracts

A process employed by the DoD is called Planning, Programming, Budgeting, and Execution (PPBE) which is a multi-year resource cycle that is designed to assist them in the obtainment of their strategic objectives (McGarry, 2020). "The process is designed to produce [the] DoD's portion of the President's annual budget request to Congress and [provide] updates to the department's five-year spending plan known as the Future Years Defense Programme, or FYDP" (McGarry, 2020, p. 1). The Department of Defense has multiple contracting options available to them: sole-source procurement, multiple contracts, normal procurement (Bame, 2019). Sole source procurements are often given to larger organisations with a history of government contracts;

multiple award contracts are given for the larger projects or programmes in which multiple companies will then obtain the privilege to bid on the individual task orders associated with that project or programme; finally, normal procurement has two options; the first is under $25,000 which uses a simplified and expedited acquisition route, the second is for contracts over $25,000, for these all contracts must be publicized on the Federal Business Opportunities website (Bame, 2019). The majority of information gathered for this research was through the standard procurement route of contracts above $25,000 and published on the Federal Business Opportunities websites.

There are also two standardised business processes worth noting; these are Request for Information (RFI) and Request for Proposals (RFP). An RFI is a process to collect information about suppliers, whereas, an RFP is a project announcement to solicit bids from the contracting organisation. A Production - Other Transaction Authority (P-OTA) is an additional method that can be used by the armed forces to engage industry and academia for research and prototypes, whilst not being subjected to federal laws and regulations (U.S. Air Force, n.d.). The expedited process was originally restricted to DoD weapons or weapons systems, however, this was later revised to projects that support the mission effectiveness of military personnel or the underlying platforms, systems, or components of the DoD (U.S. Air Force, n.d.). Another type of contract worth stating is the Indefinite Delivery / Indefinite Quantity mechanism; this allows for an indefinite number of services to be supplied for a fixed period and are usually used within services and architectural contractual obligations. Finally, some contracts have been issued by the U.S. General Service Administration (GSA), a federal support agency that leverages the buying power of the federal government to acquire the best value contract solutions and services for the American people (U.S. General Services Administration, n.d.).

Private-Sector Partnerships

The use of private contractors to provide services to the military has endured an increasing role within the United States since the end of the Cold War with the number of private contractors on hire by the matching or outnumbering the number of U.S. military personnel in its recent engagements (Petersohn, 2010). As defence budgets reduced the number of personnel and have demanded more operational efficiencies, private organisations offer a possibility for the military to gain new technology and reducing long-term costs by providing services solely for the time of the operation (Petersohn, 2010). Private Military and Security Contractors (PMSC) offer a degree of flexibility for armed forces, they provide a wealth of knowledge for specialist high-technological skills that would be unrealistic to maintain in-house and enables the military to leverage an element of investments and risk transfers onto the PMSC (Hesketh, 2018). Additionally, a PMSC has an important political affirmation by permitting politicians to supplement military personnel with contractors thus adhering to political promises of not increase the number of troops involved in conflicts (Singer, 2005). However, they are not without risks such as reduced accountability, loss of skills within the armed forces, rising dependence of the private sector, cause issues with integration, and the reduction in the loyalty of personnel for private firms towards the armed forces (Petersohn, 2010; Hesketh, 2018).

The United States Cyber Command is seeking further support for its connections to academia through an innovative collaboration method, a new partnership of approximately fifty universities has been devised to leverage the insights and knowledge of the universities to facilitate the prototyping of emerging concepts (U.S. Cyber Command, 2019). The largest of these partnerships was through their partnership with the Maryland Innovation and Security Institute, this partnership resulted in the creation of a public-private mission accelerator called DreamPort (U.S. Cyber Command, 2019). DreamPort has engaged small, medium, and large industrial partners and

participants in engaging new ideas and identifying potential talent, furthermore, it has supported the education of over 1,000 USCYBERCOM personnel whilst supporting approximately 350 students from high school and university (Pomerleau, 2020). This partnership has reduced the cumbersome barriers of entry imposed on DoD suppliers through developing competitions to identify non-traditional defence companies that support the mission objectives of U.S. Cyber Command (Pomerleau, 2020). One way that a private-sector product is leveraged by USCYBERCOM is through utilising the application VirusTotal, this software allows the organisation to share data on malicious activities with industry so that they can quickly be informed of potential malware threats providing them with time to establish countermeasures (U.S. Cyber Command, 2019).

One of the first large scale contracts submitted by the U.S. General Service Administration (GSA) on behalf of U.S. Cyber Command for suppliers to submit Request for Proposals (RFP) was a $475 million five-year contract that covered eighteen task areas such as knowledge management, training, cybersecurity, intelligence, software development, as well as, cyber operations (Sternstein, 2015). This RFP proved controversial as it had a line stating that the "contract shall assist in providing maneuver [sic], fires and effects through the application of capabilities in and through the cyber domain" (Sternstein, 2015, p. 2). This signalled that USCYBERCOM intentions were not just to seek to outsource professional services and defensive capabilities but also offensive capabilities. This was further cemented with a line in the proposal noting that "the contract will 'test innovative technology' for 'cyberspace offensive and defensive capabilities'" (Sternstein, 2015, p. 2). Approximately one month after publication, the RFP was cancelled with the U.S. GSA providing vague reasoning as to why, they stated that the "government has determined it is necessary to reassess the needs of USCYBERCOM and to consider whether another acquisition strategy could better meet those needs" (Biesecker, 2015, p. 1).

In the later part of the same year, 2015, a similar contract to the aforementioned appeared but this time as a Request for Information (RFI) and with a reduced budget of $460 million; the solicitation was for a variety of support services for the unification of existing cyberspace resources, supporting the centralization of command, helping to improve the DoD's existing capabilities, and enabling the armed services' ability to conduct operations (Pomerleau, 2015). Sternstein (2015, p. 1) noted that the work order contained information to advance the "cyber joint munitions effectiveness" through producing novel "cyber weapons" in cooperation with other entities, even going as far as arranging and conducting "joint cyber fires". Ultimately, the task orders were split and awarded to numerous private organisations including; Vencore, Booz Allen Hamilton, Science Applications International Corporation, CACI, and Secure Mission Solutions (Abott, 2016). Subsequently, after the awarding of the contract, Science Application International Corporation subcontracted a part of their task order to another organisation, NCI (NCI, 2016), with another portion of the contract being subcontracted to the company Fulcrum (Budik, 2016).

U.S. Cyber Command is not the sole organisation responsible for tendering contractors, with U.S. Cyber Command being staffed by personnel from the Service Cyber Components (SCC), additional contracts are also awarded through the individual Services. The United States Army Cyber Command (ARCYBER) awarded a cyberspace operational support task order to the company Perspecta worth $905 million, this included supporting ARCYBER headquarters, the Service components of USCYBERCOM, and other potential DoD cyber mission partners (Perspecta, 2019). In a contract as large as this, it is unlikely that a single organisation will have the full range of skills and knowledge available within their organisation. Three months after the award of this contract, FireEye, a cybersecurity company announced that it had been awarded a subcontract by Perspecta to provide incident and network response including intelligence methodologies and best practices for ARCYBER (FireEye, 2019). The U.S. Army Cyber Command operates five Regional Cyber

Centres (RCC), the management of these are outsourced to five separate contractors; "Continental U.S. – Directviz Solutions LLC ($50.3 million), Europe – Northrop Grumman Corp. ($24.4 million), Pacific – Lualima Government Solutions LLC ($16.5 million), Southwest Asia – Agile Defense Inc. ($4.5 million), Korea – RS3 Joint Ventures LLC ($6.5 million)" (Cornillie, 2020, p. 2). The geographical diverseness and the large number of contractors involved has caused ARCYBER to seek to consolidate and centralise the RCCs into a single contract to standardize operations due to rising complexities and issues with interoperability (Cornillie, 2020).

The U.S. Army Cyber Command in 2020 awarded a one-year $11.7 million contract to BAE Systems "to assist with the operation, maintenance, and technical aspects of the ARCYBER enterprise IT environment" (BAE Systems, 2020, p. 1). The year prior to awarding this contract, the U.S. GAO found in their report the Army was struggling to match the demands placed on it by the accelerated pace of establishment of multiple new cyber and electronic warfare (U.S. Government Accountability Office, 2019). The U.S. GAO (2019, p. 2) noted that "the Army activated a cyber battalion in December 2018, and as of March 2019, this unit was understaffed by more than 80 percent. Army guidance directs Army staff to conduct assessments on new units to determine whether the Army can staff, equip, and train these organisations". The report further comments that "the Army did not assess the staffing, equipping, and training risks" (U.S. Government Accountability Office, 2019, p. 2), and concludes that "if the Army does not assess risks for units activated at an accelerated pace, those units may be unable to effectively conduct multi-domain operations" (U.S. Government Accountability Office, 2019, p. 2).

