2020

Protecting the Protector: Mapping the Key Terrain that Supports the Continuous Monitoring Mission of a Cloud Cybersecurity Service Provider

Chris Bush

Protecting the Protector: Mapping the Key Terrain that Supports the Continuous Monitoring Mission of a Cloud Cybersecurity Service Provider

by

Chris Bush

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2020

We hereby certify that this dissertation, submitted by Chris Bush conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Gertrude W. Abramson, Ed.D.
Chairperson of Dissertation Committee

12/14/2020
Date

Steve R. Terrell, Ph.D.
Dissertation Committee Member

12/14/2020
Date

Kim Round, Ph.D.
Dissertation Committee Member

12/14/2020
Date

Approved:

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

12/14/2020
Date

College of Computing and Engineering
Nova Southeastern University

2020

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Protecting the Protector: Mapping the Key Terrain that Supports the Continuous Monitoring Mission of a Cloud Cybersecurity Service Provider

by

Chris Bush

December 2020

Key terrain is a concept that is relevant to warfare, military strategy, and tactics. A good general maps out terrain to identify key areas to protect in support of a mission (i.e., a bridge allowing for mobility of supplies and reinforcements). Effective ways to map terrain in Cyberspace (KT-C) has been an area of interest for researchers in Cybersecurity ever since the Department of Defense designated Cyberspace as a warfighting domain. The mapping of KT-C for a mission is accomplished by putting forth efforts to understand and document a mission's dependence on Cyberspace and cyber assets. A cloud Cybersecurity Service Provider (CSSP) continuously monitors the network infrastructure of an information system in the cloud ensuring its security posture is within acceptable risk. This research is focused on mapping the key terrain that supports the continuous monitoring mission of a cloud CSSP.

Traditional methods to map KT-C have been broad. Success has been difficult to achieve due to the unique nature of the Cyberspace domain when compared to traditional warfighting domains. This work focuses on a specific objective or mission within cyberspace. It is a contextual approach to identify and map key terrain in cyberspace. Mapping is accomplished through empirical surveys conducted on Cybersecurity professionals with various years of experience working in a cloud or CSSP environment. The background of the Cybersecurity professionals participating in the survey will include United States Government personnel/contractors, and other Cybersecurity practitioners in the private sector. This process provided an approach to identify and map key terrain in a contextual manner specific to the mission of a typical cloud CSSP. Practitioners can use it as a template for their specific cloud CSSP mission.

Acknowledgments

This journey has been a significant one. It has been a humbling experience. I have learned so much in regard to perseverance. I started this program with Nova Southeastern University (NSU) back in September of 2012 and I truly am thankful to the whole staff for their support and guidance.

I was blessed to have a patient and understanding dissertation chair in Dr. Gertrude Abramson Professor Emerita. She did a commendable job in keeping me focused and ensured that I made progress. Without her guidance and encouragement along with the committee members Dr. Kim Round and Dr. Steven Terrell, this dissertation would not have been possible.

To my brother and best friend Lashon, you have given me support and encouragement through this process. Do know I made the "shot" for the both of us. I love you brother.

To Annette, I am grateful for the support you have given me. I remember the long road trips from Virginia to Fort Lauderdale to meet NSU's on-campus requirements. When I was exhausted, you took the bulk of the time behind the wheel. Thank you for the support. I finally finished!

To my mother Deborah, you are the kindest dearest loving woman. You raised my Brother and me in New York City. Sometimes we had no place to call our own. Even when we did, there were times we did not have food to eat. I watched you persevere and overcome obstacles to raise three successful God-fearing members of society. Without you, I would not be here, and I thank you. What you could not provide in the material, you made up with abundance of love. No matter how the world treated me. What people said about me, or did to me, I knew I was loved, and I took that love with me out into the world. It helped me overcome. I now know that love is the love of Christ Jesus and it is a big part of me today. I try my best to infuse my kids with that same love because I know how powerful it is.

To my beloved children Nigel, Kalin, and Matthew. I love you very much. Everything I do is for you. I hope this accomplishment serves as inspiration and evidence that you can accomplish whatever you set your mind to. Matthew, although you are not biologically mine, I always treated you like you were because I know you are truly a blessing from God. Kalin, you are the sweetest daughter a father could have. Your beauty and heart are only matched by your high intellect. I am so amazed at how you grow and learn each day. Nigel, you are creative and mathematically gifted. I expect great things from you. I am so proud of you. Who is like you Nigel…? I could not ask God for a better son. The love you have given me so unconditionally has changed me forever.

Most importantly, thank you to my Lord and Savior Christ Jesus. Completing this dissertation means the end of a chapter. I am ready for what you have next in mind for me. I am thankful to all who have helped and encourage me throughout this chapter in my life.

Table of Contents

List of Table

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

The main objective of a Cybersecurity Service Provider (CSSP) is to protect an Information System (IS) along with its resources and assets. The mission of a CSSP includes the activities and services undergone to achieve its objective. A CSSP can offer a full spectrum of services to the IS it supports. These services may include the detection of malicious activity, response to incidents, and sustainment of the mission. The success of an IS's mission is directly dependent upon the success of the CSSP executing its mission. If the CSSP fails its mission, the IS fails and impacts the success of the overall mission it supports. The Department of Defense (DoD) Chief Information Officer (CIO) (2016), has mandated the use of a DoD CSSP by all its networks and systems.

The DoD CIO (2014) published a memo regarding updated guidance on the acquisition and use of commercial cloud computing services. The DoD CIO memo (2014) allowed DoD components to responsibly acquire cloud services in accordance with security requirements documented in the Federal Risk and Authorization Management Program (FedRAMP). DoD has required the monitoring of all cloud systems. Therefore, all cloud systems are required to establish a service level agreement (SLA) with a certified CSSP (DoD CIO, 2014).

As per DoD Instruction 8530.01 (2017), the measurement of the effectiveness of CSSP services is done by reviewing support agreements or contracts. Understanding the key terrain of a CSSP protecting a DoD IS is an additional way to foster confidence in CSSPs supporting DoD's mission. Applegate, Carpenter, and West, (2017) have defined key terrain as any locality, or area, the seizure or retention of will provide a marked advantage to either combatant.

Problem Statement

The problem is that effective ways are needed to map key terrain in Cyberspace (KT-C). Researchers have been fascinated with mapping key terrain in Cyberspace ever since the DoD designated Cyberspace as a new warfighting domain back in 1996 (Applegate, Carpenter, & West, 2017; Conti, Cross, Nowatkowski & Raymand, 2014; Bodeau, Graubart, & Heinbockel, 2013). In July of 2016, the North Atlantic Treaty Organization (NATO) joined the United States (US) and recognized Cyberspace as the fifth warfighting domain. As a result, a cyber-attack on a NATO ally is considered an act of war (Paganini, 2016). NATO's Deputy Secretary General Rose Gottemoeller believes the cyber ware fare challenges we face today must be grappled in quite a different way (2018). Traditional approaches are ineffective in cyberspace. Conti et al (2014) noted that cyber terrain differs from physical terrain in many fundamental ways. The challenges Cyberspace face are unique to the challenges of the traditional world. Gabel, Detlev, Libard, and Orzechowkis (2015) noted that technical innovation throws up new online dangers. Consequently, the domain of Cyberspace is constantly changing.

This problem is significant because research has not focused on mapping key terrain to specific objectives or missions within Cyberspace as identified in the work of Applegate et al, (2017). In almost every effort to identify key terrain in cyberspace, research has failed in the following areas:

- Research does not ascertain how to identify key terrain in a contextual manner, rather than focusing on what items should be key terrain.
- Research efforts omitted the planning concepts of objective and mission, which are essential to identifying key terrain for a military operation.

- Research efforts have often confused or misidentified key terrain with critical assets.

Conti et al (2014) emphasize that past research has defined KT-C as lists of assets like systems, devices, protocols, data, software, processes, cyber-personas or other network entities. As a result, lists like these leave the impression that everything is KT-C.

Dissertation Goals

The dissertation goal was to map the key terrain that supports the Continuous Monitoring (CM) mission of a cloud CSSP. Mapping of the key terrain was accomplished by assessing the responses of Cybersecurity professionals that have experience working within a cloud or CSSP environment. This work also ascertained how to identify key terrain in a contextual manner specific to the mission of a typical cloud CSSP. Practitioners should be able to use it as a template for their specific cloud CSSP mission. Moreover, researchers can build upon it in the context of a cloud CSSP or apply the methods to other areas within cyberspace. Cyber risk is now firmly at the top of the international agenda as high-profile breaches raise fears that hack attacks and other security failures could endanger the global economy (Gabel & Orzechowkis, 2015). CSSPs are vital to protecting the mission of diverse efforts in cyberspace.

This work sought to protect the mission of the protector. A CSSP's mission involves the CM of assets within cyberspace. Chawla et al. (2011) define CM as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. This is important to the mission of Cybersecurity as a whole. Researchers and practitioners in the area of Cybersecurity (civic and commercial), military, and the government should find this work of interest. With recent concerns over Russian hacking, the

United States Intelligence Community (IC) in a Joint Analysis Report (JAR) identified the mission of CISSPs as vital (Department of Homeland Security, 2016).

Research questions

Key terrain supporting a cloud CSSP's CM mission was investigated, guided by the following research questions:

1. What is the mission of a typical cloud CSSP?
2. What are the assets (personnel, systems, tools, devices, protocols, facilities, etc.) of a cloud CSSP?
3. What are the critical assets of a cloud CSSP?
4. How do the critical assets rank in respect to the CM mission of a cloud CSSP?
5. What is the terrain analysis of the assets supporting the CM mission of a cloud CSSP?

Relevance and Significance

Cyberspace is vastly different from the other four warfighting domains consisting of land, air, maritime, and space (Pantin, 2017). The missions and challenges to the Cyberspace warfighting domain are unique to the traditional world (Gabel, Detlev, Libard & Orzechowkis 2015). Methods that are based on the unique characteristics of Cyberspace provide effective approaches to map KT-C.

This work is relevant to the Cybersecurity community because it provides a new and effective way to map KT-C. This is a contextual approach that focuses on a specific objective or

mission within Cyberspace to identify and map key terrain. The specific objective of a CSSP's continuous monitoring mission is a context that is unique to the Cyberspace warfighting domain. This work encourages research to pull away from traditional key terrain analysis. Pantin noted that a framework or tool to assist in the identification of key terrain in Cyberspace would prove beneficial and is an area of study that not many have attempted (2017). The findings of this work can be used to identify new and existing security controls/measurements that can be used/implemented to improve and protect the security posture of a CSSP.

Barriers and Issues

The first barrier was getting approval from government agencies concerning this study. Access to the personnel conducting the day to day continuous monitoring is critical. There were two approaches used to accomplish this. The author's professional background granted access to the individuals that can give approval. He works as a government civilian for the Defense Information Systems Agency (DISA) with the Joint Service Provider (JSP) at the Pentagon. Prior to becoming a government worker, the author was a contractor supporting various DoD and DoS agencies. He also has over nine years serving in the United States Navy. Second, the author used a vast number of contacts on LinkedIn. The goal was to find a wide variety of experienced CSSP personnel.

A second barrier was getting Institutional Review Board (IRB) approval. This work involved human subjects, the instruments, and protocols used had to be approved by Nova Southeastern University's IRB prior to conducting the study. Once the IRB approval was obtained, the study had to be completed within a year otherwise it would have to go before the IRB again for approval.

Limitations and Delimitations

This study is limited by the fact that most of the work, personnel, tools, and protocols used are strongly grounded in the DoD/Government perspective. As a result, future research may study how it applies to the commercial sector.

A delimitation of this study is the possibility that not all participants in the study would have direct CSSP work experience. To ensure a high number of quality personnel participating in the study, the study will allow participants with indirect CSSP experience. An example of indirect CSSP experience would be incident response personnel or Cybersecurity personnel responsible for auditing, accrediting and authorizing a CSSP to operate within a DoD environment. To ensure participants have the adequate level of knowledge, personnel must be associated with a CSSP is someway.

Definitions and Acronyms

Terms used throughout this document are defined below.

Accreditation – Formal declaration by an Authorizing Official (AO) or principal that an IS is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards (CNSSI, 2015).

Authorization – Access privileges granted to a user, program, or process or the act of granting those privileges (CNSSI, 2015).

Cloud Service Provider (CSP) – An organization, commercial or private, that offers/provides cloud Services. Use of the term refers to any or all Cloud Service Providers, DoD or non-DoD (DoD CIO, 2014).

Cloud Service Offering (CSO) – A CSP's product or service offering. In other words, a CSO is the actual Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) solution available from a CSP. A CSP may provide multiple CSOs (e.g., Microsoft O-365 (SaaS) and Azure (I/PaaS)). CSO also refers granularly to optional services or software available within any of the service types (e.g., one or more specific database applications optionally available for customer usage under PaaS) (DoD CIO, 2014).

Commercial CSP – A Non-DoD Non-Federal Government organization offering cloud services to the public and/or government customers as part of a business venture, typically for a fee with the intent to make a profit (DoD CIO, 2014).

Computer Network Defense (CND) – Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities (CNSSI, 2015).

Continuous Monitoring (CM) – Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions (Chawla, Dempsey, Johnson, Jones, Orebaugh, Scholl & Stine, 2011).

Cybersecurity – The activity of protecting information and information systems (networks, computers, databases, data centers, and applications) with appropriate procedural and technological security measures (Abdulraza & Zakari, 2016).

Cybersecurity Service Provider (CSSP) – Offers and provides Cybersecurity services in accordance with the DoD CND service provider certification and accreditation program (DoD, 2003).

Cyberspace – the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries (CNSSI, 2015).

DoD CSP – A DoD organization offering cloud services that may be owned and operated by DoD or a contractor for the benefit of the Department (e.g., milCloud). Such services will typically be offered under a cost recovery model. A DoD CSP may offer cloud services to non-DoD mission partners (DoD CIO, 2014).

DoD Off-Premises – A facility (building/container) or information technology infrastructure is Off-Premises if it is not physically or virtually on DoD owned or controlled property (i.e., On-Premises physically or virtually) (DoD CIO, 2014).

DoD On-Premises – A facility (building/container) or information technology infrastructure is On-Premises if it is physically on DoD owned or controlled property. That is, it is within the protected perimeter (walls or "fence line") of a DoD installation (i.e., Base, Camp, Post, or Station (B/C/P/S) or leased commercial space) which is under the direct control of DoD personnel and DoD security policies (DoD CIO, 2014).

Infrastructure as a Service (IaaS) – As defined in NIST SP 800-145, "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)" (NIST, 2011).

Key Terrain – Any locality, or area, the seizure or retention of will provide a marked advantage to either combatant (Applegate et al, 2017).

Key Terrain in Cyberspace (KT-C) – Physical and logical elements of the Cyberspace warfighting domain that enable mission essential warfighting functions (Bodeau et al, 2013).

Non-DoD CSP – A commercial or Federal Government owned and operated CSP (DoD CIO, 2014).

Platform as a Service (PaaS) – As defined in NIST SP 800-145, "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment" (NIST, 2011).

Software as a Service (SaaS) – As defined in NIST SP 800-145, "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings" (NIST, 2011).

Warfighting Domain – The five domains used to conduct war consisting of land, air, maritime, space, and cyber (Pantin, 2017).

Summary and structure of the dissertation

This dissertation report is structured into five chapters. Chapter one provides a background of cloud CISSPs and the history of mapping key terrain in cyberspace. Chapter one, identifies the problem statement, presents research questions, and acknowledges the significance of this work. Barriers, issues, and limitations of this report are addressed along with its limitations and delimitations.

Chapter two offers a literature review which includes previous research in cyberspace, key terrain, cybersecurity, cloud computing, CSSP, and information security continuous monitoring. Chapter two uses literature as a basis to establish the need for research to identify more effective ways to map key terrain in Cyberspace (KT-C).

Chapter three provides the methodology used to conduct the research to include the design and approach. Chapter three discusses the participants, instruments, data collection, and resources used in this work.

Chapter four focuses on the results of the research describing the outcome of phase one and phase two. Chapter five focuses on the research conclusions discussing the implications and recommendations to further this work.

Chapter 2

Review of the Literature

Overview

A review of the literature concerning the mapping of key terrain that supports the CM mission of a cloud CSSP addressed the following areas: Defining Cyberspace and the domain of Cyberspace, to include discussing what makes it unique from traditional warfighting domains. Defining the traditional understanding of key terrain and how it relates to the definition of key terrain in Cyberspace (KT-C), also discussing how it relates to an organization's mission and the significance of mapping key terrain. Defining Cybersecurity, establishing its importance and what is being done about it. Defining what a CSSP is and its role in protecting an IS. Defining cloud computing and what a cloud service provider is. Lastly, defining Information Security Continuous Monitoring (ISCM), describing the development and implementation of ISCM in the context of the United States Government's development and implementation of CM.

Cyberspace Definition

There is no consensus on the definition of Cyberspace (Kuehl, 2009). Kramer (2009), noted that there are numerous definitions of the term Cyberspace. The original source of the term is from William Gibson's 1984 cyberpunk novel "Neuromancer" where Cyberspace was referred to as a navigable, digital space of networked computers accessible from computer consoles. William Gibson is credited with inventing the term Cyberspace (Dodge & Kitchin, 2003; Whittaker, 2004; Kuehl, 2009; Thil, 2009). Dodge and Kitchin (2003) noted that the term Cyberspace is derived from the Greek word kyber (to navigate). Cyberspace literally means

'navigable space'. In the 1990s, the term Cyberspace became popular because it was able to capture the technological advances and ideas that were emerging due to the booming computer and internet phenomena (Thil, 2009).

Carsten Hoff (architect) and Sysanne Ussing (artist), have created works using the term Cyberspace since the 1960s (Kryger & Lillemose, 2015). However, their vision did not include computers. When Hoff was asked why his work did not include computers, his response was that computers did not exist at the time. For this reason, Gibson's use of the term Cyberspace best captures the phenomena as it is used today.

In the past, people may have just associated Cyberspace with a computer connected to the internet. Nevertheless, in the present, the term Cyberspace has evolved to mean much more. Cyberspace encompasses a broad political, social, economic, cultural, and financial network (Whittaker, 2004). The Committee on National Security Systems (CNSS) official Glossary (CNSS, 2015) defines Cyberspace as the interdependent network of information technology infrastructures and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

The Domain of Cyberspace

Researchers have been fascinated with mapping key terrain in Cyberspace ever since the DoD designated Cyberspace as a new warfighting domain back in 1996 (Applegate, Carpenter, & West, 2017; Conti, Cross, Nowatkowski & Raymand, 2014; Bodeau, Graubart, & Heinbockel, 2013). As per Applegate et al (2017), Cyberspace is different from the physical warfighting domains of land, sea, air, and space. It is a nonphysical realm consisting of the interdependent networks of IT infrastructures and resident data, including the Internet, telecommunications

networks, computer systems and embedded processors, controllers, and even the individuals who interact with these systems.

Cyberspace is a new warfighting domain in which warfare attempts to disrupt, deny, degrade, distort, or destroy information and/or information systems necessary to employ military power in the physical domains. DoD has determined that the Cyberspace warfighting domain overlaps overall traditional warfighting domains (Kotson, Schulz, & Zipkin, 2015). It is recognized that all missions within the DoD depend on cyber infrastructure. This fact cannot be said about the other traditional domains. As per Paganini (2016), it's very hard to imagine a military conflict today without a cyber dimension. During the Command, Control, Computers, Communication, intelligence and surveillance (C4ISR) integration Conference (2006), the Secretary of the Air Force Michael W. Wynne remarked that defending and fighting in the Cyber Domain is absolutely critical to maintaining operations in Ground, Sea, Air, and Space. The capital cost of entry to Cyberspace is low. The threat is, that a foe can mass forces to weaken the network that supports operations in other warfighting domains.

Working with other agencies, the DoD is responsible for defending the United States homeland and United States interests from attack, including attacks that may occur in cyberspace. In a manner consistent with the United States and international law, the DoD seeks to deter attacks and defend the United States against any adversary that seeks to harm United States national interests during times of peace, crisis, or conflict (DoD, 2015). Within the DoD Cybersecurity strategy, President Obama has established three primary missions in Cyberspace:

- The first mission, DoD must defend its own networks, systems, and information: The Defense Department must be able to secure its own networks against an attack and recover quickly if security measures fail.

- The second mission, DoD must be prepared to defend the United States and its interests against cyber attacks of significant consequence: If directed by the President or the Secretary of Defense, the United States military may conduct cyber operations to counter an imminent or ongoing attack against the United States homeland or United States interests in cyberspace.
- The third mission, if directed by the President or the Secretary of Defense, DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans: For example, the United States military might use cyber operations to terminate an ongoing conflict on United States terms or to disrupt an adversary's military systems to prevent the use of force against United States interests.

Bambauer (2010) considered government as a key threat to internet freedom. This is due to the fact that the government can control information with its ability to criminalize speech and block content. Barlow (1996) proclaimed cyberspace's desire to be free from government control and expressed the idea of an utopian new world order in which the current governing powers had no right or power to be a part of. (Barlow, 1996) sought to establish cyberspace as a new realm untainted by the seemingly oppressive governments of the world. The article was written in 1996; the work was published the same year the DoD established the cyberspace domain. The author gave the article authority from the future warning that government control over Cyberspace will limit its potential. However, for the sake of the physical world, certain rules must be established (Crovitz, 2011). It is vital that the new Cyberspace domain achieve a balance of freedom and government control through compromise.

Key Terrain Definition

The United States Army Operations Manual (1986) defines key terrain as "any feature, locality, or area which affords a marked advantage to the combatant who controls it." Applegate et al (2017) have defined key terrain as any locality, or area, the seizure or retention of will provide a marked advantage to either combatant. Most often the term key terrain refers to land, water, air, surface or near subsurface terrain (i.e., space).

Key terrain can represent types of physical configurations as well as cultural variability (Pingel, 2003). A broad definition of key terrain makes sense because the non-physical can have influence over the preferred method of military deployment. Collins (1998) explains that the term terrain encompasses the irregularities and configuration of the medium of conflict in whatever form it may take. Key terrain is more than purely areas or locations; key terrain is also the function that makes the areas or locations key.

Conti et al (2014) point out that key terrain was used to describe non-geographic features of an area of operations during General David Petraeus' Senate Confirmation Hearing for Commander of the International Security Assistance Force (ISAF) in Afghanistan when he described the key terrain to be the "human terrain". Human terrain is defined as the human population in the area of operations as defined and characterized by sociocultural, anthropologic, and ethnographic data and other non-geographical information (Grau, Kipp, Prinslow & Smith 2006). Winning the hearts and minds of the people gives a great advantage in war. Tools and weapons of choice can be propaganda campaigns using mediums such as the media, social media, religion, money, fear, and love to inspire and control the population.

Key Terrain in Cyberspace Definition

As previously noted, Applegate et al (2017) have defined key terrain as any locality, or area, the seizure or retention of will provide a marked advantage to either combatant. Cyberspace has logical localities or areas. As a result, KT-C can be defined as any asset, locality, or area within cyberspace, the seizure or retention will provide a marked advantage to either combatant. What establishes KT-C is a matter of debate (Gondree, Leyba, Parker, Price & Staples, 2017).

Jakobson (2013) claims that cyber assets and services, and their intra-/inter-dependencies define what KT-C is. An argument is made that KT-C is encompassed with three sub-terrains which include hardware, software, and service sub-terrains. The hardware sub-terrain includes Network infrastructure (i.e., routers, switches, firewalls, servers, printers, terminal devices, etc.). The software sub-terrain includes software components such as operating systems (OS), applications, etc. The service sub-terrain represents all services like file-transfer, e-mail, universal time, and security services.

In opposition to Jakobson's (2013) approach, Conti et al (2014) note that KT-C research encompasses lists of assets like systems, devices, protocols, data, software, processes, cyber-personas, or other network entities, will leave the impression that everything is KT-C. The work presents a framework for characterizing cyber terrain along the following planes:

- Supervisory Plane. The supervisory plane provides oversight and the authority to start, stop, modify, or redirect a cyber operation. Cyber terrain at the supervisory plane is comprised of elements of cyberspace that either performs a supervisory function or provide a conduit for command and control.
- Cyber Persona Plane. The cyber persona plane identifies identities in the cyber domain. These identities might have a many-to-one or one-to-many relationship with physical

individuals. Here cyber terrain includes such features as user accounts or credentials that provide access to information resources.

- Logical Plane. This plane consists of the operating system, application software, and software settings on a device, and the logical links between networked devices. The terrain at this level includes a wide range of software systems, services, and protocols that keep networks running and computers doing useful work.
- Physical Plane. The physical plane maps to the physical layer of the Open Systems Interconnect (OSI) model and includes components of a computer system and attached hardware. This plane is comprised of the devices that people often interpret as being cyber terrain, such as the routers, switches, and other network devices that physically connect devices in a network.
- Geographic Plane. The geographic plane describes the geographic area in which an IS, or portions of it resides. It is the most static of the planes – geography changes at an extremely slow rate. While the logical location of a network device in cyberspace is often more important than its geographic position, geography can also be relevant, and failure to recognize geographic impact to operations can be costly. Geography is also important when considering the potential path of a state-sponsored cyber operation. Just like flying over one country en route to bombing another could cause an international incident, routing attack packets through a neutral third party could have consequences. This poses a particular challenge during cyber operations when the path that data takes across the Internet can rarely be controlled or even accurately predicted.

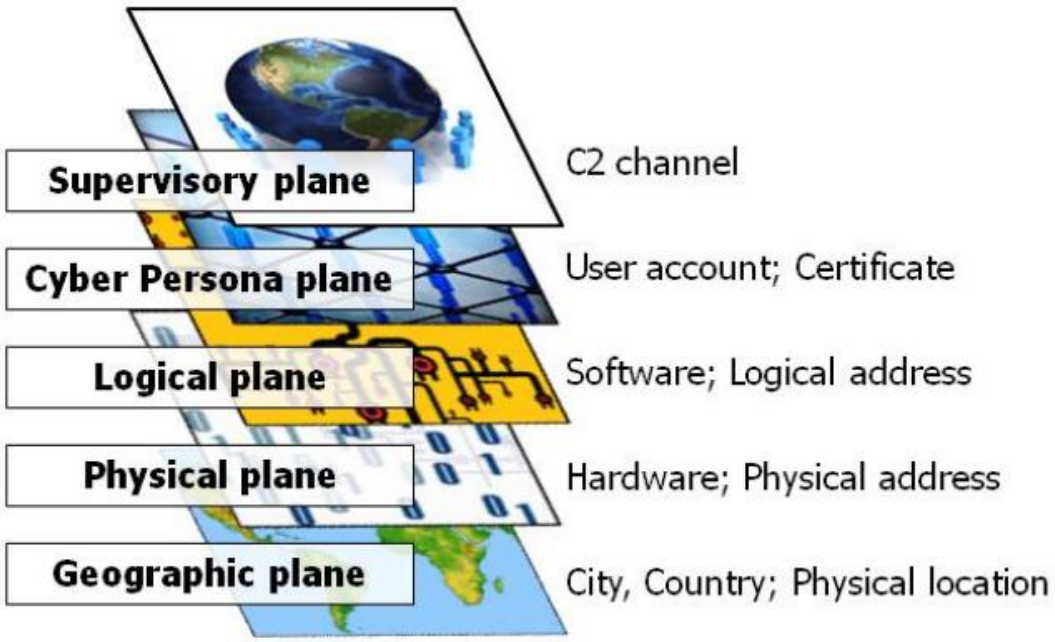

Figure 1. Cyberspace planes

DoD depicts a similar three-layer framework in Joint Publication (2013): the physical network layer, the logical network layer, and the cyber persona layer.

Kotson et al (2015) note that the assets identified as being critical in enabling DoD missions are referred to as the KT-C. Bodeau et al (2013) believed that KT-C constitutes those physical and logical elements of the domain that enable mission essential warfighting functions. Their work seeks to map KT-C to an organization's mission. The work of Bodeau et al (2013) concluded that a map of KT-C will help determine whether:

- Assumptions about features of the cyber terrain (e.g., adversary characteristics and possible adversary actions) are consistent.
- A claim or hypothesis is meaningful to a specific real-world situation or can be evaluated in a given environment.
- A set of claims or hypotheses assume the same environment and thus could be evaluated in a common integration experiment.

- Evidence or analytic results obtained in a given evaluation environment could be used to confirm or disconfirm a given claim or hypothesis.
- A claim or hypothesis supported by evidence from a given evaluation environment could be – or could fail to be – meaningful and relevant to a given real-world situation

Cyber Terrain Mission Mapping

Conti et al (2014) stated that the goal of mission mapping is to identify KT-C. Mission mapping is used to associate cyber terrain with the missions that use it. In the absents of a mission or adversary, these elements are no longer KT-C (Guion & Reith, 2017).

Cybersecurity Definition

According to the United States Executive Office (2009), Cybersecurity is defined as the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation. The private sector defines Cybersecurity with different verbiage yet stays within the spirit of the definition provided by the United States Government.

Pusey and Sadera (2012) refered to Cybersecurity as involving the technical interventions that protect data, identity information, and hardware from unauthorized access or harm. The study pointed out that Cybersecurity includes antivirus software, Internet content filters, firewalls, and password protection. Abdulraza and Zakari (2016) refers to Cybersecurity as the activity of protecting information and information systems (networks, computers, databases, data

centers and applications) with appropriate procedural and technological security measures. It was found that certain solutions like firewalls and anti-virus software are essential to implementing Cybersecurity but are not sufficient to ensure the security of information systems. Pingel (2003), found that the bulk of the work being done to solve cybersecurity problems comes from the computer science community.

Within the release of its May 2018 Cybersecurity Framework version 1.1, the National Institute of Standards and Technology (NIST) define cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks (NIST, 2018). The Cybersecurity Framework version 1.1 was developed by the United States Commerce Department's NIST to provide national and economic security.

Figure 2. Cybersecurity framework version 1.1 core functions.

The NIST states that there are five core functions identified within its Cybersecurity Framework. The core functions are defined below (NIST, 2014).

- Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy
- Protect: Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
- Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables the timely discovery of cybersecurity events. Examples of outcome Categories within this Function include Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this

Function include Response Planning; Communications; Analysis; Mitigation; and Improvements.

- Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include Recovery Planning; Improvements; and Communications.

Importance of Cybersecurity

Eisenmann, Gullestrup. Nolan, & Stephenson (2009) state that hackers don't exactly subscribe to a moral code. Therefore, an organization must be responsible and practice due diligence in keeping security in mind. The proliferation of technology presents cybersecurity challenges and leads to significant national risks. According to the Department of Homeland Security (DHS), more than 20 billion devices are expected to be connected to the internet by 2020 (DHS, 2018). This presents a high risk to a civilization's national and economic security.

The President of the United States Executive Office (2009) identified Cybersecurity as one of the most serious economic and national security challenges we face as a nation. Moreover, President Obama believed that we as a government or as a country are not adequately prepared for. The United States faces threats from a growing set of sophisticated malicious actors who seek to exploit cyberspace. Motivations include espionage, political and ideological interests, and financial gain. Nation-states continue to present a considerable cyber threat. But non-state actors are emerging with capabilities that match those of sophisticated nation-states (DHS, 2018).

The national and economic security of the United States depends on the reliable functioning of critical infrastructure (NIST, 2018). To strengthen the resilience of this infrastructure, President Obama issued Executive Order 13636 (EO), "Improving Critical Infrastructure Cybersecurity," on February 12, 2013. This Executive Order calls for the development of a Cybersecurity Framework that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services.

By the execution of the DHS (2018) Cybersecurity strategy, DHS expects to improve national cybersecurity risk management by 2023. DHS will accomplish this by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities.