One of the largest ongoing projects developed for USCYBERCOM by any of its SCCs is the 'Unified Platform' project, it was initiated by U.S. Air Force Cyber Command (AFCYBER) under the DoD's Joint Cyber Warfighting Architecture that seeks to "consolidate service-specific cyber capabilities and

data processing, storage, and sharing" (U.S. Government Accountability Office, 2020, p. 199). The Government Accountability Office (GAO) (2020, p. 200) found that the programme was initiated without key elements approved such as "approved requirements, a cost estimate informed by independent analysis, or a formal schedule risk assessment", and since the programme was initiated the cost has risen by 500% compared to its initial estimate (U.S. Government Accountability Office, 2020). The new amount required now stands at $588.98 million over a five-year acquisition period with $152.19 million already being spent on the programme (Coble, 2020). Nevertheless, two months after initiation, Northrop Grumman was awarded a $54.6 million contract to act as the system coordinator, and six months after that five additional companies were brought in to provide software development support at an undisclosed sum (U.S. Government Accountability Office, 2020; Northrop Grumman, 2019). Further to this contract, Northrop Grumman was awarded an additional $24 million contract to deliver cyber enterprise services on the Unified Platform programme (Northrop Grumman, 2019).

USCYBERCOM is also seeking to adopt commercial cloud services and conduct a migration of its capabilities to a third-party cloud provider, to do so they awarded Stratus Solutions, a partnership between Applied Insight and The Acadia Group (BusinessWire, 2019). The contract was allocated to deliver an accelerated migration of cloud services by utilising Stratus Solutions commercial platform-as-a-service product and knowledge for design, implementation, operational, and security and governance procedures (BusinessWire, 2019). In October 2020, the U.S. Air Force Cyber Command awarded a $93 million contract to BlackHorse Solutions for the integration and development of technological mission automation solutions in support of USCYBERCOM mission requirements (BlackHorse Solutions, 2020). To improve the efficiency of its operations, the AFCYBER outsourced Software Development Security Operations (DevSecOps) to Northrop Grumman to leverage their support in adopting Lean-Agile and DevSecOps methodologies

(Northrop Grumman, 2021). USCYBERCOM first exercised their capability to utilise the Production-Other Transaction Agreement (P-OTA), a method that allows the organisation to go outside of the traditional federal procurement contracts process, to award Recorded Future a $50 million contract to use their security intelligence platform for real-time threat analysis (Recorded Future, 2020).

Science Applications International Corporation was awarded a further contract worth $93 million for capability support in the coordination, planning, training of cyber forces and cyber operations (BusinessWire, 2017). Additionally, a further 5-year $165 million contract was provided to Booz Allen Hamilton to provide plans and policy, training and command administrative and staff support services to USCYBERCOM (Booz Allen Hamilton, 2018). U.S. Cyber Command marked a shift from building to maintaining a skilled workforce in 2018, the following year U.S. Government Accountability Office (2019, p. 2) noted that "many of the 133 CMG teams that initially reported achieving full operational capabilities no longer had the full complement of trained personnel and therefore did not meet USCYBERCOM's readiness standards". In June 2020, the ARCYBER on behalf of the joint Services released its contract entitled Cyber Training, Readiness, Integration, Delivery, and Enterprise Technology (TRIDENT), to assist with developing training in support of U.S. Cyber Command (Pomerleau, 2020). The contract worth up to $957 million is designed in support of the DoD's Defend Forward strategy with this contract including the creation of the Persistent Cyber Training Environment (PCTE), an online platform for personnel to be able to log in to training and rehearse missions (Pomerleau, 2020).

Hypothesis Testing

This case study has explored the phenomenon of outsourcing occurring within the United States Cyber Command. This section will test the original three

hypotheses that were based on trends in the cyber industry and within the larger defence sector.

H1: United States Cyber Command and its Service components are understaffed.

One of the primary narratives mentioned throughout the case study is the U.S. Cyber Command's rapid expansion since its inception. With the threat of cyber warfare looming and the perceived weakening of the U.S.' military superiority, the command and subsequently its Cyber Mission Force was quick to declare full operational capabilities. However, the U.S. Government Accountability Office identified flaws in the expansion recognized that the units were struggling to meet the threshold of full operational capability as previously suggested by the USCYBERCOM due to the units being understaffed. Furthermore, the research indicated that there are issues in the development and training of the personnel required as the organisation struggles to adapt to the high-technological skill requirement, which results in U.S. Cyber Command often turning to the private sector who already have this skillset. The previous changes to organisation structures that began in the late 90s are likely to have exacerbated this with the disjointedness of the organisations and their talent pool. At present, USCYBERCOM is implementing mitigation methods to overcome these risks although it is likely that these will take time to come to fruition.

H2: United States Cyber Command lacks the technological capabilities to project force.

Expanding the technological capabilities needed to project force differs from traditional defence projects due to the dual nature of the software being deployed. Third-party software is essential for the operation of U.S. Cyber Command and often relies upon the private sector to adapt their existing software to support the USCYBERCOM mission. To do so, often high-skill and

specialist knowledge is needed which is currently lacking within the command. Currently, the U.S. Cyber Command has an over-reliance on its interagency partnership with the National Security Agency and outsourcing task orders to industrial partners in order to provide supplementary support on its programmes. This hypothesis is interlinked with the first hypothesis in that by lacking the personnel to develop, implement, maintain, and operate, the command is lacking the technological capabilities to project force and is relying on the private sector to support its mission.

H3: United States Cyber Command is increasing the number of projects being outsourced.

The United States Cyber Command appears to be following the DoD trend of outsourcing projects and necessary services to fulfil its full strategy. The accumulation factors of *H1* and *H2* has resulted in the requirement for USCYBERCOM to outsource aspects where it lacks either the personnel or the technology to do so. After the command reached full operational capabilities and the Cyber Mission Force was established, USCYBERCOM sought to expand its capabilities and have increased the number of contracts being tendered. One of the primary contributory factors for the need to outsource is the previous reluctance to adapt to the changes in warfare from senior military officials and politicians who saw the capability of cyber as minute compared to traditional weaponry. This has caused the United States to fall behind its adversaries who realized the potential of cyber warfare to challenge the status quo of U.S. military and technological superiority in the new and emergent form of warfighting.

Conclusion

This case study on the U.S. Cyber Command's use of outsourcing has challenged the idea the United States military has technological dominance over its adversaries. The rapid implementation and expansion of the U.S.' cyber

military units have failed to match the pace of the growing need to develop two critical factors; the personnel of these units and their technological infrastructure and software. These two factors have accumulated into USCYBERCOM becoming understaffed and underequipped thus increasing their reliance on the private sector to fulfil their shortfall. The use of cyber in warfare has been seen as a secondary objective for U.S. senior military personnel and politicians in comparison to conventional weaponry. During this time, the United States has become one of the most technologically advanced and dependent countries, concurrently, its adversaries were presented with an opportunity to challenge the shortfall in the U.S.' military capabilities. As the United States Cyber Command continues to mature as a branch of the armed forces and addresses the shortcomings of the organisation, it will reduce its current over-reliance on the private sector. Steps are being taken to mitigate the risks associated with the issues occurring in staffing and its technological capabilities, however, these measures will take time to evolve and flourish. Crucially, as other military forces begin their expansion into cyber warfare, the threats associated with cyber will rise with the U.S. becoming of increasing risk, unless a paradigm shift occurs with its leaders recognising the need to increase budgets for cyberspace operations and the growing importance of cyber as a warfighting domain.

Summary

The Department of Defense (DoD) declared cyberspace a domain of conflict in 2004, that resulting in the United States Cyber Command officially being established in June 2009. USCYBERCOM followed a series of predecessor units in the late-90s and early-2000s and consists of intelligence and information technology capabilities, both offensive and defensive. The command reached full operational capability in October 2010 and by 2012 had established its operational arm, the Cyber Mission Force which by 2018 was comprised of 6,000 personnel. On August 15th 2017, the command was elevated to a Unified

Combatant Force, this allowed USCYBERCOM to shift its strategic vision from reactive and cautionary to increasing offensive persistently engaging with adversaries using a persistent force. During Fiscal Year ’20, USCYBERCOM had a budget of $592 million, this was 6% of the DoD’s $9.6 billion overall budget for cyberspace activity. Intergovernmental agency partnerships are vital to the success of the U.S. Cyber Command, which has major partnerships with the Department of Homeland Security and the National Security Agency and also provides support for federal agencies that support critical national infrastructure. The DoD stipulate that a multi-year resource cycle is implemented for a funding period over five years to incorporate the USCYBERCOM budget into the larger DoD budget request. Being a federal agency, all contracts tendered by United States Cyber Command or on their behalf must follow the laws and regulations enacted by the federal government.

The United States Cyber Command has sought to outsource projects to private sector firms to leverage their technical expertise and for the adoption of new technological capabilities to reduce long-term costs thus gaining a degree of flexibility. USCYBERCOM has developed partnerships with academia to leverage their knowledge and to target future personnel. A collaborative mission accelerator called DreamPort was devised with a research institute to engage with new suppliers and reduce the DoD’s barriers of entry. The first large scale programme to be outsourced was subsequently cancelled shortly after publication to provide time for the organisation to reassess its needs and acquisition strategy. Later in the year, the contract was tendered again for a slightly smaller amount and focused on the centralisation of the command, improving existing capabilities, and conducting operations including offensive. The Service Cyberspace Components of the command can also issue their own contracts, one such contract was the Army’s outsourcing of the operation of its Regional Cyber Centres. Concerns have been raised by the U.S. Government Accountability Office at the rate of expansion resulting in the organisation lacking the personnel required to staff the new units. Furthermore, the note that

contracts have been tendered for new technological capabilities without the necessary approval processes being completed stemming from a lack of oversight. The Unified Platform programme has increased in the budget by 500% since its inception due to a lack of requirement testing and third-party pricing analysis. Additional contracts have been awarded for several projects including gaining new technology, conducting cloud migrations, leveraging expertise, automating certain procedures, and implementing new methodologies.

This research has found that the three hypotheses tested have proven to be interlinked, as U.S. Cyber Command is lacking personnel with deep technological knowledge, they are struggling to independently develop new technological capabilities to project their force, thus, in turn, they seek assistance in the form of outsourcing to the private sector. Whilst mitigations methods are currently being implemented to address these concerns, it will take time to come to fruition, and in the meanwhile, increase the reliance of the U.S. Cyber Command on the private sector.

Chapter Five: Discussion and Recommendations

Introduction

This chapter assesses and evaluates the effect that outsourcing has had on the United States' ability to conduct offensive cyber operations. The purpose of this research was to answer the question of 'How does the private sector support the development of United States' offensive cyber capabilities?' The discussion revolves around three key themes; the insufficient ethical and legal frameworks, the blurred lines of operations, and the lack of oversight and accountability. Based on the discussion around these key themes, four supplementary recommendations are made; update international agreements and establish norms, implement additional measures of accountability, enhance cyber education offerings, and apply a shift in strategic thinking. The chapter concludes by recognising areas of future research and summarizes the key points.

Discussion of Findings

This dissertation has sought to provide answers on the effect that the private sector has on the United States' offensive cyber capabilities. The results of this research confirm that the United States, in particular, the United States Cyber Command relies upon the outsourcing of multiple aspects of their work orders to the private sector. These results are aligned with the initial hypothesis that the private sector plays an important and crucial role in providing support to and developing new offensive cyber capabilities for the United States to enhance their strategic capabilities. One of the primary reasons for the continued outsourcing of tasks is that it allows costs to be converted into a regular monthly payment, as well as, providing access to new technology and people. While the use of outsourcing does have benefits, it is not without its drawbacks and controversies. The following three subsections discusses these challenges, categorising them into three key themes. First discussed is the insufficient ethical and legal framework that materialises from the lack of laws and

regulations concerning actions taken by individuals within the cyberspace. Subsequently followed by the blurred lines of operations that formulates from defensive cyber operations that often require computer exploits to be used against an adversary. Moreover, there exists a lack of accountability and oversight over the private sector contractors, many of whom are now participating in offensive cyber actions. To mitigate these risks, a new pipeline of cyber education and training programmes must be devised and policymakers must start considering cyber as a primary domain of operations. Norms will be established in the cyberspace as it matures, but more should be done to increase oversight on private-sector contractors.

Key Theme: The Insufficient Ethical and Legal Frameworks

The ethical and legal frameworks that govern activities within the cyberspace have become outdated and are no longer sufficient for use. Rothrock (1994) was one of the first academics to identify that the use of information warfare could be coupled with conventional warfare to achieve an application of force both in the physical domain and in the cyberspace. Growth in military cyber operations has continued and since 2010 more countries are beginning their progression in the realm of offensive cyber capabilities. As more countries develop these skills and capabilities, the cyberspace risks devolving into a lawless domain. Cyber is more than a new technology, it is a new domain of warfighting. Many nation-states are creating new offensive cyber capabilities to supplement existing force structures and devising new tactics to challenge traditional military norms. The tactics can be utilised by the force structure to enhance their operational capabilities and impose challenges on their adversaries.

The ability to remove geographical limitations, the difficulty in define international boundaries, the lower barriers of entry, and the difficulty in attributions are all reasons that have led to the growth in cyber. Recently, a new threat has grown, the Advanced Persistent Threat (APT). APTs secretly operate concealed under the guise of the nation-state and private entity, a partnership

that greatly benefits both. The hackers do not face legal reprisal from the state and the state maintains plausible deniability for their actions. With the backing of a nation-state, the hackers are able to be fruitfully paid for their work and gain access to the best technology. Meanwhile, the nation-state is able to conduct operations and limit the possible response options for their actions. The cyberspace has difficult to define international boundaries and while countries are able to exercise control over the Internet Service Providers (ISPs), these restrictions can be circumvented. International norms governing the activities conducted in the cyberspace by individuals based in another country prove difficult to manage. Activities that take place over two legal jurisdictions require the extradition of the individual to be held accountable for their crimes. The lack of international boundaries means that cyber-attacks can take place over a wide range of targets without geographical hindrance. Further cemented by the potential of anonymizing attacks, attributing the attacks to a specific individual is extremely difficult and often relies on multiple intelligence gathering techniques to be synthesised.

Legal understanding and principles surrounding the use of mercenaries have been collectively agreed upon and understood by international partners for centuries. But recent years has seen the growth of private military and security contractors. These contractors operate in a grey area of international law, neither as a civilian or military personnel. Whilst the United States have utilised heavily the capabilities provided by contracting organisations, they are not held to the same standards as the soldiers they are deployed alongside overseas. The lawlessness of the cyber domain is magnified by the inability of nation-states to reach a collective agreement on the norms of operations. Defenders have to secure against a whole host of exploits but the attacks only need to find a single vulnerability; cyber-attacks are skewed towards the attacker (Conti & Surdu, 2009). The cyberspace has evolved differently from what was predicted by many academics and scholars who focused on the large-scale cyber-attack and war that would destroy critical systems and liken a ‘cyber pearl harbour’ (BBC,

2012). Instead, the types of attacks witnessed were more subtle using provocative disinformation campaigns. Without norms being established, the appropriate response options were limited. The *Tallinn Paper* was written by the NATO Cooperative Cyber Defence Centre of Excellence and was the first attempt to reach a norm on the appropriate level of response and the different levels of attacks (Boeke & Broeders, 2018).

Key Theme: The Blurred Lines of Operations

Military operations have quickly incorporated the cyberspace into a domain of operations and as a result, new tactics and doctrines have emerged. However, the cyber domain presents as much of a risk as an opportunity. Cyber can both be weaponised and act as a target. The expansion of cyber weaponry has now reduced the distinctions between civilian and military infrastructure. While increased hostilities in the cyberspace and large-scale cyber espionage has caused cyber to be one of the most contested international security requirements. Cyber operations have veered in a direction not predicted by the literature (Harknett & Smeet, 2020). Critical national infrastructure, often owned by the private sector, has been increasingly seen as a norm to target within the cyberspace. State actors, terrorist groups, lone individuals, and loosely associated groups, have all captured new features and exploited them for gains. Hoffman (2019) noted the ability to conduct attacks below the threshold of armed response, this has given birth to a new dimension between war and peace. Distributed Denial of Services (DDOS) attacks, web-page defacement, and disinformation campaigns have been utilised by all the actors. Whilst society begins its new era of cyber operations, the line between offensive and defensive measures becomes obfuscated.