In April 2015, DoD presented a strategy that comprised of five strategic goals for its cyberspace missions (DoD, 2015):

- Build and maintain ready forces and capabilities to conduct cyberspace operations: To operate effectively in cyberspace, DoD requires forces and personnel that are trained to the highest standard, ready, and equipped with best-in-class technical capabilities.
- Defend the DoD information network, secure DoD data, and mitigate risks to DoD Missions: DoD cannot defend every network and system against every kind of intrusion. DoD's total network attack surface is too large to defend against all threats and too vast

to close all vulnerabilities. DoD must take steps to identify, prioritize, and defend its most important networks and data so that it can carry out its missions effectively

- Be prepared to defend the United States' homeland and the United States' vital interests from disruptive or destructive cyber attacks of significant consequence: The Defense Department must develop its intelligence, warning, and operational capabilities to mitigate sophisticated, malicious cyber attacks before they can impact the United States.
- Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages: DoD must be able to provide the President with a wide range of options for managing conflict escalation. If directed, DoD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities.
- Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability: Over the next five years, in addition to ongoing partner capacity building efforts in other regions, DoD will focus its international engagement on the Middle East, the Asia-Pacific, and key NATO allies. Through the course of this strategy, DoD will constantly assess the international environment and develop innovative partnerships to respond to emerging challenges and opportunities.

The Trump administration took cybersecurity very seriously. The President of the United States Executive Office (2017) drafted an executive order focused on strengthening the cybersecurity of federal networks and critical infrastructure. President Donald J. Trump's executive order addressed the following cybersecurity concerns:

- Cybersecurity of Federal Networks

    - The President sort to hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises.
- Cybersecurity of Critical Infrastructure
    - The President sort to use his authorities and capabilities to support cybersecurity risk management efforts of the owners and operators of the nations' critical infrastructure focusing on the critical infrastructure at the greatest risk.
- Cybersecurity for the Nation
    - The President wanted to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity while respecting privacy and guarding against disruption, fraud, and theft.

The Trump Administrating is drafting another cyber executive order that focuses on securing cloud computing for companies like Amazon (Amazon Web Services) and Microsoft (Microsoft Azure) (Geller & Overly, 2020).

The United States is not the only nation concerned with Cybersecurity readiness. The European Network and Information Security Agency held a Cybersecurity exercise in October 2014, involving 29 countries and more than 200 organizations, including government bodies, telecoms companies, energy suppliers, financial institutions and Internet service providers (Gabel & Orzechowkis, 2015). The world is responding to the threat cyber presents to the global community. The Global Risks Report published by the World Economic Forum (WEF) (2015) warned that 90 percent of companies worldwide recognize they are insufficiently prepared to

protect themselves against cyber attacks. Annually, cybercrime costs the global economy over $400 billion with the United States accounting for $120 billion (Lewis, J.A., 2013).

Table 1. Putting Malicious Cyber Activity in Context

Putting Malicious Cyber Activity in Context			
CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Note. Reprinted from The Economic impact of cybercrime and cyber espionage, by Lewis, J. A. (2013). *Center for Strategic and International Studies (CSIS).*

Cyber risk is now firmly at the top of the international agenda as high-profile breaches raise fears that hack attacks and other security failures could endanger the global economy (Gabel & Orzechowkis, 2015). As technical innovation throws up new online dangers, Cybercrime is only likely to increase, despite the best efforts of government agencies and Cybersecurity experts. Its growth is being driven by the expanding number of services available online and the increasing sophistication of cyber criminals who are engaged in a cat-and-mouse game with security experts (Gabel & Orzechowkis, 2015).

In response to the global concern of Cybersecurity, the President of the United States Executive Office (2009) mandated a comprehensive national Cybersecurity initiative focused on 12 initiatives:

- Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.

- Initiative #2. Deploy an intrusion detection system of sensors across the Federal enterprise.
- Initiative #3. Pursue deployment of intrusion prevention systems across the Federal enterprise.
- Initiative #4: Coordinate and redirect research and development (R&D) efforts.
- Initiative #5. Connect current cyber ops centers to enhance situational awareness.
- Initiative #6. Develop and implement a government-wide cyber counterintelligence (CI) plan.
- Initiative #7. Increase the security of our classified networks.
- Initiative #8. Expand cyber education.
- Initiative #9. Define and develop enduring "leap-ahead" technology, strategies, and programs.
- Initiative #10. Define and develop enduring deterrence strategies and programs.
- Initiative #11. Develop a multi-pronged approach for global supply chain risk management.
- Initiative #12. Define the Federal role for extending Cybersecurity into critical infrastructure domains.

A recent CompTIA (2016) study on the international trends in Cybersecurity found that 78 percent of the private sector sees the importance of Cybersecurity going up either moderately higher or significantly higher. The study was conducted across 12 different countries and collected information from 1,509 Information Technology and business executives that were divided into two distinct categories: Maturing Economies (Brazil, India, Malaysia, Mexico, South Africa, Thailand, and the UAE) and Mature Economies (Australia, Canada, Germany, Japan, and the UK).

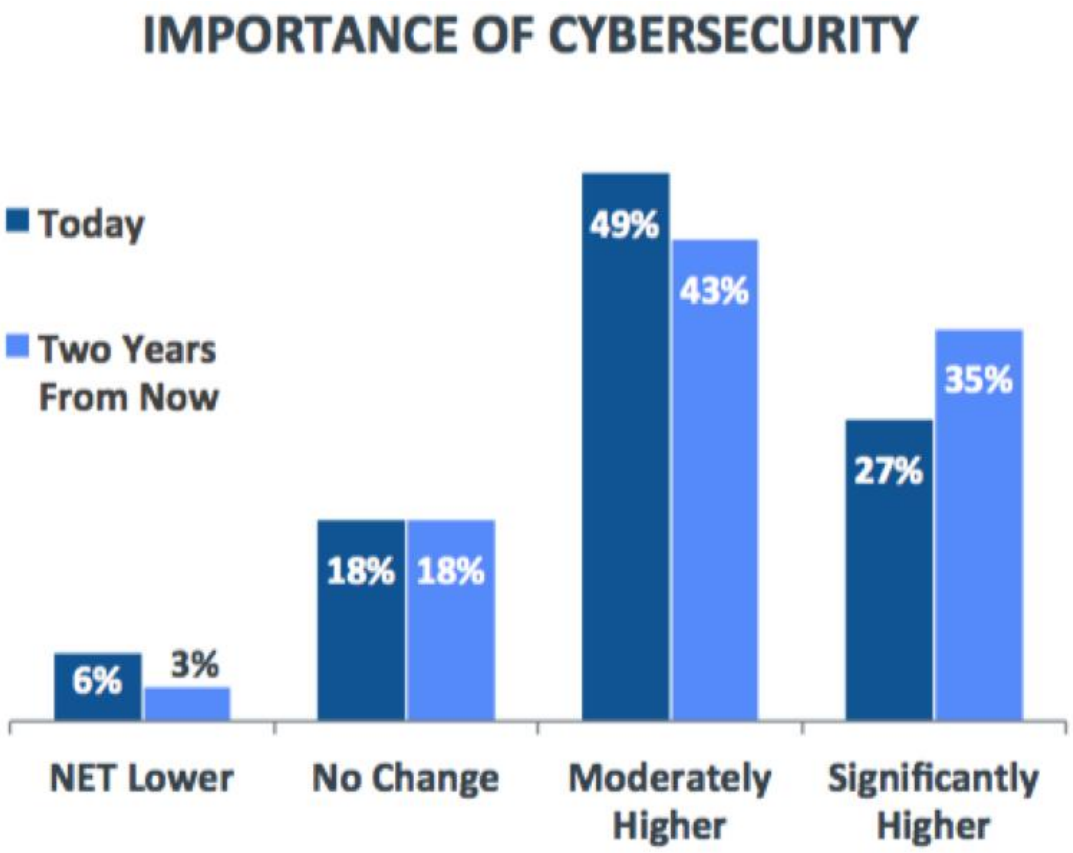

Figure 3. Importance of cybersecurity.

Cybersecurity Service Provider

A CSSP can be also known as a Computer Network Defense Service Provider (CNDSP). The two terms are used interchangeably by the DoD Chief Information Officer (DoD, 2016). As per DoD Instruction 8530.01 CSSPs accomplish the following:

- Offer and provide Cybersecurity services in accordance with the DoD Computer Network Defense (CND) service provider certification and accreditation program (DoD, 2003).
- Execute Cybersecurity responsibilities and authorities in accordance with DoD Component policy, memorandum of agreements, contracts, or support agreements.

- Comply with directives and orders of United States Strategic Command (USSTRATCOM_ and supported DoD Component Navy Operational Support Center (NOSC) and organizations.
- Document all supported entities and associated systems in accordance with DoD Component policy, Memorandum of Agreements (MOAs), contracts, or support agreements.

As per DoD instruction all DoD-owned, managed or operated information systems and computer networks must enter a service relationship with a CSSP (DoD, 2003). Service relationships require subscribers to contribute to computer network situational awareness, including information such as asset inventory and changes in configuration updates to ports, protocols, and services (PPS) registration.

DoD requires all DoD components to measure the effectiveness of a CSSP in accordance with support agreements, MOAs, or contracts. The DoD Chief Information Officer (CIO) and his staff are to resolve issues that cannot be resolved between a DoD component cybersecurity service provider and the external subscribers, as required (DoD, 2016). The following is DoD (2015) guidance on how to measure a components alignment to a CSSP:

- Ensure a Component-established policy, or signed CNDSP Service Agreement, has been established and executed. In addition to any other requirements, the policy or Service Agreement (and any supporting contracts) will include the following requirements:
  - Maintain and provide at least every six months, or upon CNDSP request, accurate configuration management documentation. At a minimum, documentation will include network diagrams, software and hardware inventories, and any PPS listing changes in the PPS Management Registry.

- Notify the CNDSP and provide at least annually any configuration management changes involving connectivity, including location, sensor name, Communications Circuit System Designator (CCSD), bandwidth, IP address space, backend connections, and any changes that could affect NETOPS.
- Update POC information every six months, including leadership/management, all POCs involved in cyber incident handling during and after normal work hours, Senior Security Officer (SSO), policy Point of Contact (POC) lists, and other POCs as requested.
- Provide HBSS data feeds as agreed-upon between the subscriber and the CNDSP. i. If implemented, make HBSS data feeds available to the CNDSP.
- Specify and document agreed-upon security log data and an agreed-upon interval to facilitate network defense and incident response. i. Is there a Component-established policy for, or signed Service Agreement with, a CNDSP that meets the identified requirements? - If yes, then Achieved. - If no, then Not Achieved.

- Provide the CNDSP with network diagrams, software and hardware inventories, network PPS registration, updated POC information, HBSS data feeds (if implemented), and security log data as agreed to in the Agreement or Component-established policy.
  - Have the network diagrams and network PPS listings been updated within six months? - If yes to both, then Achieved. - If no to either or both, then Not Achieved.
  - Has the POC information defined in Agreement or Component-established policy with the CNDSP been updated within six months? - If yes, then Achieved. - If no, then Not Achieved.

- Are HBSS feeds (if implemented) provided to the CNDSP? - If the implementation of HBSS is required and the feeds have been made available, then Achieved. - If HBSS is implemented and operating in a Disconnected, Intermittent, or Limited bandwidth (DIL) environment that limits the ability to transmit the feeds, then Amber (Qualified Yes). - If the implementation of HBSS is required and the feeds have not been made available, then Not Achieved. - If the implementation of HBSS is not required, then Gray (Not Applicable).
- Are security logs provided in accordance with the Agreement or Component established policy with the CNDSP? - If yes, then Achieved. - If no, then Not Achieved.

DoD is not the only organization investing in CSSPs. Pathirana (2017) noted that many organizations today are on a drive to engage CSSPs to tackle everyday challenges or to manage a specific security initiative. Considering the trend of cybercrime, it is safe to expect the demand for competent CSSPs to increase.

Cloud Computing Definition

Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). Can be rapidly built and released with minimal management effort or service provider interaction (NIST, 2011). An organization choosing to use cloud computing services will benefit from cloud computing's convenience, scalability, low costs, security, and high availability

cloud computing is composed of five essential characteristics, three service models, and four deployment models:

Essential Characteristics:

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

Service Models:

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

Deployment Models:

1. Public cloud
2. Community cloud
3. Private cloud
4. Hybrid cloud

Essential Characteristics:

1. **On-demand self-service**: Prime feature of most cloud offerings which allows the management of one's own services without having to communicate with a service provider. Cloud computing provides resources on demand, i.e. when the consumer wants it. This is made possible by self-service and automation. Self-service means that the consumer performs all the actions needed to acquire the service, instead of going through an IT department.

2. **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). Access to resources in the cloud is available over multiple device types. This not only includes the most common devices (laptops, workstations, etc.) but also includes mobile phones, thin clients, and so on.

3. **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

4. **Rapid elasticity**: Elasticity is the degree to which a system can adapt to workload changes by provisioning and deprovisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible.
5. **Measured service**: Resource usage is monitored, measured, and reported (billed) transparently based on utilization. In short, pay for use. This provides transparency for both the provider and consumer of the utilized service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).

Service Models:

1. **Software as a Service (SaaS):** Software on-demand refers to computer applications that are delivered as a service via the Internet. This type of software is also referred to as on-demand software, SaaS (Software-as-a-Service) and Applications-as-a-Service.
    a. **Examples:** Email, Applications

2. **Platform as a Service (PaaS):** PaaS is a service providing remote utilization of an application development platform utilizing cloud computing. This includes not only the remote use of software (as in Software-as-a-Service) but a complete application development and distribution platform.
    a. **Examples:** Operating System, Database, Web Server, Development Tools

3. **Infrastructure as a Service (IaaS):** IaaS architecture is the structural design of a computing network that enables the delivery of computing resources as a service via the cloud. Physical resources such as processing capacity and data storage are examples of common components that may be incorporated into a cloud computing environment, under the IaaS (infrastructure as a service) model of IT resource delivery.
    a. **Examples:** Virtual Machines, Servers, Network, Storage, Load balancers

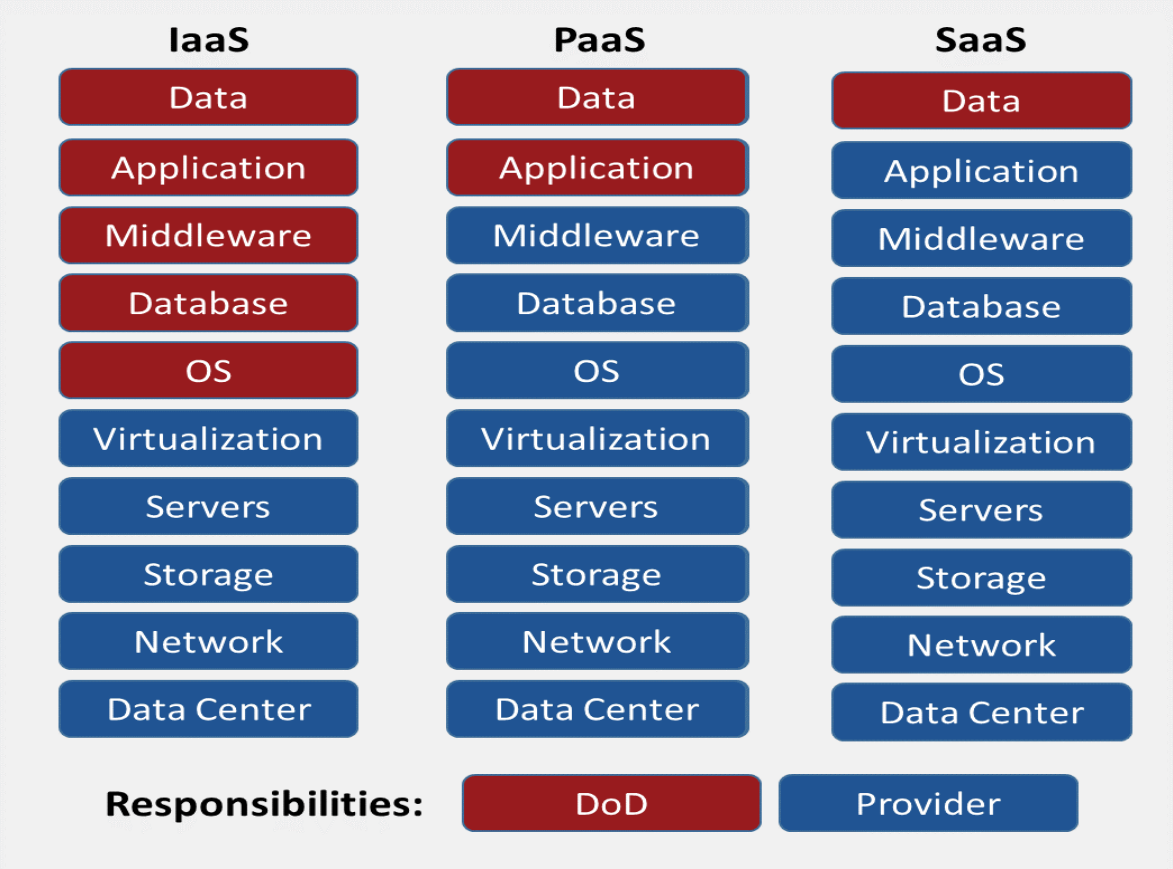

Figure 4. Cloud Service Models.