The nature of cyber operations is fundamentally distinct from conventional military operations and in order to usher this new domain of operation into the military, new methods of strategic thinking need to be applied. However, some have argued that cyber warfare is merely the natural progression of existing

methods through new means (Berkowitz, 1995; Harknett & Smeet, 2020). While cyber operations share similarities with existing methods, having advanced weaponry and tools available for use will also require new doctrines, strategies, and planning in order to gain the full effectiveness of these (Arquilla & Ronfeldt, 1993). Offensive cyber capabilities aren't too dissimilar from defensive cyber capabilities. The U.S. Defense Science Board (2018) analysed the cyberspace as a strategic capability and found that defence is also a necessary foundation for an offence. In order for the soldiers to operate efficacy and efficiently within the cyber domain, the systems that they utilise for offensive cyber operations must be protect resilient against cyber-attacks. To defend a network from an adversary, it may be required to search for exploits on your adversaries' network, and to do this, it is necessary to enter their network. The steps to conducting this purely defensive operation would only be a small amount of work away from conducting offensive operations. This is vital to ensuring that when orders are given for an offensive operation, the important foundations have already been laid.

To combat future and emerging threats within the cyber domain, the United States Cyber Command was stood up. The U.S. Department of Defense has allocated a large budget towards cyberspace operations, a sum that is larger than the cyberspace budget for all other federal agencies (Healey, 2020). However, the budget is still insignificant in comparison to the overall budget allocated to the entire Department of Defense at less than 1.5% (U.S. Department of Defense, 2020). Cyber has grown rapidly as the barriers of entry for threat actors is much smaller than conventional weaponry. Growth has also occurred to the ability to conduct highly targeted attacks on specific systems without triggering an armed response, this presents significant new opportunities (Nakasone, 2019). The dual-purpose nature of cyber technologies is imperative in the expansion of offensive cyber capabilities. The wider range of potential customers for these new technologies has given the private sector the jolt required to increase the production and development of cyber weaponry. If

cyber operations are skewed in favour of the adversary, it would be sensible to prepare for the inevitable and focus on how to recover from any attack (Hayden, 2011). The United States Cyber Command was the U.S.' latest answer to meet the growing demands of conducting operations within the cyber domain. The previous structure of the organisations resulted in a disjointedness that causes friction between the previous establishments; a friction that grew out of the need to expand operations and saw the offensive units and defensive units being split between multiple organisations (Warner, 2015).

Key Theme: The Lack of Accountability and Oversight

The use of contractors has expanded significantly since the First Gulf War, since then, contractors deployed by the United States have, at times, been more than the number of troops deployed. Originally, contracting organisations were used to design, develop, and maintain products, but as time has progressed, more contractors are now providing services. Eisenhower's leaving presidential speech, he warned about the rising threat originating from the military-industrial defence complex, even suggesting that caution needs to be applied due to the potential for power to be displaced (NPR, 2011). At present, there have been limited measures of accountability and a lack of oversight imposed onto these contractors. Whilst deployed overseas, even less oversight is applied. The measures of accountability are normally ad-hoc and greatly vary in severity dependent on public opinion on the matter; there is a clear double standard in the application of the law between contractors and military personnel (Scahill, 2007). In contrast to contractors who are deployed alongside military personnel overseas, the cyber contractors are well removed from the fallout of cyber operations due to operations taking place remotely (Maurer & Hoffman, 2019). Therefore, ascertaining jurisdiction over the contractors for compliance and accountability is made harder. With organisations now being contracted to provide offensive cyber capabilities and required to participate in offensive cyber operations, the need for accountability and oversight is dramatically increased.

Two decades ago, Adams (1999) suggested that information warfare would become dominated by mercenaries. The cyber domain has further cemented the need for contractors as the technology utilised may require someone with a specific and niche set of skills or knowledge for a short period of time. The next generation of contractors, the so-called consumer companies, may likely become more difficult to regulate than other notable defence contractors. This is because of the dual nature of the technology and services that these consumer companies provide, whereas, traditional defence contractors usually have a smaller range of clients and are able to tailor their offerings to better meet the requirements of the restrictive environment in which they operate. The DoD works with a multitude of suppliers from large enterprises to small-medium enterprises. The average contract size was $1.1 million and 92% of the contract were for less than $1 million (Apgar & Keane, 2004). Organisations who have won over $100 million in contractors can be called defence primes, these prime defence contractors are responsible for 80% of the DoD's procurement budget, this has caused a top-heavy structure that has increases the barriers for entry for smaller companies. Consequently, these prime organisations have gained access to favourable contracts and closed-door bidding (Makinson, 2004). Critical national infrastructure in many countries, including the U.S. is owned by private entities rather than the state. This presents a lot of challenges as threat actors are beginning to target this civilian infrastructure throughout the cyberspace. The government doesn't have full control over the organisation and is unable to impose its rules and regulations on the use of information technologies. Additionally, the military's role in this sector is limited as civilian infrastructure is not traditionally the responsibility of the military to safeguard.

The case study highlighted the rapidly expanding force structure with an inadequate system of training and progression of future troops. The expansion of the troops was hindered by the rotational placements of soldiers who change their job roles every so often. The U.S. Government Accountability Office (2019) indicated that problems were specifically of note in the Army Cyber

Command who had 80% less of the necessary troop numbers. After the report was published, a new $1 billion contract was released by the Army Cyber Command for the private sector to design and deliver the next training programme (Pomerleau, 2020). The lack of cyber education follows similar trends noted in the private sector. Being able to offer higher rates of pay makes the private sector more lucrative for employees but they still experience a similar issue in recruiting.

Recommendations

Throughout the course of this research paper, several points have been identified concerning room for improvement within the United States current approach to utilising the private sector to support their offensive cyber capabilities. These recommendations have been based on the open-source research conducted and, if implemented, could mitigate potential problems from emerging. Four recommendations have been suggested; update international agreements and establish norms; implement additional instruments of accountability; enhance cyber education offerings; apply a shift in strategic thinking.

Update International Agreements and Establish Norms

There exist no norms of operations in the cyber domain and previously agreed international agreements are no longer suitable for the purpose. The novelty of the domain has seen many nation-states devise new methods to impose challenges on their counterparts. Internationally the use of cyber operations has risen and it is of utmost importance that collective agreements on the application of force are updated. New policies and procedures should be devised for establishing the norms within the cyberspace. These norms would limit the number of cyber-attacks taking place against civilian infrastructure. Although, this might take years, at the minimum a new collective ethical approach should be normalised

Implement Additional Instruments of Accountability

The existing measures and instruments used by the United States are insufficient for holding private sector contractors to account. These are often ad-hoc and vary greatly depending on the public's opinion on the matter. There exist minimal measures imposed on the contractors to ensure that those are held accountable for their actions. Furthermore, there is a lack of additional consequences for those contractors who do not follow regulations, this applies to the organisational level, as well as, the individual level. Recent conflicts have seen contractors outnumber soldiers, but contractors have been held to the same legal scrutiny. As private industrial partners contribute to an emerging offensive posture portrayed by the United States within the cyberspace domain, a new legal precedent needs to be established. It is necessary to apply new additional instruments of accountability and oversight throughout the lifecycle of the contract to ensure that the contractor fulfils its obligations in a legal manner. Embedding due diligence and civil repatriations into future contracts may reduce the contractor's desire to conduct acts beyond the reasonable expectations of the tendered contract.

Enhance Cyber Education Offerings

The present-day state of cyber education in the United States is insufficient to prevent threats. Neither the government nor the private sector is able to cope with existing threats and attacks against systems and data. The existing educational pipeline of employees is inadequate to meet the current demand for trained cyber security and information technology professionals. Rapid growth in the industry is expected, therefore, the educational pipeline is inadequate to meet the future demand level. Further investment is needed into the educational system within the United States focusing on reducing the shortfall of information technology and cyber security employees. By creating a new pipeline for cyber talent into the workforce, the United States can enhance the flow of human capital and mitigate the exacerbation of future potential security risks. Additionally, basic cyber education is vital for all employees in the

government using networked devices and all end-users should be required to undergo simple training to gain the privilege of using the devices.

Apply a Shift in Strategic Thinking

A shift in strategic thinking should be applied to the cyberspace. In recent times, the cyberspace domain has been often underfunded, and, as a result, underequipped to deal with existing and future threats. This is a result of cyber weaponry and defence being considered secondary to conventional military power. There are rising risks associated with the technological expansion of cyber capabilities of the United States' adversaries. Senior policymakers and military officials need to recognise the growing trends of offensive cyber operations. Instead of placing the cyberspace as a secondary function to support conventional operations, strategic thinking needs to be applied to the cyberspace as a primary domain of operations. This shift in strategic thinking will overcome some of the issues being seen with the still novel cyber doctrine and the expansion of cyber capabilities will begin to act as a deterrence to adversaries.

Areas of Future Research

The research for the case study was focused purely on the outsourcing of the United States offensive cyber capabilities to the private sector, one area of interest to future researchers may be to research the effect of outsourcing between United States federal agencies. The United States Cyber Command relies heavily on its partnership with the National Security Agency, particularly nearer to the inception of the agency, further exploration could be conducted analysing the flow of work and task orders between the two agencies as this was deemed out of the scope of this dissertation. Internally within the United States of America, more research should take place along a similar methodology to this research paper on other agencies approaches to outsourcing including the National Security Agency or the Department of Homeland Security. Additionally, as the research methodology of this paper was qualitative, the results gathered were subjective, therefore, another pathway for future research

would be to do similar research but with a quantitative statistical analysis approach. Moreover, in recent years, other countries have begun to develop offensive cyber capabilities and are using private sector support in order to achieve their objectives. Once research has been conducted on other countries, these investigations could be then compared and contrasted against the approach of the United States. The United States Cyber Command is a branch of the armed forces but has expanded its reach to identify foreign adversaries seeking exploits in critical national infrastructure. More research could be done to establish, if any, the role of the armed forces in the protection of critical national infrastructure.

Conclusion

The assessment of the United States Cyber Command approach has seen contractors fill the void of knowledge and the shortfall of talent needed within the organisation. The accumulation of these factors has led to the private sector being necessary to support the U.S. Cyber Command during its initial establishment phase and throughout as it progressed to full operational capability. Ultimately, this has had a profound effect on the ability of the United States to conduct offensive cyber operations. This research has been focused on reducing the gaps in the literature that normally focus on the defensive stance rather than offensive cyber weaponry. Without the ability to contract out specific task orders to private organisations, the United States Cyber Command would be severely limited in its ability. The contractors have provided support in training future cyber warriors, establishing procedures and best practices, and developing the software need to conduct operations. The continued and expanding use of the private sector in offensive cyber operations and the training of military personnel in the United States Cyber Command has presented an ethical dilemma towards the participation of these civilians in military operations. However, additional measures of accountability and oversights are necessary to ensure that the contracting agency fulfils its obligations and its

employees act in a legal manner. Contractors should continue to provide short-term support, but cyber education needs to be improved to combat future threats. A shift in strategic thinking should be applied to make cyber a primary domain of military operations and not considered secondary to conventional weaponry. The threat of cyber warfare will continue to grow as more countries expand and the United States needs to be ready to match its adversaries.

Summary

This dissertation sought to provide answers on the effect that the private sector has on the United States' offensive cyber capabilities. The results of this research confirm that the United States, in particular, the United States Cyber Command relies upon the outsourcing of multiple aspects of their work orders to the private sector. These results are aligned with the initial hypothesis that the private sector plays an important and crucial role in providing support to and developing new offensive cyber capabilities for the United States to enhance their strategic capabilities. One of the primary reasons for the continued outsourcing of tasks is that it allows costs to be converted into a regular monthly payment, as well as, providing access to new technology and people. While the use of outsourcing does have benefits, it is not without its drawbacks and controversies. The ethical and legal frameworks that govern activities within the cyberspace have become outdated and are no longer sufficient for use. Growth in offensive cyber capabilities is continuing with more countries seeking new technology, the cyberspace risks becoming a lawless domain. Military operations have quickly incorporated the cyberspace into a domain of operations and as a result, new tactics and doctrines have emerged. However, the cyber domain presents as much of a risk as an opportunity. The expansion of cyber weaponry has now reduced the distinctions between civilian and military infrastructure. There is a lack of accountability and oversight placed over the contractors and their employees. Contracts are becoming predominately services rather than products. Existing measures of oversight and accountability

are often ad-hoc and vary greatly dependent on public opinion. With contractors now participating in offensive cyber operations, it has become a necessity to increase regulation.

Based on the findings of the research, four recommendations have been placed forward; update international agreements and establish norms in the realm of cyberspace to limit cyber-attacks against civilian infrastructure; implement additional instruments of accountability for holding private sectors contractors to account throughout the lifecycle of the contractor; enhance cyber education offerings to reduce the threat of the insufficient number of cyber security and information technology professionals; apply a shift in strategic thinking to consider the cyber domain as a primary domain of operations and not secondary to conventional weaponry. Future research should be continued on the outsourcing of U.S. offensive cyber capabilities between federal agencies and on each agency. Additionally, work can be carried against other countries and contrasted with the results of this dissertation. The United States Cyber Command has been using contractors to fill the voids in its capabilities proving that private sector support is necessary for the operation of the command by providing support in training, establishing new procedures, and developing software.

Chapter Six: Conclusion

Conclusion

The cyberspace has changed warfare, new opportunities, new challenges, and new threat actors have surfaced. The threat arising from within the cyberspace will inevitability continue to grow in the near future and a new partnership between hackers and nation-states has formed in the search of exploits and the hunt for data. This research aimed to analyse the effect that the private sector has on the United States' offensive cyber capabilities. In order to achieve the aim, three research objectives were established; (a) explore and determine the factors contributing to the increased outsourcing of offensive cyber capabilities; (b) investigate and identify the offensive cyber capabilities being outsourced by the United States; (c) assess and evaluate the effects that outsourcing has on the ability of the United States to conduct offensive cyber operations. First literature surrounding two key themes, the cyberspace as a strategic capability and the cyberspace as an outsourced commodity, was reviewed to provide a contextual understanding of the broader topic. Following on, a qualitative case study on the United States' latest branch of the armed forces, the United States Cyber Command was conducted to study the organisation and how it has been utilising private sector in support of its strategic objectives. Afterwards, the discussion assessed and evaluated the impact that the private sector support has had on the ability of the United States to conduct offensive cyber operations.

This research paper has studied the research question of 'How does the private sector support the development of the United States offensive cyber capabilities?' The hypothesis of this research was that the private sector plays an important and crucial role in providing support to and developing new offensive cyber capabilities for the United States to enhance their strategic capabilities. After interpreting the results of the literature review, case study, and discussion, this paper concludes that this hypothesis was correct. The literature review studied the history of the cyber domain and the initial factors

that led to the requirement of outsourcing. The research objective of this chapter was to explore and determine the factors that contributed to the increased outsourcing of offensive cyber capabilities. The case study on the United States Cyber Command specifically investigated and identified the offensive cyber capabilities being outsourced by the United States. While the discussion assessed and evaluated the effects that outsourcing has on the ability of the United States to conduct offensive cyber operations. These research objectives were all identified as the necessary information required in order to provide a succinct answer to the research question.

To answer the research question, three supporting questions were suggested; (1) What are the reasons why offensive cyber capabilities are being outsourced rather than matured in-house? (2) What are the offensive cyber capabilities being outsourced by the United States? (3) What effect does the outsourcing of offensive cyber capabilities have on the United States' ability to conduct offensive cyber operations? Often the United States turns to outsourcing activities because they reduce long-term costs, provide access to new technology, people, and knowledge. By seeking contractors to bid on the task orders, the organisation offers an element of risk transfer for unexpected costs and delays, while providing flexibility in how and when new personnel are needed. Furthermore, the private sector enables politicians to affirm their promises of reducing troop numbers overseas but at the same time increasing the number of contractors overseas. The United States Cyber Command is seeking to expand its organisation to rapidly meet the rising cyber threats from adversaries. Meanwhile, they have been unable to expand their organisations to meet the requirements and have turned to the private sector for support in multiple areas such as software development, programme management, cloud migrations, best practices, and training. Ultimately, outsourcing products and services has had a positive effect on the ability to conduct offensive cyber operations, however, it is not without issues. Contractors fulfil a wide range of roles to support the deployment and operation of the military, it has been said

that the military would be unable to deploy without them. But contractors operate with a murky legal status, outside the boundaries of international rules and regulations and are normally subject to less legal accountability for their actions.

The research question is an important field of study as the cyberspace matures as a domain of operations. To meet the expanding desire of gaining offensive cyber capabilities, the U.S. has been partnering with multiple organisations to fulfil their needs. This research has specifically shown how the U.S. Cyber Command relies heavily on these industrial partners to meet the basic specification necessary to operate as a full unified command. This is indicative of a poorly funded, underequipped, and understaffed organisation that is incapable of solely defending its networks against adversaries. The outcomes reached in this paper are of the qualitative kind and are subjective to interpretation, but the methodology chosen to conduct this research was suitable for requirements. The approach taken has provided new insights into the United States' strategic development of new offensive cyber capabilities because of its ability to adequately expand its internal force due to a lack of expertise. This results in the organisation having to contract in the knowledge and technology from other organisations. Additional investigation and exploration should be given to this topic, particularly as other countries begin to integrate the cyberspace into their warfighting domain. Further research should be conducted to compare and contrasts the United States' use of contractors within the cyber domain, as well as, the nature of outsourcing within other U.S. federal organisations like the National Security Agency.