Deployment Models:

1. **Public cloud:** Infrastructure is provisioned for open use by the general public; exists on the premises of the cloud provider On-demand self-service.

2. **Private cloud:** Infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers; may exist on or off provider premises.

3. **Community cloud**: Infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns; may exist on or off provider premises.

4. **Hybrid cloud:** Infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but bound by standardized or proprietary technology; location depends on specific model.

Impact Levels:

Impact levels can be defined as the level of data to be stored/processed and potential impact of an event resulting in the loss of confidentiality, integrity, or availability of data, systems, or networks. The security control baseline for all Impact Levels is based on moderate confidentiality and moderate integrity in accordance with (IAW) Federal Information Processing Standards Publications 199 (FIPS-199), DoDI 8510.01 and CNSSI 1253. Availability is determined by the mission owner and should be specified in a contract or service level agreement.

Table 2. Cloud Impact Levels

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

Note. Reprinted from the Cloud computing security requirements guide (SRG), by the Defense Information System Agency (DISA) (2017). https://dl.cyber.mil/cloud/SRG/index.html#4RISKASSESSMENTOFCLOUDSERVICEOFFERINGS

Cloud Service Provider

A Cloud Service Provider (CSP) is an entity that offers one or more cloud services in one or more deployment models (DoD, 2017). CSPs offering SaaS may leverage one or more third party Cloud Service Offerings (i.e., for IaaS or PaaS) to build out a capability or offering. The DoD CIO describes CSPs as an organization, commercial or Private, that offers/provides cloud services. Use of the term refers to any or all Cloud Service Providers, DoD or non-DoD (DoD CIO, 2014)

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services (FedRAMP, 2011).

The use of FedRAMP is mandated for all Federal Agencies by the Office of Management and Budget (OMB) as their systems and applications are migrated to the commercial cloud under the Federal Government's Cloud-First initiatives. The December 2011 OMB FedRAMP policy memo requires Federal departments and agencies to utilize FedRAMP approved CSPs (FedRAMP, 2011).

Information Security Continuous Monitoring in Government

Aspects associated with ISCM is identified in the comprehensive national Cybersecurity initiative by the President of the United States Executive Office (2009). Initiatives one, two, three, and five directly relate to ISCM:

- Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.
- Initiative #2. Deploy an intrusion detection system of sensors across the Federal enterprise.
- Initiative #3. Pursue deployment of intrusion prevention systems across the Federal enterprise.
- Initiative #5. Connect current cyber ops centers to enhance situational awareness.

The United States Government identifies the National Institute of Standards and Technology (NIST) special publication 800-137 as the official guidance concerning ISCM. Within the special publication, the work of Chawla, Dempsey, Johnson, Jones, Orebaugh, Scholl and Stine (2011) define ISCM as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and

analyzed at a frequency sufficient to support risk-based security decisions to adequately protect government/organization information. Chawla et al. (2011) also established that ISCM uses both automation and manual techniques to validate implementation compliance with government/organizational mandated security controls. The implementation of a robust continuous monitoring program allows an organization to understand the security state of the system over time and maintain the initial security authorization in a highly dynamic operating environment with changing threats, vulnerabilities, technologies, and missions/business functions.

Chawla et al. (2011) provide guidance on the development of a comprehensive ISCM program. The key to success with the development of an ISCM requires the communication of all stakeholders in executing the following process:

- Define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
- Establish an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
- Implement an ISCM program and collect the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.
- Analyze the data collected and Report findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.
- Respond to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.

- Review and Update the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization's information infrastructure, and increase organizational resilience.

Chawla et al. (2011) required the development of an ISCM Enterprise Architecture (EA) to determine how information will be collected and delivered throughout as well as external to the government/organization. The core requirements of an architecture implemented to support ISCM are the following:

- Data collection,
- Data storage,
- Data analysis capabilities,
- and retrieval and presentation (reporting) capabilities

Booth, Feldman, McBride, Mell, Ouyang, Regland and Waltermire (2012) established the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Framework Extension as an example of a suitable ISCM EA to follow when implementing an ISCM strategy. CAESARS was the result of a DHS evaluation of successful CM implementations within the civilian government: Department of State, Department of Justice, and Department of the Treasury. Booth et al. (2012) note that the CAESARS EA consists of the following subsections:

- Data Sources: The data sources for CM include the categories of people, process, technology, and the environment. The people, process, and environment data types do not always lend themselves to fully automated data collection efforts and in most cases will require some human data collection effort.

- Data collection: A variety of methods, both automated and manual, can be used to collect data. Human-generated data (e.g., from user surveys or security compliance documentation) should be collected using mechanisms that harness automation and that leverage standardized methods. In addition, the appropriate frequency for data collection needs to be determined for each data feed.
- Data storage and Analysis: The collected data will initially reside in a local repository near the point of collection and then may be aggregated at higher tiers in the organization. Having CM data available at each tier enables users at that tier to have an appropriately abstracted view into the organization's security posture.
- Consumer Presentation: Each tier within the data storage layer will provide a view of the data to consumers. The presentation layer needs to be flexible enough to satisfy diverse data display needs because the CM implementation must support many types of consumers. Primarily the CM implementation should support the operational mission of helping to secure an organization (likely through situational awareness dashboards). It will also need to support compliance reporting, executive-level reporting, and reporting of non-security use cases.
- Consumer, Decisions and Decision Drivers: There are many types of consumers that need CM data ranging from system administrators, to the organization Chief Information Officer (CIO), to possibly external compliance or auditing entities. These consumers need to make decisions (especially those regarding effectiveness, efficiency, security, and compliance) based on a set of drivers.

According to the Joint Task Force Transformation Initiative Interagency Working Group (2013), ISCM activities are implemented in step six of the Department of Defense (DoD) Risk Management framework that consists of the following steps:

- Step 1: Categorize the IS based on a FIPS Publication 199 impact assessment.
- Step 2: Select the applicable security control baseline based on the results of the security categorization and apply tailoring guidance (including the potential use of overlays).
- Step 3: Implement the security controls and document the design, development, and implementation details for the controls.
- Step 4: Assess the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Step 5: Authorize IS operation based on a determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the IS and the decision that this risk is acceptable; and
- Step 6: Monitor the security controls in the IS and environment of operation on an ongoing basis to determine control effectiveness, changes to the system/environment, and compliance with legislation, Executive Orders, directives, policies, regulations, and standards.

The implementation of an ISCM strategy cannot be efficiently achieved through manual processes alone or through automated processes alone. They must both be used to implement continuous monitoring effectively (Chawla et al., 2011). An effective ISCM strategy is comprised of the following:

- Includes metrics that provide meaningful indications of security status at all organizational tiers.
- Ensures the continued effectiveness of all security controls.
- Verifies compliance with information security requirements derived from organizational missions/business functions, federal legislation, directives, regulations, policies, and standards/guidelines.
- Is informed by all organizational IT assets and helps to maintain visibility into the security of the assets.
- Maintains awareness of threats and vulnerabilities.
- Necessitates actionable communication of security status across all tiers of the organization.

DoD (2014) has taken steps to implement a multi-tiered cybersecurity risk management process to protect United States interests, DoD operational capabilities, and DoD individuals, organizations, and assets from the DoD information enterprise level, through the DoD component level, down to the IS level. DoD is adopting NIST 800-137 as its approach for ISCM. An effective ISCM strategy utilizes both automated and manual means to assess the effectiveness of security controls. The strategy should encompass people, processes and procedures, technology, and operating environments. Chawla et al. (2011) recommended a three-tiered approach to establish an effective organizational–wide ISCM strategy.

- **Tier 1**: Risk management activities address high-level information security governance policy as it relates organizational risk to its core missions, and its business functions.
- **Tier 2**: In this tier, criteria for continuous monitoring of information security are defined by how core mission/business processes are prioritized with respect to the overall goals

and objectives of the organization, the types of information needed to successfully execute the stated mission/business processes, and the organization-wide information security program strategy.

- **Tier 3**: The last tier addresses risk management from an IS perspective. These activities include ensuring that all system-level security controls (technical, operational, and management controls) are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time.

Figure four is a depiction of a three-tiered continuous monitoring strategy in which the following activities are executed:

(A) Assets provide information to the tools.

(B) The tools collect information from the assets.

(C) The tools store the information in their respective repositories.

(D, E) Analysis of the information presents data in a way that is meaningful to consumers.

(F, G) Consumers use the information to make organizational risk management decisions that are based on the decision drivers provided by policies at tier 1.

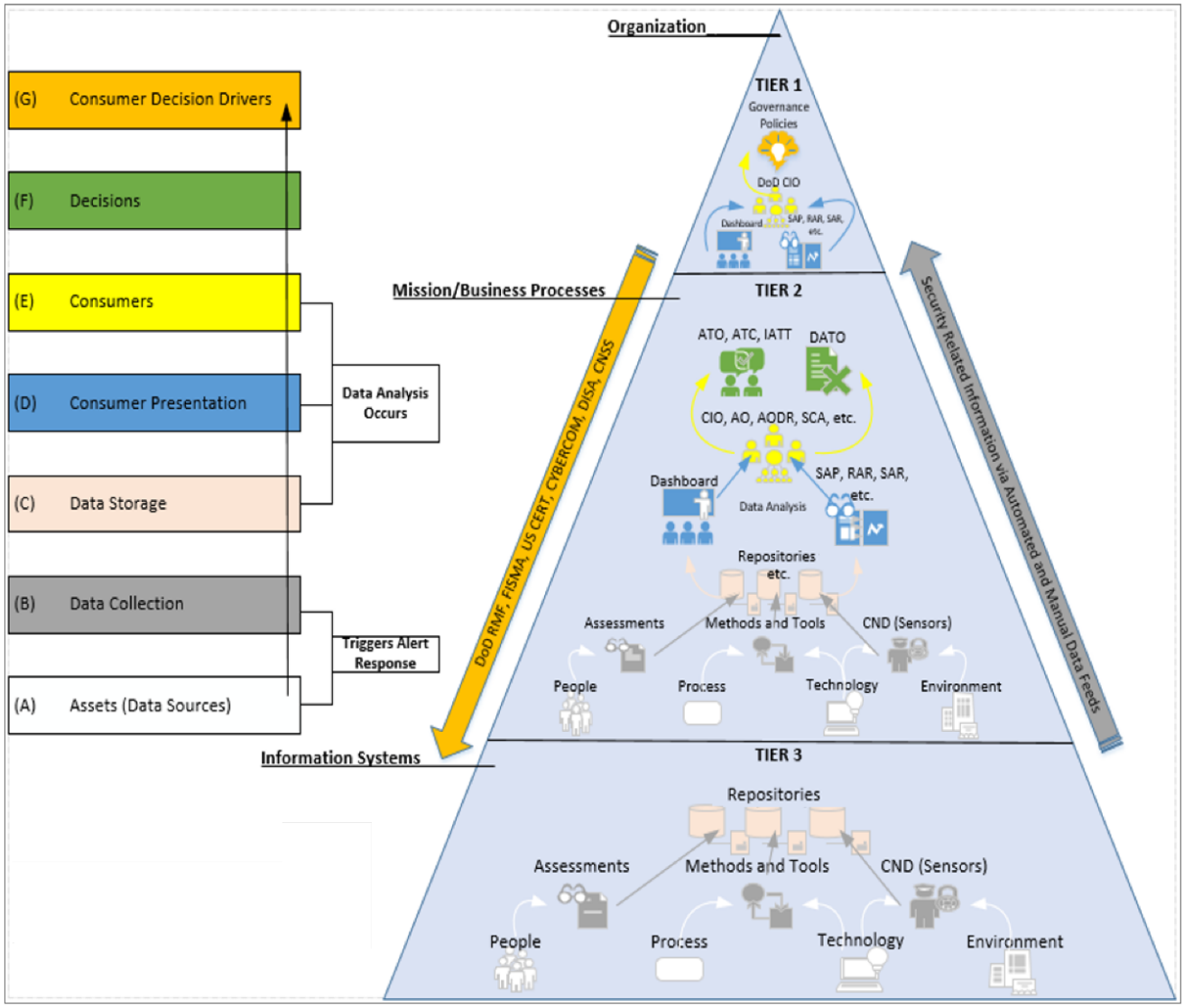

Figure 5. Three-tiered information security continuous monitoring architecture.

Chapter 3

Methodology

Overview of Research Methodology

Future cyber strategists and military minds will have to break from the traditional mindset when identifying key terrain in Cyberspace (Pantin, 2017). This work provided an effective way to map KT-C through a contextual approach that focused on a specific objective or mission within cyberspace. Each context can be used as modules that fit together to form the big picture. This chapter covers the design and method of the study. The sections to come describe the research's theoretical framework, the approach used to conduct the research, how data was collected, and the resources that were required to complete this study.

Research Design

Research can use a quantitative or a qualitative approach (Nardi, 2003; Creswell, 2003). The research design for this study used the mixed method approach. Bougie and Sekaran (2016) mentioned that the mix method approach allows the researcher to collect mixed data on many types of research questions. Once the data are collected, the data can be validated and evaluated. Studies that use the mix method draw on the strengths of mixed research (Creswell, 2013). A mixed-method approach to research allows for a more comprehensive evaluation of the constructs and enhances the overall confidence in the findings of the study (Shank, 2006). Creswell (2013) argued that there are four key features to mixed methods research:

- Collecting and analyzing qualitative and quantitative data in response to research questions.

- Using rigorous qualitative and quantitative methods
- Combining or integrating quantitative and qualitative data using a specific type of mixed method design.
- Framing the mixed methods design within a broader framework (e.g., experiment. Theory, or philosophy).

The purpose of this descriptive study was to map the key terrain that supports the CM mission of a cloud CSSP. This study had minimal interference with the day to day activities of the participants and is correlational in nature. The study setting is non-contrived and took place in the natural environment of cybersecurity professionals. Correlational studies done in non-contrived settings are called field studies (Bougie & Sekaran 2016). The research strategy utilized the mixed method approach to develop, test, validate and correlate the results from surveys used to identify the key terrain that supports the CM mission of a cloud CSSP. Fowler (2013) argued that the purpose of a survey is to produce statistics that are a quantitative or numerical description of some aspects of the study population. A survey is a system for collecting information from or about people to describe, compare, or explain their knowledge, attitudes, and behavior (Fink, 2003). According to Fink, the survey system includes setting objectives for data collection, designing the study, preparing a reliable and valid survey instrument, administering the survey, managing and analyzing survey data, and reporting the results.

Galliers (1992) defined surveys as essentially ‘snapshots’ of practice, situations or views at a particular point in time. Quantitative techniques are often used in analyzing survey results. Surveys are undertaken using questionnaires or interviews from which inference may be made. For this reason, the use of surveys was ideal in ascertaining the critical assets that map to the key

terrain that supports the CM mission of a cloud CSSP. The survey instruments were developed and validated for the qualitative and quantitative phases of the mixed-method research. The research model followed the steps shown in figure 6.