The number of threats is continuing to grow and each attack becomes more sophisticated. States are beginning to realise the potential opportunities within the cyberspace. This has accelerated the need for a new norm of military operations to emerge in order to defend and deter against attacks on civilian infrastructure. Employees of private sector companies are now conducting

offensive cyber operations at the behest of the U.S. military. At present, the United States has insufficient instruments of oversight to ensure that these organisations are held accountable for their action and the actions of their employees. Threats will continue to burgeon governments as more countries seek to gain powerful offensive cyber capabilities. The United States has been challenged by multiple adversaries through a diverse range of exploits and tactics, technological superiority has been relied on by leaders to dominant the battlefield, although, this superiority might not be as farfetched as some are led to believe. The United States Cyber Command is beginning to take steps to mitigate risks and address the shortcomings of their organisation with new training programmes are emanating through contracts with the private sector. The weakest link in a secure environment can be the end-user, more must be done nationally to address the insufficient cyber security knowledge across all stakeholders in the government. The private sector has massively supported the development of the United States offensive cyber capabilities and as the threat continues to accelerate in scale, the industrial partners will continue to provide a vital lifeline to meet the growing demands. Multiple reasons have contributed to the rise in private sector support services provided including the ability to covert capital costs into regular monthly payments, gain access to new technology and people, reduce long-term liabilities, and follows the trend of the United States Department of Defense in tendering new contracts for services rather than products. The outcomes found through this research have shown that the United States has relied heavily on the private sector to contribute a vital role, not only in the development of offensive cyber capabilities but also the overall cyber capabilities of the United States.

Bibliography

Abott, R., 2016. *Six Companies Win CYBERCOM Support Services Contract Worth Up To $460 Million.* [Online] Available at: https://www.defensedaily.com/six-companies-win-cybercom-support-services-contract-worth-up-to-460-million/business-financial/ [Accessed 18 Mar 2021].

Adams, T. K., 1999. The new mercenaries and the privatization of conflict. *The US Army War College Quarterly: Parameters,* 29(2), pp. 103-116.

Apgar, M. & Keane, J. M., 2004. New business with the new military. *Harvard Business Review,* 82(9), pp. 45-56.

Arquilla, J. & Ronfeldt, D., 1993. Cyberwar is coming!. *Comparative Strategy,* 12(2), pp. 141-165.

BAE Systems, 2020. *BAE Systems to deliver system integration and information technology management for Army Cyber Command.* [Online] Available at: https://www.baesystems.com/en/article/bae-systems-is-awarded-contract-with-the-us-army-cyber-command-to-provide-it-support-and-service [Accessed 19 Mar 2021].

Bame, M., 2019. *Overview Of the DoD Procurement Process.* [Online] Available at: https://www.thoughtco.com/overview-dod-procurement-process-1052245 [Accessed 16 Mar 2021].

Baxter, P. & Jack, S., 2008. Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report,* 13(3), pp. 544-559.

BBC News, 2008. *Blackwater incident: What happened.* [Online] Available at: http://news.bbc.co.uk/1/hi/7033332.stm [Accessed 06 Jun 2021].

BBC, 2012. *Leon Panetta warns of 'cyber Pearl Harbour'.* [Online] Available at: https://www.bbc.co.uk/news/av/technology-19923046 [Accessed 01 Jun 2021].

BBC, n.d.. *Alan Turing: Creator of modern computing.* [Online] Available at: https://www.bbc.co.uk/teach/alan-turing-creator-of-modern-computing/zhwp7nb
[Accessed 01 Jun 2021].

Berkowitz, B. D., 1995. Warfare in the Information Age. *Issues in Science and Technology,* 12(1), pp. 59-66.

Biesecker, C., 2015. *DoD Cancels RFP For $475 Million Cyber Command Support Contract.* [Online] Available at: https://www.defensedaily.com/dod-cancels-rfp-for-475-million-cyber-command-support-contract/cyber/
[Accessed 18 Mar 2021].

BlackHorse Solutions, 2020. *BlackHorse Solutions, Inc. Awarded $93M Contract to Deliver Mission Automation Solutions to U.S. Cyber Command.* [Online]
Available at: https://www.blackhorsesolutions.com/news/BlackHorse-Contract-Award-93M.html
[Accessed 19 Mar 2021].

Boeke, S. & Broeders, D., 2018. The demilitarisation of cyber conflict. *Survival,* 60(6), pp. 73-90.

Booz Allen Hamilton, 2018. *The General Services Administration Awards Booz Allen a 5 Year, $165M Contract to Support USCYBERCOM.* [Online] Available at: https://investors.boozallen.com/news-releases/news-release-details/general-services-administration-awards-booz-allen-5-year-165m
[Accessed 18 Mar 2021].

Boulding, K. E., 1962. *Conflict and Defense: A General Theory.* 1st ed. New York: Harper & Brothers.

Brent, L., 2019. *NATO's role in cyberspace.* [Online] Available at: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html
[Accessed 19 Jun 2021].

Brown, R., 2020. *Don't Underestimate The Rise In US-China Tech Tensions.* [Online]
Available at: https://www.forbes.com/sites/randybrown/2020/09/03/dont-underestimate-the-rise-in-us-china-tech-tensions/?sh=45249d053ebd
[Accessed 02 Jul 2021].

Buck-Lew, M., 1992. To Outsource or Not. *International Journal of Information Management,* 12(1), pp. 3-29.

Budik, L., 2016. *Fulcrum Wins Portion of USCYBERCOM Support Contract.* [Online]
Available at: https://washingtonexec.com/2016/07/fulcrum-wins-portion-uscybercom-support-contract/#.YFTBoq9KjZs
[Accessed 19 Mar 2021].

Bundeswehr, n.d.. *The Cyber and Information Domain Service.* [Online] Available at: https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service
[Accessed 12 Apr 2021].

BusinessWire, 2017. *SAIC Awarded $93 Million USCYBERCOM Task Order.* [Online]
Available at: https://www.businesswire.com/news/home/20171018005178/en/SAIC-Awarded-93-Million-USCYBERCOM-Task-Order
[Accessed 19 Mar 2021].

BusinessWire, 2019. *US Cyber Command Appoints Applied Insight Company Stratus Solutions to Deliver Secure, Scalable and Compliant Cloud Platform.* [Online]
Available at: https://www.businesswire.com/news/home/20190926005529/en/US-Cyber-Command-Appoints-Applied-Insight-Company-Stratus-Solutions-to-Deliver-Secure-Scalable-and-Compliant-Cloud-Platform
[Accessed 19 Mar 2021].

Butler, L. W., 2001. *Computer Security in the Real World.* Louisiana, Annual Computer Security Applications Conference.

Capdevielle, E., 2017. *Cyber-security – what are the risks from increased connectivity?.* [Online]
Available at: https://eiuperspectives.economist.com/technology-innovation/cyber-security-what-are-risks-increased-connectivity
[Accessed 21 Jun 2021].

Citizenfour. 2014. [Film] Directed by Laura Poitras. United States, Germany: HBO Films, Participant Media, Praxis Films.

Clausewitz, C. v., 1873. *On War.* 1st ed. London: N. Trübner & Co.

Coble, S., 2020. *Cost of US Cyber Command Program Quintuples.* [Online] Available at: https://www.infosecurity-magazine.com/news/cost-of-us-cyber-

command-program/
[Accessed 19 Mar 2021].

Computer History Museum, n.d.. *Timeline of Computer History.* [Online] Available at: https://www.computerhistory.org/timeline/computers/ [Accessed 04 Jun 2021].

Congressional Research Service, 2020. *Emerging Military Technologies: Background and Issues for Congress,* Washington, D.C.: Congressional Research Service.

Congressional Research Service, 2021. *Defense Primer: Department of Defense Contractors.* [Online] Available at: https://fas.org/sgp/crs/natsec/IF10600.pdf [Accessed 23 Jul 2021].

Conti, G. & Surdu, J., 2009. Army, Navy, Air Force, and Cyber - Is it Time for a Cyberwarfare Branch of Military. *IAnewsletter,* 12(1), pp. 14-18.

Cornillie, C., 2020. *Army to Merge $100 Million Regional Cyber Operations Contracts.* [Online] Available at: https://about.bgov.com/news/army-to-merge-100-million-regional-cyber-operations-contracts/
[Accessed 19 Mar 2021].

Craft, P., 2019. *JFHQ-DODIN - Fight The DODIN.* [Online] Available at: https://www.disa.mil/-/media/Files/DISA/News/Events/Symposium-2019/1---COL-Craft_Fight-the-DODIN_approved-Final.ashx
[Accessed 02 April 2021].