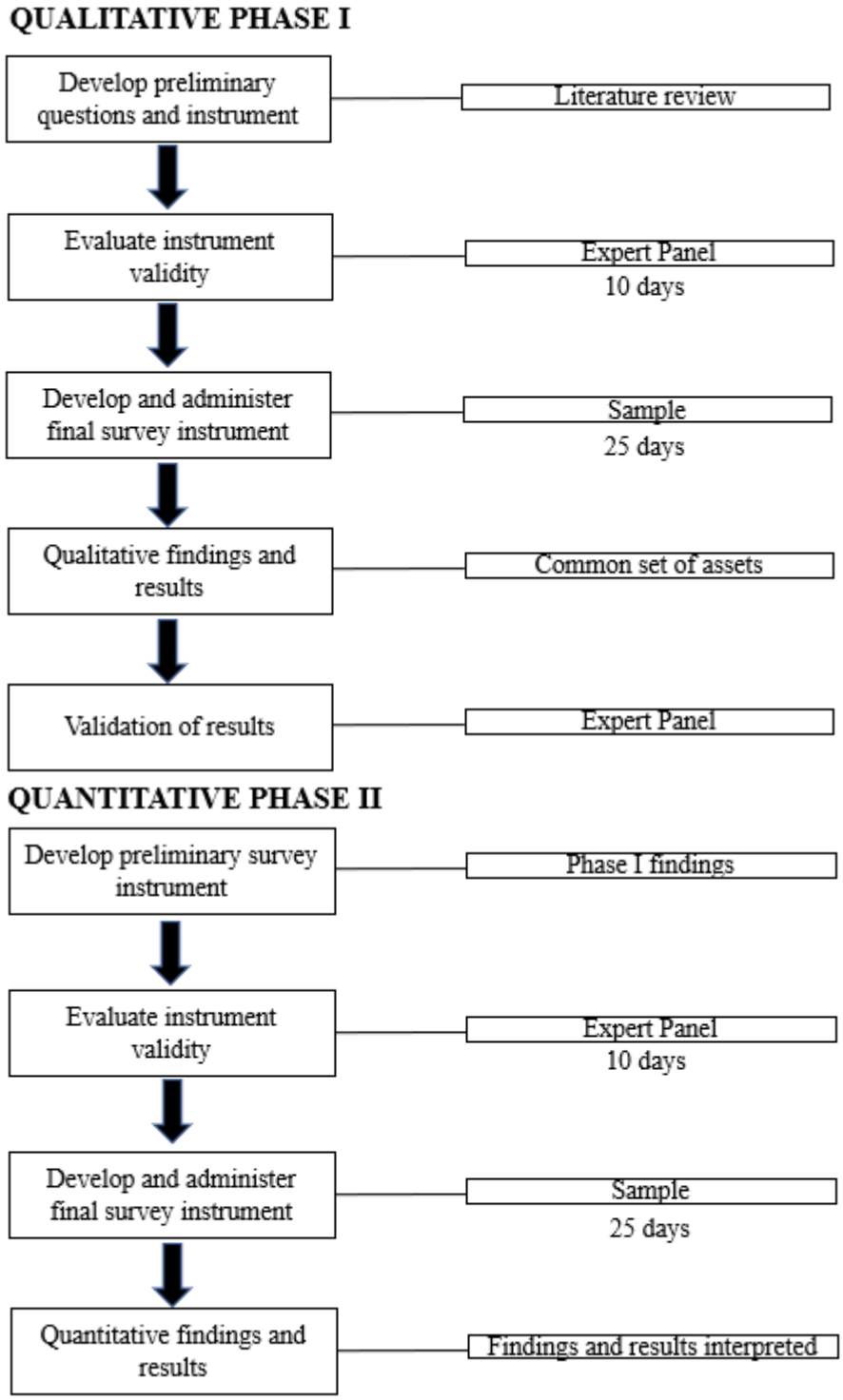

Figure 6. Research model

The quantitative survey used a seven-point Likert-type scale to collect data. Seven-point scales are considered to produce more accurate responses than a five-point scale Finstad (2010).

Approach

The qualitative approach used relied heavily on content analysis of literature reviews. The content analysis was based on research covering the cyberspace domain, KT-C, and the continuous monitoring mission of a cloud CSSP. Based on the content analysis, a list of preliminary questions was developed as shown in Table 3.

Table 3. Preliminary Questions

Q1	What is the mission of a typical cloud Cybersecurity Service Provider?
Q2	Identify the assets (personnel, systems, tools, devices, policies, facilities, etc.) of a typical cloud CSSP.
Q3	Of the identified assets, which ones do you consider critical (the mission will fail without it) of a typical cloud CSSP?

The list of preliminary questions was presented to a panel of cybersecurity professionals who support the mission of a cloud CSSP. The panel of experts validated the questions and provide feedback for introducing additional questions to the list using the expert review questionnaire presented in appendix B. Ten days was dedicated to interviewing the experts who were willing to participate in the validation. The minimum number required was ten experts. Therefore, more time would have been allotted to meet the minimum number of interviews.

A final survey instrument was developed based on the feedback of the panel of experts. The developed survey instrument was administered to participants that comprised of cybersecurity professionals who support the mission of a CSSP. The qualitative findings and

results were used to identify the mission of a typical CSSP along with the identification of a cloud CSSP's assets.

The quantitative approach used the findings and results of the final qualitative survey instrument to develop a preliminary quantitative survey instrument. The instrument utilized a seven-point Likert-type scale to assess the common set of assets identified as part of the continuous monitoring mission of a cloud CSSP. The instrument had two sections. A section for non-critical assets and a section of critical assets. Participants were asked to rank the importance of non-critical assets to the continuous monitoring mission of a cloud CSSP. In section two, participants were asked to identify the estimated time of restoration (ETR) associated with a critical asset. Critical assets enable a cloud CSSP's continuous monitoring mission. If a critical asset is unavailable, the continuous monitoring mission is halted until the asset is restored. Table 4 is an example of the preliminary quantitative survey instrument.

Table 4. Preliminary Quantitative Survey Instrument

How important is the identified asset to the continuous monitoring mission of a CSSP?

	1.) Very unimportant	2.) Unimportant	3.) Somewhat unimportant	4.) Neutral
	5.) Somewhat unimportant	6.) Important	7.) Very important	

	Assets	1	2	3	4	5	6	7
1	Asset Example 1	o	o	o	o	o	o	o
2	Asset Example 2	o	o	o	o	o	o	o
3	Asset Example 3	o	o	o	o	o	o	o

If the identified critical asset fails, how will it impact the estimated time of restoration (ETR) to the continuous monitoring mission of a CSSP?

	1.) ETR < 1 hr.	2.) ETR > 1 hr. < 8 hrs.	3.) ETR > 8 hrs. < 24 hrs.	4.) ETR > 24 hrs. < 48 hrs.
	5.) ETR > 48 hrs. < 72 hrs.	6.) ETR > 72 hrs. < 96 hrs.	7.) ETR > 96 hrs.	

	Citical Assets	1	2	3	4	5	6	7
1	Asset Example 1	o	o	o	o	o	o	o
2	Asset Example 2	o	o	o	o	o	o	o
3	Asset Example 3	o	o	o	o	o	o	o

Once the instrument was developed, it was administered to an expert panel of cybersecurity professionals who support the mission of a CSSP. The expert panel evaluated the validity of the instruments. During this time, the panel had the chance to make suggestions for changing the criticality status of identified assets. The experts were given ten days to provide feedback. A final survey instrument was developed based on feedback and validation from the expert panel. The final survey was administered to participants. From there, the results were analyzed, interrupted, and reported.

Participants

The participants were cybersecurity professionals from the Department of Defense (DoD), and private sector contractors supporting the mission of a CSSP. The participants had experience working in a CSSP environment or supporting a CSSP's mission on or off-site for DoD branches, commands, and field activities. The sample size sort was approximately 100 participants. This was to give a 10% margin of error (or confidence interval). The margin of error derives from the formula $1/\sqrt{N}$, where N is the number of participants or sample size (Niles, 2018). The participants were recruited utilizing LinkedIn and professional contacts to include Cybersecurity professionals with various years of experience working in a CSSP environment. They were asked to participate in a survey answering the following in regard to a typical cloud CSSP:

Identify the mission of a typical cloud CSSP.

- Identify the assets (personnel, systems, tools, devices, protocols, facilities, etc.) of a typical cloud CSSP.
- Identify the critical assets of a typical cloud CSSP.

- Identify the ranking of critical assets in respect to the CM mission of a typical cloud CSSP.

Privacy Protection

Research involving human participants required IRB approval by the researcher's institution (Creswell, 2003). The IRB ensures there are no ethical concerns with the research. Moreover, the IRB protects the participants' privacy. This research did not collect any personal identifiable information (PII) associated with any participant. PII was not significant and had no bearing on the findings of this research. Therefore, in the event the data had a compromise of confidentiality, the participants were assured that their anonymity was protected. The only participant specific information collected was associated with the years of experience working in a CSSP environment:

Table 5. Security Experience Question

1. How many years of experience do you have with CSSPs?	Under 1	1 to 2	3 to 5	5 to 10	Over 10

Cover Sheet

A cover sheet was provided to include a statement informing the participant that the survey was for a doctoral dissertation stating the following:

- All information collected is confidential.
- This survey complies with IRB requirements.
- All information gathered will remain anonymous.

Survey Instruments

The preferred survey instruments used for this research was interviews. Interviewing is a useful data collection method, especially during the exploratory stages of research (Bougie & Sekaran, 2016). The interviews were conducted in the form of a structured questionnaire as shown in Appendix A, Appendix B, and Appendix C.

Survey Monkey was utilized so participants can answer the questions in off hours. Survey Monkey is an online survey tool used to create surveys and design research questions. The tool is very popular and easy to distribute to the participants in the research. The following is the website for Survey Monkey: https://www.surveymonkey.com/

Considering the classified nature of some participants involved in this research, there was a situation in which a participant did not have access to Survey Monkey. To overcome this obstacle, the survey questions were delivered via email. If a participant did not have access to a computer, he or she would have been contacted via phone or in person to conduct the survey.

Data Collection

The data collection method for the surveys came in the form of interviews and questionnaires from the following:

- Electronic media (e.g., email, website, etc.).
- Papers handed out in-person or mailed.
- Interviews conducted in-person, over the phone, or video conferenced (e.g., Skype).

This research did not collect any personal identifiable information (PII) associated with any participant. PII is not significant and had no bearing on the findings of this research. Therefore, if the data had a compromise of confidentiality, the participants were assured that their anonymity

was protected. This data was available to the researcher, the Institutional Review Board and other representatives, and any granting agencies (if applicable). All confidential data was kept securely offline in a Federal Information Processing Standards (FIPS) 140 approved encrypted external HD. All data will be kept for 36 months from the end of the study and destroyed after that time by wiping the drive with BleachBit or similar technology.

After the initial survey, the data were analyzed, and a second survey was sent to the participants. The second survey was a terrain analysis of all assets identified as being critical to the CM mission of a typical CSSP. The results of the terrain analysis conclude the research.

Resources

The resources needed to conduct the research associated with mapping the key terrain that supports the continuous monitoring mission of a Cybersecurity service provider included the following:

- Volunteer participants from the United States Government personnel/contractors, and other Cybersecurity practitioners from the private sector.
- Equipment and tools to conduct surveys (e.g., computer, printer, phone, software, paper, survey monkey, etc.).
- A Survey Analysis Tool/ Quantitative Research - Methods of Data Analysis & Software.
- Access to a Cybersecurity Service Provider

Research level of effort

The following is the high the level of effort put forth to complete the study on mapping the key terrain that supports the continuous monitoring mission of a cloud CSSP:

- Initiated the Dissertation Process
- Worked with the Dissertation Chair
- Produced the Dissertation Documents
    - Dissertation Idea Paper
    - Dissertation Proposal
    - Dissertation Report
- Defend the Dissertation
- Complete the Dissertation Report
- Publish Dissertation Results

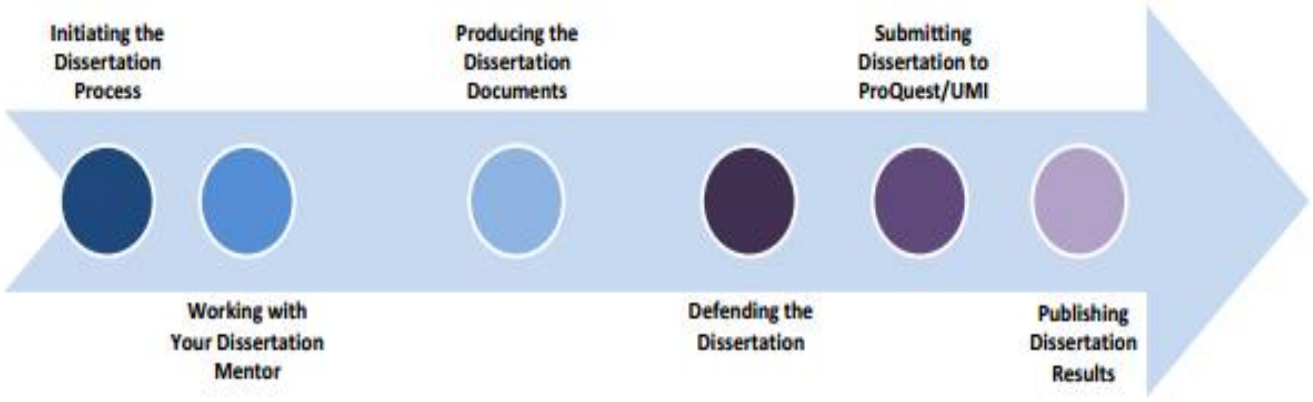

Figure 7. The dissertation process: From Nova Southeastern dissertation guide

Chapter 4

Results

Overview

This study had two phases. The first phase presented is a qualitative study that relied heavily on content analysis of literature reviews. The second phase presented is a quantitative study. It used the findings and results of phase one to understand the estimated time of restoration for each asset identified.

Phase One – The Qualitative Study

Phase one's primary objective sought to understand three subjects:

- The mission of a typical cloud CSSP
- Identify the assets (personnel, systems, devices, polices, facilities, etc.) of a typical cloud CSSP
- Identify the critical (the mission will fail without it) assets of a typical cloud CSSP

Data was captured in the form of interviews and questionnaires using electronic media (e.g., email, website, etc.) and papers handed out in-person or mailed. For this phase of the study, the initial survey instrument was sent to a panel of ten CSSP experts. The experts responded positively. Initially, this study was to focuse on the continuous monitoring mission of a typical CSSP. However, feedback from three of the ten experts changed the focused to a cloud CSSP. The significance of cloud computing in the DoD community is what drove the change. The experts found the survey instrument appropriate.

The survey instrument was administrated to 103 cybersecurity professionals via LinkedIn. Only 57 have responded positively resulting in a response rate of approximately 55%. This did not meet expectations based in the design of the research. A sample size of 57 participants gave a 13% margin of error (or confidence interval). This is an increase of 3% from design expectations of 10% margin of error. The margin of error derives from the formula $1/\sqrt{N}$, where N is the number of participant or sample size (Niles, 2018). The results to RQ1.1 are identified below:

The mission of a typical cloud CSSP as defined by the cybersecurity professionals who participated in this study was derived from the feedback of 24 participants. Out of the 57 participants that completed the questionnaire, only 24 provided feedback regarding what they believed to be the mission of a typical cloud CSSP. Each of the 24 participants gave a response that could be put into two categories:

- Ensure the mission of a cloud information system
- Deliver cybersecurity services to a cloud information system

The following summarizes the responses of the 24 participants: The mission of a cloud CSSP is the mission assurance of cloud information systems through the execution of cyber services as defined in the Service Level Agreement (SLA) made in conjunction with information system owners.

The 57 participants who responded identified 28 different assets that support the continuous monitoring mission of a cloud CSSP. The 28 assets were split into four categories (People, Policy, Infrastructure and Platform). The following is a breakdown of how many assets fell in each category: People (6), Policy (12), Infrastructure (6), and Platform (4). Policy received the most assets and platform received the least.