Crumpler, W. & Lewis, J. A., 2019. *The Cybersecurity Workforce Gap,* Washington, D.C.: Center for Strategic & International Studies.

Cyberspace Solarium Commission, 2020. *CSC Final Report,* Washington, D.C.: Cyberspace Solarium Commission.

da Cruz, J. d. A. & Pedron, S., 2020. Cyber Mercenaries: A New Threat To National Security. *International Social Science Review,* 96(2), pp. 1-35.

DARPA, n.d.. *Paving the Way to the Modern Internet.* [Online] Available at: https://www.darpa.mil/about-us/timeline/modern-internet [Accessed 01 Jun 2021].

Department of Defense & Department of Homeland Security, 2017. *Memorandum of Agreement between the Department of Defense and the Department of Homeland Security regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations.* [Online]
Available at: https://fas.org/sgp/othergov/dod/dod-dhs-cyber.pdf [Accessed 15 Mar 2021].

Donnelly, J. M. & Ratnam, G., 2019. *US is woefully unprepared for cyber-warfare.* [Online]
Available at: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/us-is-woefully-unprepared-for-cyber-warfare-52560026
[Accessed 18 Apr 2021].

Dumez, H., 2015. What Is a Case, and What Is a Case Study?. *Bulletin of Sociological Methodology,* 127(1), pp. 43-57.

European Union Agency for Cybersecurity, 2019. *Cybersecurity Skills Development in the EU,* Brussels: European Union Agency for Cybersecurity.

FireEye, 2019. *FireEye Joins Team to Provide Defensive and Cyber Threat Intelligence Operations Support to U.S. Army Cyber Command.* [Online]

Available at: https://investors.fireeye.com/index.php/news-releases/news-release-details/fireeye-joins-team-provide-defensive-and-cyber-threat
[Accessed 18 Mar 2021].

Forsvaret, n.d.. *Cyberforsvaret.* [Online]
Available at: https://www.forsvaret.no/om-forsvaret/organisasjon/cyberforsvaret
[Accessed 12 Apr 2021].

Gates, R., 2009. *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Cyberspace Operations,* Washington, DC: Department of Defence.

GCHQ, 2020. *National Cyber Force transforms country's cyber capabilities to protect the UK.* [Online]
Available at: https://www.gchq.gov.uk/news/national-cyber-force
[Accessed 02 Apr 2021].

Guimaraes, T. & Ramanujam, V., 1986. Personal computing trends and problems: An empirical study. *MIS Quarterly,* 10(2), pp. 179-187.

Harknett, R. J. & Smeet, M., 2020. Cyber campaigns and strategic outcomes. *Journal of Strategic Studies,* pp. 1-34.

Hayden, M. V., 2011. The Future of Things "Cyber". *Strategic Studies Quarterly,* 5(1), pp. 3-7.

Healey, J., 2017. Who's in Control: Balance in Cyber's Public-Private Sector Partnerships. *Georgetown Journal of International Affairs,* 18(3), pp. 120-130.

Healey, J., 2020. *The Cyber Budget Shows What the U.S. Values—And It Isn't Defense.* [Online]
Available at: https://www.lawfareblog.com/cyber-budget-shows-what-us-

values%E2%80%94and-it-isnt-defense
[Accessed 29 Mar 2021].

Hedahl, M. O., 2005. *Outsourcing the Profession: A look at military contractors and their impact on the profession of arms.* Springfield, Joint Services Conference on Professional Ethics.

Hesketh, J. J., 2018. *Contract or Command: An analysis of outsourcing in defence.* [Online]
Available at: https://ukdefencejournal.org.uk/contract-or-command-an-analysis-of-outsourcing-in-defence/
[Accessed 25 Apr 2021].

Hoffman, W., 2019. Is Cyber Strategy Possible?. *The Washington Quarterly,* 42(1), pp. 131-152.

Hutchins, E. M., Cloppert, M. J. & Amin, R. M., 2011. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,* Bethesda: Lockheed Martin.

Information Telecommunication Union, 2018. *Global Cybersecurity Index (GCI) 2018,* Geneva: ITU Publications.

Johnston, D. & Broder, J. M., 2007. *F.B.I. Says Guards Killed 14 Iraqis Without Case.* [Online]
Available at: https://www.nytimes.com/2007/11/14/world/middleeast/14blackwater.html
[Accessed 02 Jun 2021].

Joint Chiefs of Staff, 2018. *Cyberspace Operations,* Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2021. *DoD Dictionary of Military and Associated Terms,* Washington, D.C.: U.S. Department of Defense.

Jones, S. G., 2021. *The Future of Competition: U.S. Adversaries and the Growth of Irregular Warfare.* [Online] Available at: https://www.csis.org/analysis/future-competition-us-adversaries-and-growth-irregular-warfare
[Accessed 02 Jul 2021].

Lampson, B. W., 2001. Computer Security in the Real World. *Computer,* 37(6), pp. 37-46.

Leiner, B. et al., 2009. A brief history of the Internet. *ACM SIGCOMM Computer Communication Review,* 39(5), pp. 22-31.

Levy, J. S., 2008. Case Studies: Types, Designs, and Logics of Inference. *Conflict Management and Peace Science,* 25(1), pp. 1-18.

Mahony, W. C., 2020. United States defence contractors and the future of military operations. *Defense & Security Analysis,* 36(2), pp. 180-200.

Makinson, L., 2004. *Outsourcing the Pentagon,* Washington, D.C.: The Center for Public Integrity.

Maurer, T., 2017. *Cyber Mercenaries: State, Hackers, and Power.* 1st ed. Cambridge: Cambridge University Press.

Maurer, T. & Hoffman, W., 2019. *The Privatization of Security and the Market for Cyber Tools and Services,* Geneva: Geneva Centre for Security Sector Governance.

McAfee, 2016. *Hacking the Skills Shortage,* San Jose: McAfee.

McConnell, M., 2009. Cyberwar is the New Atomic Age. *New Perspectives Quarterly,* 26(3), pp. 72-77.

McGarry, B. W., 2020. *Defense Primer: Planning, Programming, Budgeting and Execution (PPBE) Process,* Washington, D.C.: Congressional Research Service.

McMurdo, J., 2015. *Cybersecurity Firms - Cyber Mercenaries.* [Online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2556412 [Accessed 04 May 2021].

Meyer, C. B., 2001. A Case in Case Study Methodology. *Field Methods,* 13(4), pp. 329-352.

Mills, A. J., Durepos, G. & Wiebe, E., 2010. *Encyclopedia of Case Study Research.* 1st ed. Thousand Oaks: Sage Publications, Inc..

Nakasone, P., 2019. A Cyber Force for Persistent Operations. *Joint Forces Quarterly,* 92(1), pp. 10-14.

NATO, 2016. *Warsaw Summit Communiqué.* [Online] Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm [Accessed 01 Jun 2021].

NATO, n.d.. *About Us.* [Online] Available at: https://ccdcoe.org/about-us/ [Accessed 03 Jun 2021].

NATO, n.d.. *NATOTerm.* [Online] Available at: https://nso.nato.int/natoterm/Web.mvc [Accessed 25 Apr 2021].

NCI, 2016. *NCI on Winning Team for Multiple-Award Contract with U.S. Cyber Command.* [Online]

Available at: https://www.nciinc.com/nci-winning-team-multiple-award-contract-u-s-cyber-command/
[Accessed 18 Mar 2021].

Nielsen, S. C., 2012. Pursuing Security in Cyberspace: Strategic and Organizational Challenges. *Foreign Policy Research Institute,* 56(3), pp. 336-356.

Noor, K., 2008. Case Study: A Strategic Research Methodology. *American Journal of Applied Sciences,* 5(11), pp. 1602-1604.

Northrop Grumman, 2019. *Northrop Grumman Awarded Cyber Enterprise Services Contract by US Air Force.* [Online] Available at: https://news.northropgrumman.com/news/releases/northrop-grumman-awarded-cyber-enterprise-services-contract-by-us-air-force
[Accessed 29 Mar 2021].

Northrop Grumman, 2019. *US Air Force Selects Northrop Grumman for USCYBERCOM Unified Platform.* [Online] Available at: https://news.northropgrumman.com/news/releases/us-air-force-selects-northrop-grumman-for-uscybercom-unified-platform
[Accessed 19 Mar 2021].

Northrop Grumman, 2021. *Northrop Grumman Contracted to Provide DevSecOps Capabilities for US Air Force.* [Online] Available at: https://news.northropgrumman.com/news/releases/northrop-grumman-contracted-to-provide-devsecops-capabilities-for-us-air-force
[Accessed 29 Mar 2021].