Table 6. Assets of a typical cloud CSSP

Name	Description	Source
People		
Analyst	A person who analyzes data	
Infrastructure support	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the cloud cybersecurity service provider network and resources	NIST SP 800-181
Incident responder	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave	NIST SP 800-181
Auditor	Conducts evaluations of components to determine compliance with published standards.	NIST SP 800-181
Service provider manager	The person responsible for controlling the activities associated with a service provider	
Personnel security manager	Manages the daily activities a personnel security program	
Policy		
Continuous monitoring strategy	Documentation on how a system maintains ongoing awareness to support organizational risk decisions.	CNSSI 4009
Incident response plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattacks against an organization's information system	CNSSI 4009
Service level agreement	Defines the specific responsibilities of the service provider and sets the customer expectations.	CNSSI 4009
Contingency plan	Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability	CNSSI 4009
Training plan	Guides the planning and delivery of instruction in the form of on the job training and certification requirements	
Change management plan	The process for dealing with changes within the environment	

Acquisition strategy	Describes the acquisition approach that Program Management will follow to manage program risks and meet program objectives	
Risk management plan	A plan on how to execute the identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks	
Physical security	The use of physical and electronic measures designed to monitor people and objects, and control access and intrusion to property and information	CNSSI 4009
Asset management	Monitors and maintains things of value	
Vulnerability management	A process to ensure that systems are safe from cyber threats	
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions.	CNSSI 4009
Infrastructure		
Storage	Systems used to store information	
Boundary security	The monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication. Protection is achieved using gateways, routers, firewalls, guards, intrusion detection/prevention systems, and encrypted tunnels	CNSSI 4009
Network Devices	Routers, switches, etc.	
Facility	Physical location where the cloud CSSP resides	
End point devices	Computer, monitors, end user devices, etc.	
Public Key Infrastructure	A system for the creation, storage, and distribution of digital certificate	
Platform		
Host based security	Anti-virus software, host intrusion detection/prevention, vulnerability scanning software, encryption of data at rest, audit logging	

Operating system	Windows, Linux, etc.	
Database	Oracle, SQL, etc.	
Security event incident manager	Software used for identifying, monitoring, recording and analyzing security events or incidents within a real-time IT environment (i.e., Splunk, Bro, Archsite, etc..)	

The 57 participants identified 16 different critical assets that support the continuous monitoring mission of a cloud CSSP. The following is a breakdown of how many assets fell in each category: People (3), Policy (3), Infrastructure (6), and Platform (4). Infrastructure received the most critical assets and policy received the least.

Table 7. Critical Assets of a typical cloud CSSP

Name	Description
People	The personnel doing the work
Infrastructure support	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the cloud cybersecurity service provider network and resources
Incident responder	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave
Service provider manager	The person responsible for controlling the activities associated with a service provider
Policy	
Continuous monitoring strategy	Documentation on how a system maintains ongoing awareness to support organizational risk decisions.

Incident response plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattacks against an organization's information system
Service level agreement	Defines the specific responsibilities of the service provider and sets the customer expectations.
Infrastructure	
Storage	Systems used to store information
Boundary security	The monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication. Protection is achieved using gateways, routers, firewalls, guards, intrusion detection/prevention systems, and encrypted tunnels
Network Devices	Routers, switches, etc.
Facility	Physical location where the cloud CSSP resides
End point devices	Computer, monitors, end user devices, etc.
Public Key Infrastructure	A system for the creation, storage, and distribution of digital certificate
Platform	
Host based security	Anti-virus software, host intrusion detection/prevention, vulnerability scanning software, encryption of data at rest, audit logging
Operating system	Windows, Linux, etc.
Database	Oracle, SQL, etc.
Security event incident manager	Software used for identifying, monitoring, recording and analyzing security events or incidents within a real-time IT environment (i.e., Splunk, Bro, Archsite, etc..)

Phase Two – The Quantitative Study

Phase two presents the quantitative findings of this research study. The dissertation goal of this study was to map the key terrain that supports the Continuous Monitoring (CM) mission of a Cloud CSSP. This was accomplished by assessing the responses of cybersecurity professionals with experience working within a cloud or CSSP environment. This work also ascertained how to identify key terrain in a contextual manner specific to the mission of a typical Cloud CSSP. The findings are presented in frequency tables. A simple frequency table is the most common way to show the number of times each item occurs in a data-set (Heiman, 2006).

The quantitative phase survey instrument was developed from the results of the qualitative phase. The qualitative results were formatted into a web-based Survey Monkey instrument and then sent out to 408 cybersecurity professionals. Only 61 responses were received. This provided a response rate of approximately 15%. The data collection period took six weeks. It proved to be difficult in finding participants who believed they had the skillset and experience to complete the survey instrument. All 61 of the participants completed 100% of the survey. A sample size of 61 participants gave an approximate 12.8% margin of error (or confidence interval). The margin of error derives from the formula $1/\sqrt{N}$, where N is the number of participants or sample size (Niles, 2018). The survey instrument did not allow for any manual input for answers. Participants selected the answers based on multiple-choice options that were derived from the results of the qualitative phase. Assets were ranked from high to low based on the weighted average of their importance level as identified by the participants. The results are identified below:

Table 8. Asset importance frequency table

	VERY UNIMPORTANT	UNIMPORTANT	SOMEWHAT UNIMPORTANT	NEUTRAL	SOMEWHAT IMPORTANT	IMPORTANT	VERY IMPORTANT	TOTAL	WEIGHTED AVERAGE
Incident responder	3.28% 2	0.00% 0	1.64% 1	4.92% 3	6.56% 4	19.67% 12	63.93% 39	61	6.26
Patch Management	3.28% 2	1.64% 1	1.64% 1	1.64% 1	8.20% 5	19.67% 12	63.93% 39	61	6.25
Continuous monitoring strategy	3.28% 2	3.28% 2	0.00% 0	3.28% 2	4.92% 3	19.67% 12	65.57% 40	61	6.25
Analyst	3.28% 2	0.00% 0	1.64% 1	3.28% 2	11.48% 7	29.51% 18	50.82% 31	61	6.11
Contingency plan	3.28% 2	0.00% 0	4.92% 3	6.56% 4	6.56% 4	16.39% 10	62.30% 38	61	6.11
Vulnerability management	3.28% 2	4.92% 3	0.00% 0	4.92% 3	6.56% 4	19.67% 12	60.66% 37	61	6.08
Incident response plan	4.92% 3	0.00% 0	1.64% 1	8.20% 5	6.56% 4	19.67% 12	59.02% 36	61	6.07
Host based security	3.28% 2	3.28% 2	1.64% 1	1.64% 1	11.48% 7	22.95% 14	55.74% 34	61	6.07
Infrastructure support	3.28% 2	1.64% 1	1.64% 1	3.28% 2	14.75% 9	26.23% 16	49.18% 30	61	6.00
Risk management plan	3.28% 2	0.00% 0	6.56% 4	4.92% 3	4.92% 3	29.51% 18	50.82% 31	61	6.00
Boundary security	3.28% 2	6.56% 4	0.00% 0	4.92% 3	6.56% 4	24.59% 15	54.10% 33	61	5.95
Service level agreement	3.28% 2	1.64% 1	6.56% 4	4.92% 3	6.56% 4	26.23% 16	50.82% 31	61	5.92
Security event incident manager	3.28% 2	3.28% 2	1.64% 1	8.20% 5	11.48% 7	19.67% 12	52.46% 32	61	5.90
Auditor	3.28% 2	1.64% 1	3.28% 2	4.92% 3	16.39% 10	24.59% 15	45.90% 28	61	5.87
Network Devices	4.92% 3	1.64% 1	3.28% 2	4.92% 3	11.48% 7	24.59% 15	49.18% 30	61	5.87
Storage	3.28% 2	0.00% 0	1.64% 1	6.56% 4	19.67% 12	31.15% 19	37.70% 23	61	5.84
Change management plan	4.92% 3	1.64% 1	1.64% 1	3.28% 2	18.03% 11	29.51% 18	40.98% 25	61	5.80
Public Key Infrastructure	3.28% 2	0.00% 0	6.56% 4	9.84% 6	8.20% 5	31.15% 19	40.98% 25	61	5.77
Asset management	3.28% 2	1.64% 1	6.56% 4	8.20% 5	8.20% 5	29.51% 18	42.62% 26	61	5.75
Service provider manager	3.28% 2	0.00% 0	3.28% 2	9.84% 6	18.03% 11	31.15% 19	34.43% 21	61	5.70
Training plan	4.92% 3	1.64% 1	0.00% 0	8.20% 5	24.59% 15	22.95% 14	37.70% 23	61	5.66
Physical security	4.92% 3	3.28% 2	6.56% 4	4.92% 3	14.75% 9	22.95% 14	42.62% 26	61	5.61
Endpoint devices	3.28% 2	3.28% 2	6.56% 4	6.56% 4	16.39% 10	27.87% 17	36.07% 22	61	5.57
Acquisition strategy	4.92% 3	1.64% 1	3.28% 2	8.20% 5	24.59% 15	26.23% 16	31.15% 19	61	5.49
Personnel security manager	4.92% 3	1.64% 1	4.92% 3	13.11% 8	16.39% 10	29.51% 18	29.51% 18	61	5.41
Facility	4.92% 3	4.92% 3	1.64% 1	8.20% 5	19.67% 12	36.07% 22	24.59% 15	61	5.39
Database	3.28% 2	3.28% 2	4.92% 3	14.75% 9	19.67% 12	21.31% 13	32.79% 20	61	5.39
Operating system	3.28% 2	3.28% 2	6.56% 4	16.39% 10	16.39% 10	22.95% 14	31.15% 19	61	5.33

The table above presented the results of one of two questions asked in the qualitative phase. This section of the study addresses the level of importance of the 28 assets identified. The results derived from the following question: “How important are the identified assets to the continuous monitoring mission of a cloud cybersecurity service provider CSSP?”

Out of the total 28 assets found in the qualitative phase of this study, the “Incident responder” asset was identified as the most important asset to the continuous monitoring mission of a cloud CSSP with a weighted average of 6.26. 39 out of the 61 participants consider it to be very important to the continuous monitoring mission of a cloud CSSP. Second place was a tie between the “Patch management” and “Continuous monitoring strategy” assets with a weighted average of 6.25. The “Continuous monitoring strategy” asset received the most responses (40) for being very important to the continuous monitoring mission of a CSSP.

The “Operating system” asset was identified as the least important asset to the continuous monitoring mission of a cloud CSSP with a weighted average of 5.33. 19 out of 61 participants consider it to be very important to the continuous monitoring mission of a cloud CSSP. The “Database” and “Facility” assets were tied as the second least important asset to the continuous monitoring mission of a cloud CSSP with a weighted average of 5.39. The “Facility” asset received the least responses (15) for being very important to the continuous monitoring mission of a cloud CSSP.

The response frequency of importance for each asset can be viewed in the below chart created using the results of a seven-point Likert-type scale questionnaire:

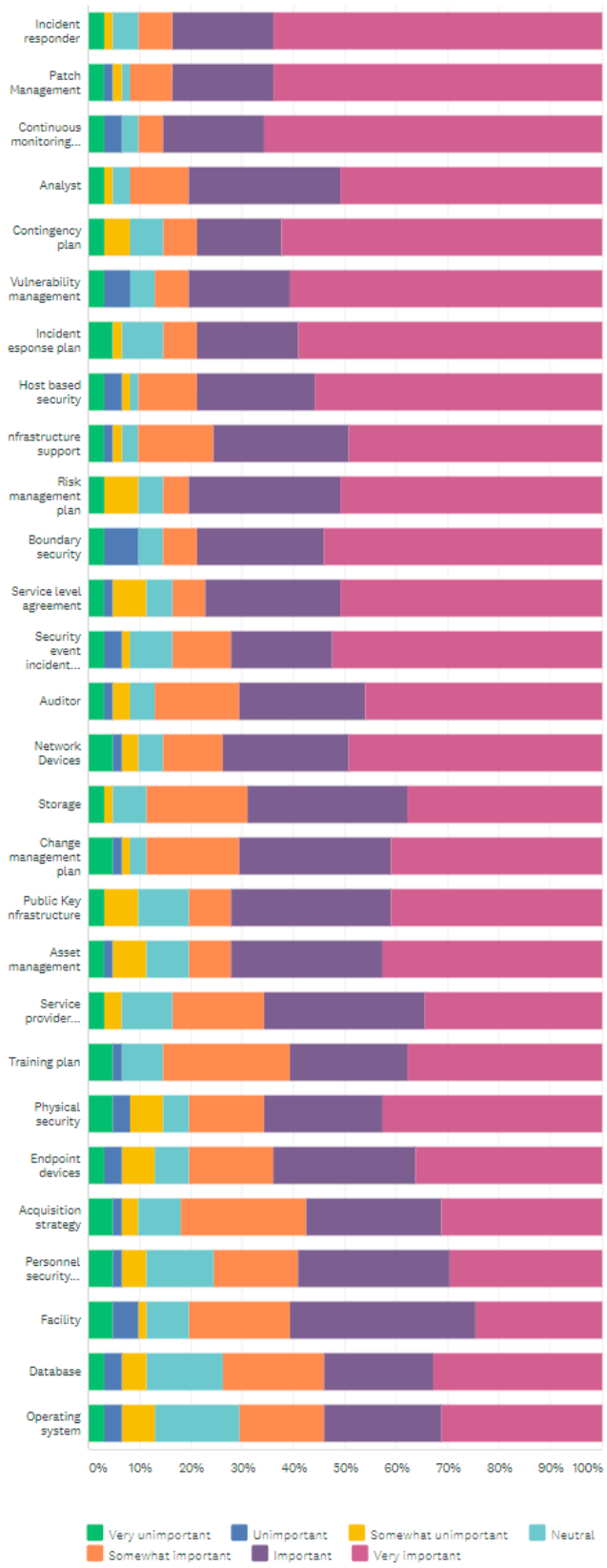

Figure 8. Asset importance frequency chart

Below is a chart identifying the weighted average for each asset:

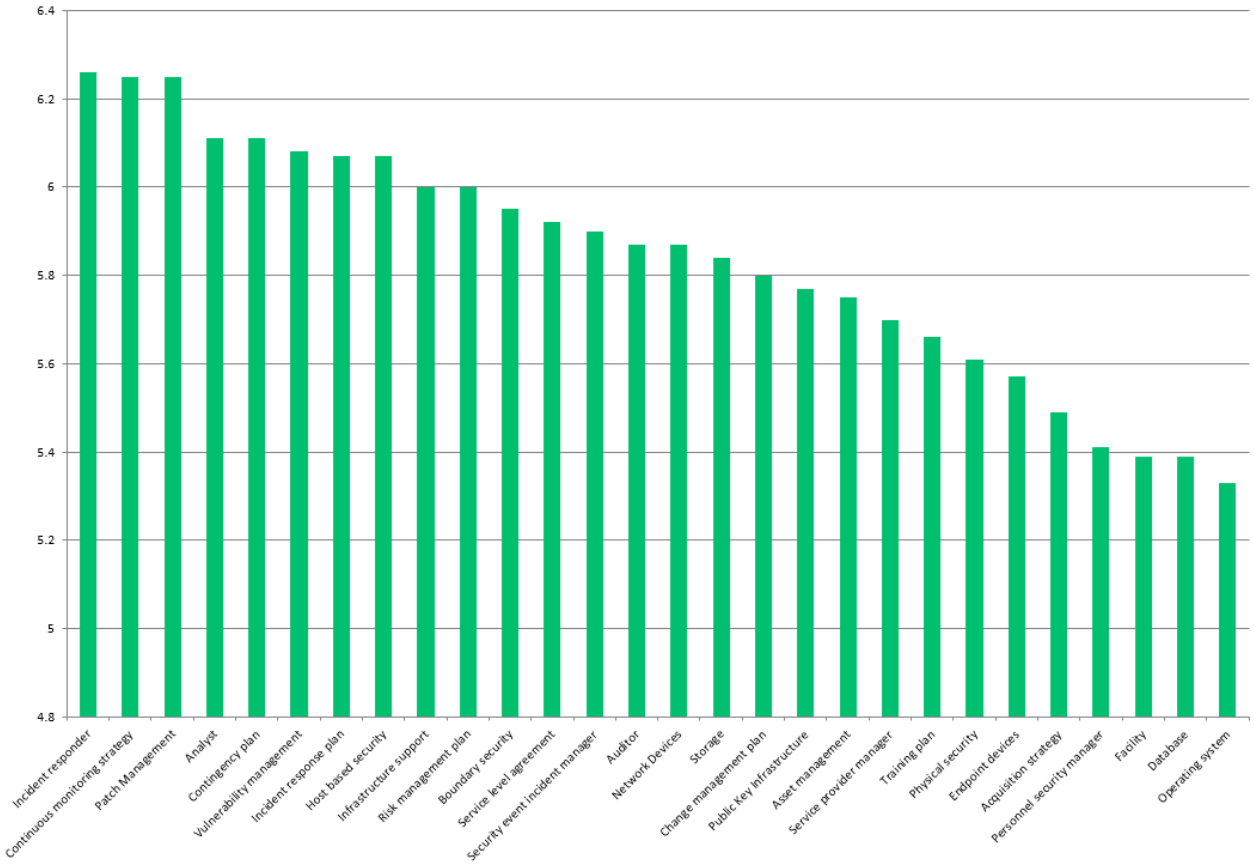

Figure 9. Asset importance weighted average chart

The table below presents the results of the second question asked in the qualitative phase. This section of the study determines the Estimated Time of Restoration (ETR) to the continuous monitoring mission of a cloud CSSP in the event one of the 16 identified critical assets should fail. The results derived from the following question: "If the identified critical asset fails, how will it impact the Estimated Time of Restoration (ETR) to the continuous monitoring mission of a cloud CSSP?"

Table 9. Asset Estimated Time of Restoration (ETR) table

	ETR < 1 HOUR	ETR> 1 HOUR < 8 HOURS	ETR> 8 HOURS < 24 HOURS	ETR> 24 HOURS < 48 HOURS	ETR> 48 HOURS < 72 HOURS	ETR> 72 HOURS < 96 HOURS	ETR> 96 HOURS	TOTAL	WEIGHTED AVERAGE
Facility	13.11% 8	22.95% 14	19.67% 12	18.03% 11	8.20% 5	4.92% 3	13.11% 8	61	3.52
Storage	14.75% 9	24.59% 15	24.59% 15	11.48% 7	6.56% 4	9.84% 6	8.20% 5	61	3.33
Incident response plan	19.67% 12	24.59% 15	19.67% 12	6.56% 4	9.84% 6	11.48% 7	8.20% 5	61	3.30
Public Key Infrastructure	16.39% 10	31.15% 19	11.48% 7	13.11% 8	11.48% 7	8.20% 5	8.20% 5	61	3.30
Infrastructure support	16.39% 10	32.79% 20	14.75% 9	11.48% 7	6.56% 4	6.56% 4	11.48% 7	61	3.25
Database	14.75% 9	27.87% 17	22.95% 14	11.48% 7	14.75% 9	1.64% 1	6.56% 4	61	3.15
Service provider manager	18.03% 11	24.59% 15	19.67% 12	14.75% 9	14.75% 9	4.92% 3	3.28% 2	61	3.11
Boundary security	19.67% 12	21.31% 13	24.59% 15	14.75% 9	9.84% 6	3.28% 2	6.56% 4	61	3.10
Endpoint devices	16.39% 10	27.87% 17	26.23% 16	9.84% 6	11.48% 7	1.64% 1	6.56% 4	61	3.03
Continuous monitoring strategy	24.59% 15	27.87% 17	13.11% 8	14.75% 9	1.64% 1	13.11% 8	4.92% 3	61	3.00
Network Devices	24.59% 15	24.59% 15	19.67% 12	11.48% 7	8.20% 5	3.28% 2	8.20% 5	61	2.97
Security event incident manager	22.95% 14	31.15% 19	16.39% 10	8.20% 5	8.20% 5	6.56% 4	6.56% 4	61	2.93
Incident responder	26.23% 16	27.87% 17	9.84% 6	16.39% 10	9.84% 6	3.28% 2	6.56% 4	61	2.92
Operating system	14.75% 9	34.43% 21	24.59% 15	9.84% 6	8.20% 5	3.28% 2	4.92% 3	61	2.92
Service level agreement	21.31% 13	27.87% 17	29.51% 18	6.56% 4	3.28% 2	4.92% 3	6.56% 4	61	2.84
Host based security	26.23% 16	29.51% 18	11.48% 7	14.75% 9	8.20% 5	4.92% 3	4.92% 3	61	2.84

The above table lists the 16 critical assets identified in the qualitative phase of this study. To be deemed a critical asset, the asset must be considered so important that if it fails the continuous monitoring mission of a cloud CSSP will fail. These critical assets are key terrain in Cyberspace (KT-C). KT-C is the physical and logical elements that an organization cannot effectively complete its mission without (Guion & Reith, 2017). The longer it takes to restore a failed asset, means the longer the mission has halted. To ensure a mission is successful, protecting assets with a high ETR should take priority over assets with a lower ETR.

Out of the total 16 assets found in the qualitative phase of this study, the "Facility" asset was identified as the asset with the highest ETR to the continuous monitoring mission of a cloud CSSP with a weighted average of 3.52. The "Facility" asset also received the most responses for having an ETR over 96 hours. 8 out of the 61 participants consider the "Facility" asset's ETR to be over 96 hours. The "Storage" asset had the second highest ETR to the continuous monitoring mission of a cloud CSSP with a weighted average of 3.33. The "Incident response plan" asset had the third highest ETR to the continuous monitoring mission of a cloud CSSP with a weighted average of 3.30.

The "Host-based security" and "Service level agreement" assets were tied for the lowest ETR to the continuous monitoring mission of a cloud CSSP with a weighted average of 2.84. The "Operating system" asset had the second lowest ETR to the continuous monitoring mission of a cloud CSSP with a weighted average of 2.92.

The response frequency of ETR for each asset can be viewed in the below chart created using the results of a seven-point Likert-type scale questionnaire:

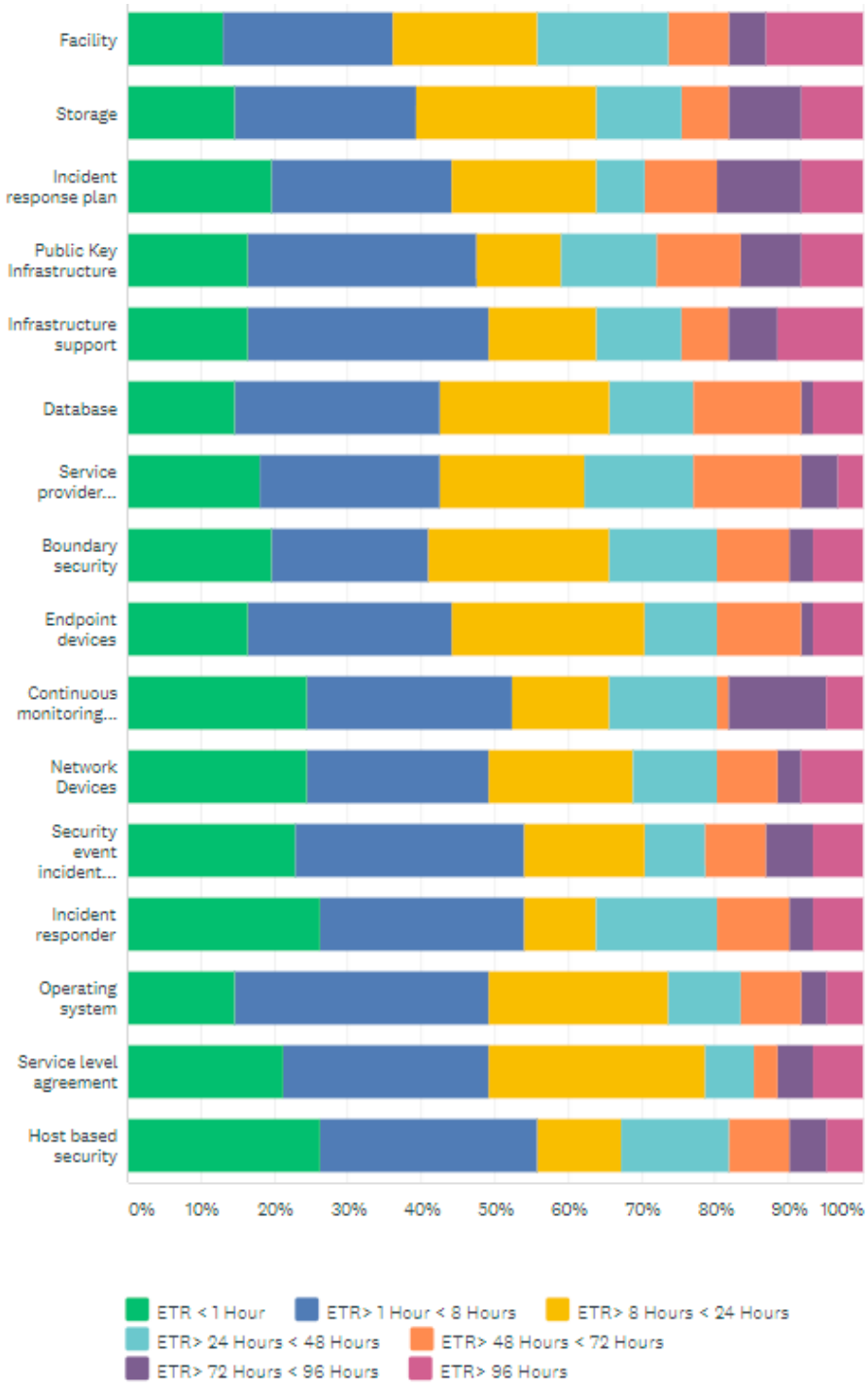

Figure 10. Asset ETR frequency chart

Below is a chart identifying the weighted average for each asset:

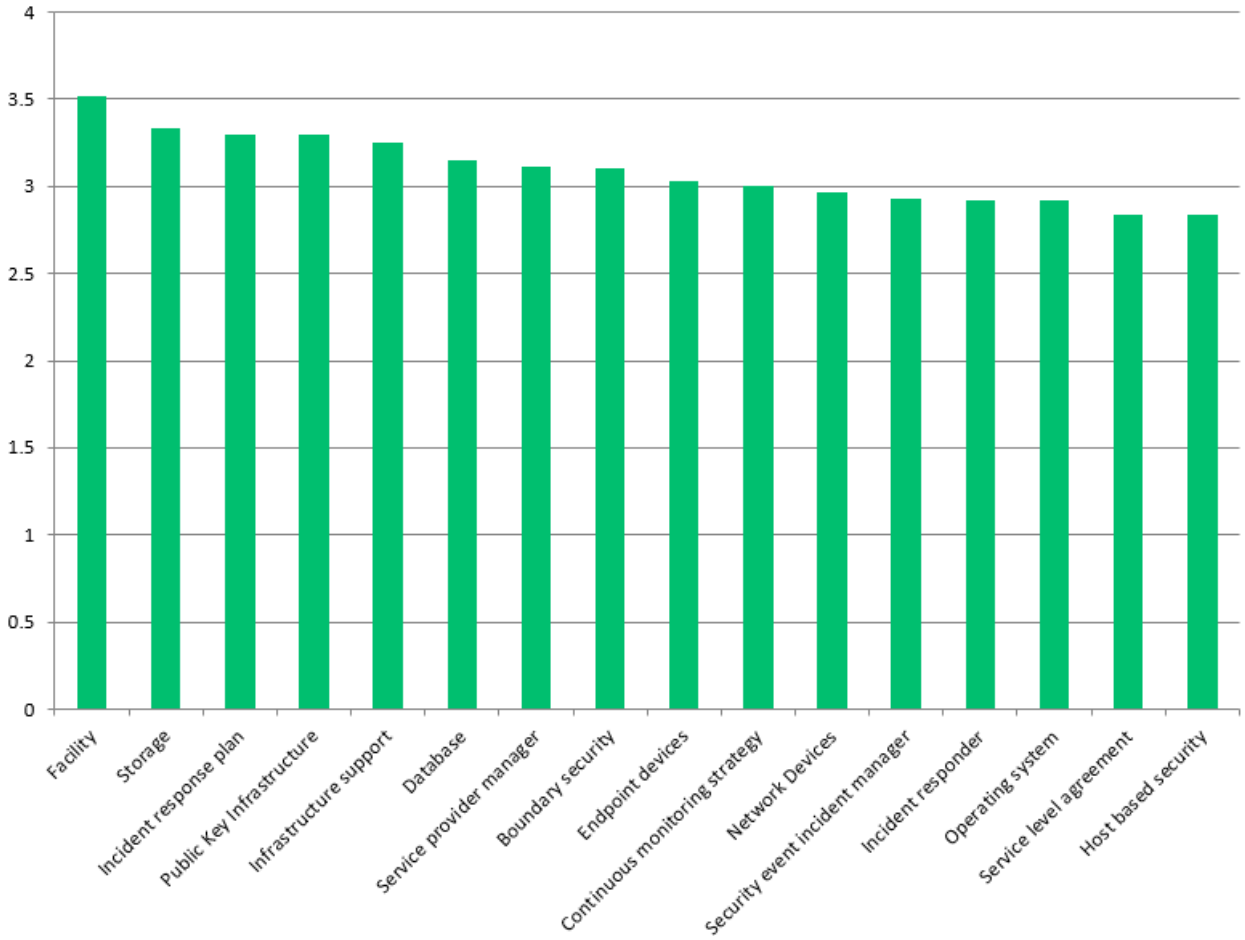

Figure 11. Asset ETR weighted average chart

To map the KT-C of the continuous monitoring mission of a cloud CSSP, the weighted average from the asset importance frequency table (Table 8) was summed with the weighted average from the asset Estimated time of restoration table (Table 9). Totaling the weighted average for both tables allowed for the ranking of all assets while ensuring only the critical assets are listed as KT-C.

Table 10. Terrain analysis table

Asset	Total	Weighted Average
Incident response plan	61	9.37
Continuous monitoring strategy	61	9.25
Infrastructure support	61	9.25
Incident responder	61	9.18
Storage	61	9.17
Public Key Infrastructure	61	9.07
Boundary security	61	9.05
Host based security	61	8.91
Facility	61	8.91
Network Devices	61	8.84
Security event incident manager	61	8.83
Service provider manager	61	8.81
Service level agreement	61	8.76
Endpoint devices	61	8.6
Database	61	8.54
Operating system	61	8.25
Patch Management	61	6.25
Analyst	61	6.11
Contingency plan	61	6.11
Vulnerability management	61	6.08
Risk management plan	61	6
Auditor	61	5.87
Change management plan	61	5.8
Asset management	61	5.75
Training plan	61	5.66
Physical security	61	5.61
Acquisition strategy	61	5.49
Personnel security manager	61	5.41
	Answered	61
	Skipped	0

The “Incident response plan” asset was found to have the highest weighted average (9.37) making it the most critical asset enabling the continuous monitoring mission of a cloud CSSP. The “Continuous monitoring strategy” and “Infrastructure support” assets were tied for the second-highest weighted average (9.25). Below, Figure 12 presents the terrain analysis of the assets that support the continuous monitoring mission of a cloud CSSP.