NPR, 2011. *Ike's Warning Of Military Expansion, 50 Years Later.* [Online] Available at: https://www.npr.org/2011/01/17/132942244/ikes-warning-of-military-expansion-50-years-later
[Accessed 04 Jun 2021].

Perhach, P., 2018. *The Mad Dash to Find a Cybersecurity Force.* [Online]
Available at: https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html
[Accessed 16 Apr 2021].

Perspecta, 2019. *Perspecta Wins New $905 Million Program to Provide Cyberspace Operations Support to the United States Army Cyber Command.* [Online]
Available at: https://investors.perspecta.com/News-and-Events/News/news-details/2019/Perspecta-Wins-New-905-Million-Program-to-Provide-Cyberspace-Operations-Support-to-the-United-States-Army-Cyber-Command/default.aspx
[Accessed 18 Mar 2021].

Petersohn, U., 2010. Privatising Security: The Limits of Military Outsourcing. *Center for Security Studies,* 80(1), pp. 1-3.

Pomerleau, M., 2015. *GSA issues $460M request for Cyber Command support.* [Online]
Available at: https://defensesystems.com/articles/2015/10/19/gsa-cyber-command-460m-support-contract.aspx
[Accessed 18 Mar 2021].

Pomerleau, M., 2020. *Army releases $1B cyber training request.* [Online]
Available at: https://www.fifthdomain.com/dod/cybercom/2020/06/12/army-releases-1b-cyber-training-request/
[Accessed 19 Mar 2021].

Pomerleau, M., 2020. *Cyber Command doubled its contract spending in the past year.* [Online]
Available at: https://www.fifthdomain.com/dod/cybercom/2020/03/09/cyber-

command-doubled-its-contract-spending-in-the-past-year/
[Accessed 29 Mar 2021].

Recorded Future, 2020. *New Contract With US Cyber Command Helps Protect Federal Agencies.* [Online] Available at: https://www.recordedfuture.com/protecting-federal-agencies/ [Accessed 19 Mar 2021].

Rid, T., 2011. Cyber War Will Not Take Place. *Journal of Strategic Studies,* 35(1), pp. 5-32.

Rogers, M. S., 2015. *CYBERCOM Fact Sheet.* [Online] Available at: https://www.stratcom.mil/Portals/8/Documents/CYBERCOM_Fact_Sheet.pdf [Accessed 15 Mar 2021].

Roser, M., Ritchie, H. & Ortiz-Ospina, E., n.d.. *Internet.* [Online] Available at: https://ourworldindata.org/internet [Accessed 01 Jun 2021].

Rothrock, J., 1994. Information Warfare: Time for Some Constructive Skepticism?. *American Intelligence Journal,* 15(1), pp. 71-76.

Scahill, J., 2007. *Outsourcing the War.* [Online] Available at: https://www.thenation.com/article/archive/outsourcing-war/ [Accessed 02 Jun 2021].

Shieber, J., 2019. *The lack of cybersecurity talent is 'a national security threat,' says DHS official.* [Online] Available at: https://techcrunch.com/2019/10/03/lack-cybersecurity-professionals-threat-dhs/
[Accessed 16 Apr 2021].

Shimeall, T., 2001. *Countering cyber war.* [Online]
Available at: https://www.nato.int/docu/review/articles/2001/12/01/countering-cyber-war/index.html
[Accessed 19 Jun 2021].

Singer, P. W., 2005. *Outsourcing War.* [Online]
Available at: https://www.foreignaffairs.com/articles/2005-03-01/outsourcing-war
[Accessed 25 Apr 2021].

Stake, R. E., 1995. *The Art of Case Study Research.* Thousand Oaks: Sage Publications.

Stanford, 2014. *Inside the NSA: An Evening with General Michael Hayden.* [Online]
Available at: https://youtu.be/_ESGBPmf0mc
[Accessed 04 Jun 2021].

Sternstein, A., 2015. *$460 Million CYBERCOM Contract Coming this Month; 'Cyber Joint Munitions' Help Wanted.* [Online]
Available at: https://www.nextgov.com/cybersecurity/2015/10/460-million-cybercom-contract-coming-month-cyber-joint-munitions-help-wanted/122526/
[Accessed 18 Mar 2021].

Sternstein, A., 2015. *CYBERCOM to Outsource $475 Million Worth of Offense and Defense Work.* [Online]
Available at: https://www.nextgov.com/cybersecurity/2015/05/cybercom-outsource-475-million-worth-offense-and-defense-work/111619/
[Accessed 18 Mar 2021].

Tabansky, L., 2011. Basic Concepts in Cyber Warfare. *Military and Strategic Affairs,* 3(1), pp. 75-92.

Tellis, W. M., 1997. Application of a Case Study Methodology. *The Qualitative Report,* 3(3), pp. 1-19.

The Secret History of Hacking. 2001. [Film] Directed by Ralph Lee. United States: 3BM Television & September Films.

The World Bank, n.d.. *Individuals using the Internet (% of population).* [Online] Available at: https://data.worldbank.org/indicator/IT.NET.USER.ZS?most_recent_value_desc=true
[Accessed 19 Jun 2021].

Trump, D. J., 2017. Elevation of U.S. Cyber Command to a Unified Combatant. *Federal Register,* 82(162), pp. 39953-39954.

U.K. Department for Digitial, Culture, Media & Sport, 2020. *Cyber security skills in the UK labour market 2020,* London: Department for Digitial, Culture, Media & Sport.

U.K. Military of Defence, 2019. *Joint Doctrine Publication 0-01.1 - UK Terminology Supplement to NATOTerm,* London: Ministry of Defence.

U.S. Air Force, n.d.. *Other Transaction Authority (OTA) Overview.* [Online] Available at: https://www.transform.af.mil/Portals/18/documents/OSA/OTA_Brief.pdf?ver=2015-09-15-073050-867
[Accessed 26 Mar 2021].

U.S. Cyber Command, 2019. *CYBERCOM Media Roundtable.* [Online] Available at: https://www.cybercom.mil/Portals/56/Documents/FOIA%20Reading%20Room%20Docs/2019-05-07_CYBERCOM_Media_Roundtable_Transcript.pdf?ver=2020-01-24-

095943-620
[Accessed 15 Mar 2021].

U.S. Cyber Command, n.d.. *U.S. Cyber Command History.* [Online] Available at: https://www.cybercom.mil/About/History/ [Accessed 15 Mar 2021].

U.S. Defense Science Board, 2018. *Task Force on Cyber as a Strategic Capability,* Washington, D.C.: U.S. Department and Defense.

U.S. Department of Defense, 2020. *DOD Releases Fiscal Year 2021 Budget Proposal.* [Online] Available at: https://www.defense.gov/Newsroom/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/ [Accessed 16 Mar 2021].

U.S. Department of Homeland Security, 2019. *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar,* Washington, D.C.: U.S. Department of Homeland Security.

U.S. General Services Administration, n.d.. *Mission (Who We Are & What We Do).* [Online] Available at: https://www.gsa.gov/about-us/careers-at-gsa/why-work-at-gsa/mission-who-we-are-what-we-do [Accessed 02 Apr 2021].

U.S. Government Accountability Office, 2019. *DoD Training: U.S. Cyber Command and Services Should Take Action to Maintain a Trained Cyber Force,* Washington, D.C.: United States Government Accountability Office.

U.S. Government Accountability Office, 2019. *Future Warfare: Army is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess*

the Staffing, Equipping, and Training of New Organisations, Washington D.C.: United States Government Accountability Office.

U.S. Government Accountability Office, 2020. *Defense Acquisitions Annual Assessment,* Washington D.C.: United States Government Accountability Office.

U.S. Government Accountability Office, 2020. *Defense Acquisitions: Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance,* Washington, D.C.: United States Government Accountability Office.

United States House of Representatives, n.d.. *Government Accountability Office.* [Online]
Available at: https://www.house.gov/the-house-explained/legislative-branch-partners/government-accountability-office#:~:text=The%20Government%20Accountability%20Office%20(GAO,benefit%20of%20the%20American%20people.
[Accessed 23 Mar 2021].

Warner, M., 2015. US Cyber Command's Road to Full Operational Capabilities. In: T. Seidule & J. E. Whitt, eds. *Stand Up and Fight: The Creation of US Security Organisations 1942-2005.* Carlisle, PA: Strategic Studies Institute, pp. 119-138.

Wechsler, O., 2019. Outsourcing in Intelligence and Defense Agencies: A Risk of an Increase in the Proliferation of Cyber Weapons?. *Cyber, Intelligence, and Security,* 3(1), pp. 95-116.

Yin, R., 2003. *Case Study Research: Design and Methods.* 3rd ed. Thousand Oaks: Sage Publications, Inc..