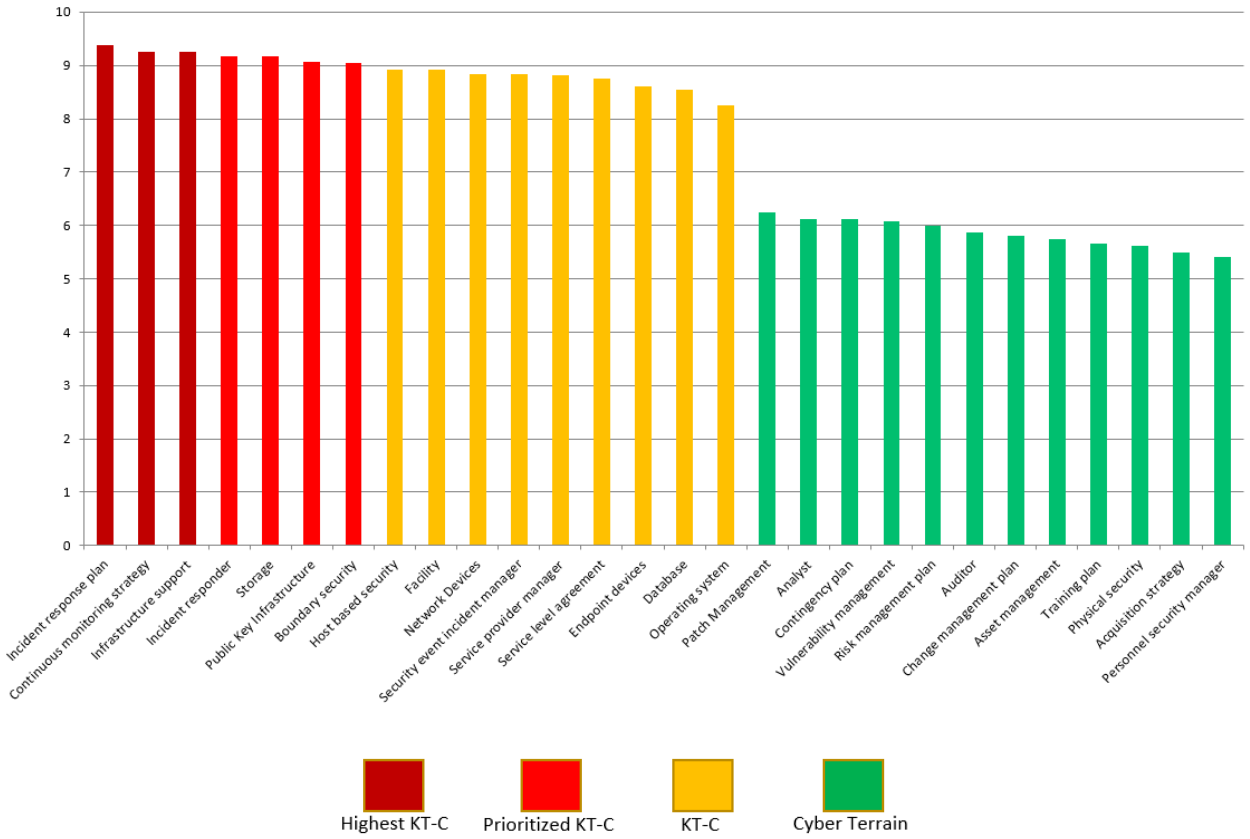

Figure 12. Terrain analysis chart

The top three assets were labeled the “Highest KT-C”. Assets with a weighted average of nine and above were labeled as “prioritized KT-C”. Assets with a weighted average of more than 8 and less than nine were labeled as “KT-C”. The remaining assets were listed as “Cyber terrain.” Phase one of this study determined the critical (the mission will fail without it) assets of a typical cloud CSSP and these assets were not identified to directly cause the continuous monitoring mission of a cloud CSSP to fail.

To visualize the KT-C enabling the continuous monitoring mission of cloud CSSP, a terrain map was created and presented in figure 13.

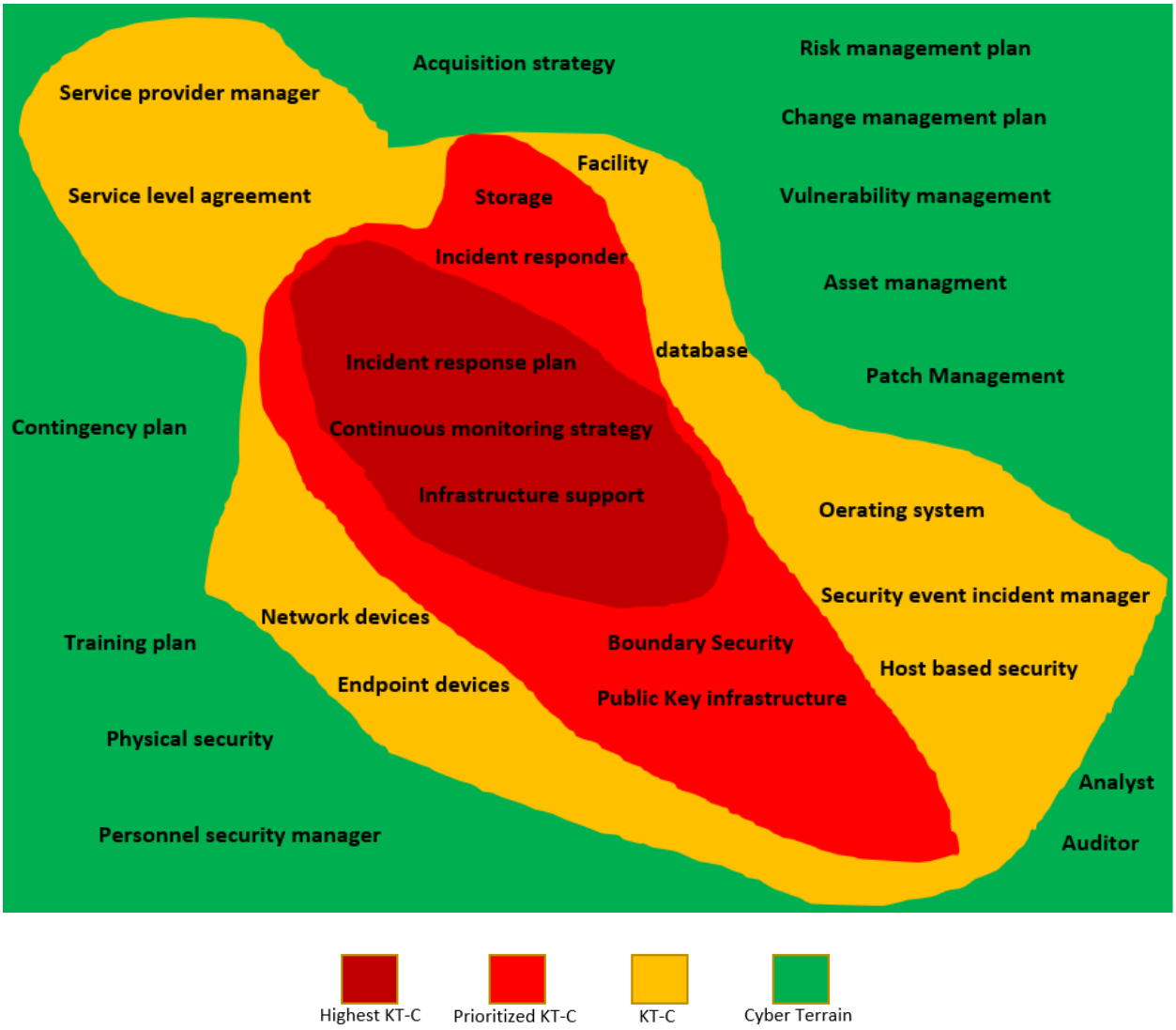

Figure 13. Terrain analysis map

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

The main objective of this study was to map the key terrain that supports the Continuous Monitoring (CM) mission of a cloud CSSP. Mapping of the key terrain was accomplished by doing a two-phase mix-method study.

The first phase was a qualitative questionnaire that resulted in a deeper understanding of the following areas:

- The mission of a typical cloud CSSP
- The assets (personnel, systems, devices, policies, facilities, etc.) of a typical cloud CSSP
- The critical (the mission will fail without it) assets of a typical cloud CSSP

The mission of a typical cloud CSSP was defined as the mission assurance of cloud information systems through the execution of cyber services as defined in the Service Level Agreement (SLA) made in conjunction with information system owners. 28 assets were identified as supporting the continuous monitoring mission of a cloud CSSP. Of those 28 assets, 16 were identified as being critical to the mission.

In the second phase, the 28 assets and 16 critical assets resulting from phase one of this study were used to create a seven-point Likert scale quantitative questionnaire. The first part of the questionnaire ranked the importance of the 28 assets (critical and non-critical) supporting a typical cloud CSSP and identified the followings assets as the top three:

- Incident responder
- Patch management

- Continuous monitoring strategy

The second part of the questionnaire focused on just the critical assets. To be considered a critical asset, the asset must be considered so important to a mission that if it fails the mission will fail. 16 critical assets were rank in accordance with their estimated time of recovery (ETR) from high to low and identified the following assets as the top three:

- Facility
- Storage
- Incident response plan

A terrain analysis for all 28 assets was accomplished by combining the weighted average of the asset importance frequency table (Table 8) with the weighted average from the asset Estimated time of restoration table (Table 9). The following three assets were identified as the highest KT-C:

- Incident response plan
- Continuous monitoring strategy
- Infrastructure support

Figure 12 presented a terrain analysis chart that ranked all the assets that supported the continuous monitoring mission of a cloud CSSP. Figure 13 presented a visualization of the terrain analysis conducted.

Implications

Results from this study have a number of implications concerning how key terrain in cyberspace is conducted in DoD. This research ascertains how to identify key terrain in a contextual manner. This approach allows for the mission mapping of cyber key terrain to be identified very early in an information systems life cycle. This means an information system's KT-C can be baked-in its accreditation package as opposed to being pasted-on after an information system is assessed and authorized in accordance with the DoD Risk Management Framework (RMF). The following process can be implemented in the DoD RMF process:

- Define and document the mission/mission criticality of an information system
- Lists all assets in a system data-call (the data-call should contain all the hardware and software for an information system)
- Identify all stakeholders [at a bare minimum the Information System Owner (ISO), Information System Security Officer (ISSO), and Information System Security Manager (ISSM) should be identified]
- Survey stakeholders to identify which assets are critical to the mission of the information system
- Rank all assets in accordance with their importance to the mission
- Identify and rank the estimated time for restoration (ETR) of critical assets
- Calculate the results to get the terrain analysis

Many of the activities in the above process are already accomplished in steps one and two of the DoD RMF process. These activities can be used to accomplish cyber key terrain mapping. Since most of the RMF activities are done in RMF steps one and two, the mapping can be started in step one and finished by step two of the DoD RMF. The terrain analysis should be updated

during continuous monitoring activities done in RMF step six. The following figure displays where the mission mapping process fits in the DoD RMF process:

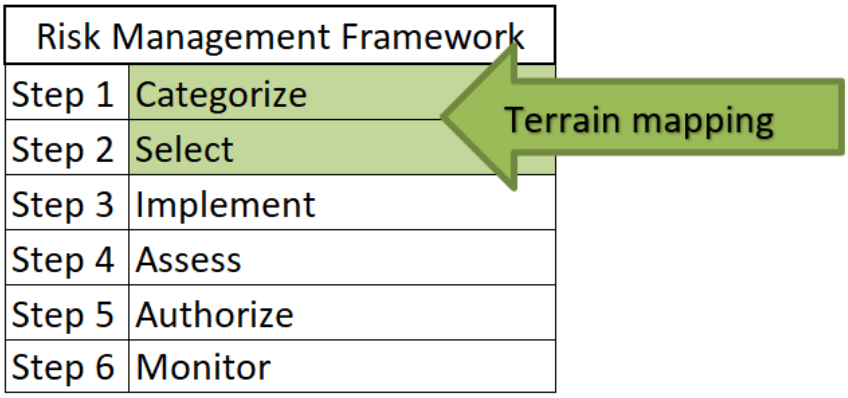

Figure 14. KT-C mission mapping in RMF

The following figure depicts multiple information system missions within an organization:

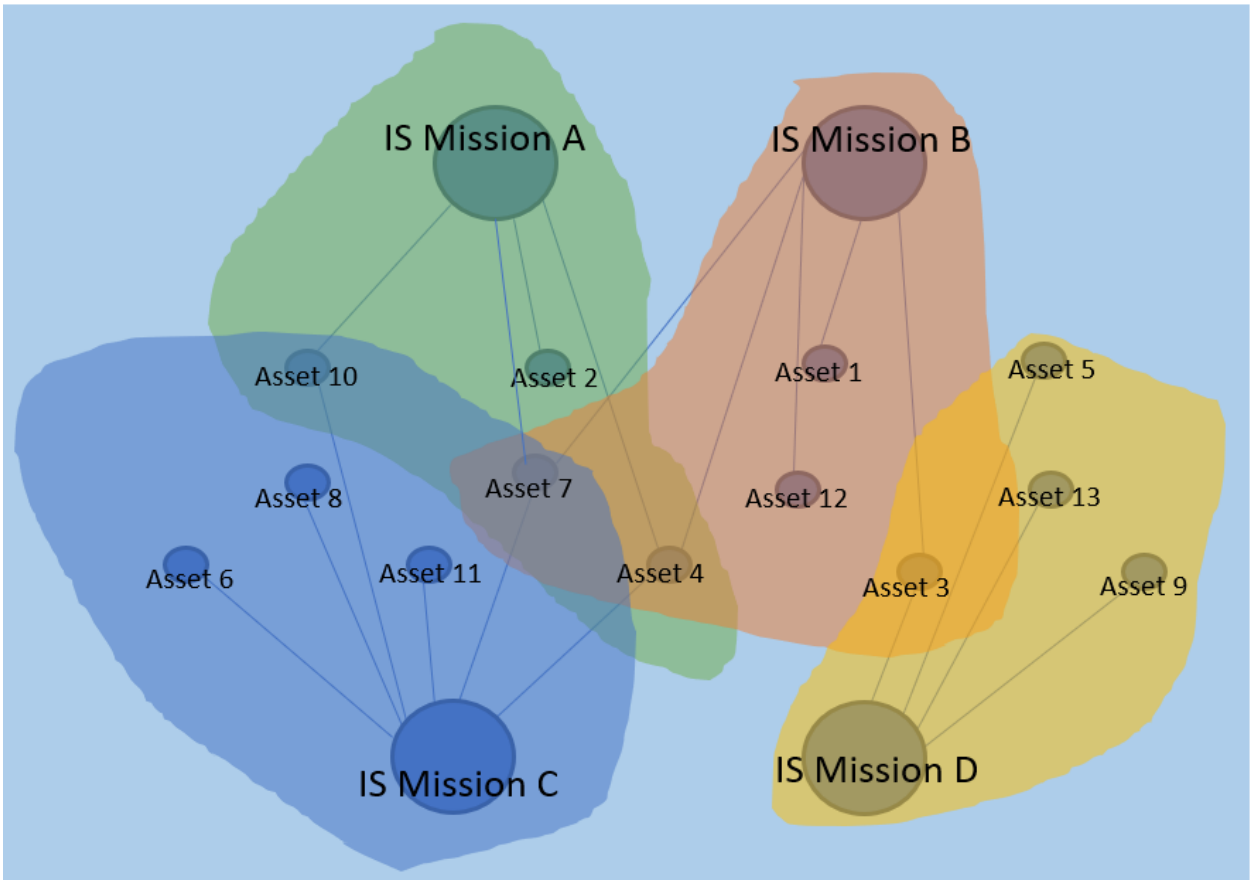

Figure 15. KT-C Big Picture

KT-C mission mapping can be combined for multiple information systems within an organization to get the big picture of an organization's KT-C. The identification of shared assets can be used to understand which assets impact the organization across multiple information system missions.

The results of this study enhanced the existing body of cybersecurity knowledge by providing the community with a better understanding of the key terrain that protects the mission of a cloud CSSP. This work provides an effective way to map KT-C through a contextual approach that focuses on a specific objective or mission within cyberspace. Each context can be used as modules that fit together to form a big picture. This study could be used to develop enhancements to the existing DoD RMF or similar frameworks to include KT-C mission mapping.

Recommendations

Results from this study prove that more research needs to be done to better understand KT-C and develop more effective ways to map key terrain in cyberspace. This study can be improved upon by increasing the data pool of participants. This study did not seek to understand why participants believed certain assets were critical (mission would fail without it) to the continuous monitoring mission of a CSSP. Future work can seek to better understand the critical asset selection phenomena and improve upon this work by creating a more effective model. This work was focused on DoD. Future work can use the techniques in this study to better understand how KT-C translates to the commercial/private sector.

Summary

This research sort to understand the key terrain that supports the continuous monitoring mission of a cloud CSSP. This study was guided by the following research questions:

1. What is the mission of a cloud CSSP?
    a. Answer: The mission assurance of cloud information systems through the execution of cyber services as defined in the Service Level Agreement (SLA) made in conjunction with information system owners.

2. What are the assets (personnel, systems, tools, devices, protocols, facilities, etc.) of a cloud CSSP?
    a. Answer: The following 28 assets were identified and split into four categories (People, Policy, Infrastructure, and Platform):

Table 11. Asset summary table

People	Policy	Infrastructure	Platform
Analyst	Continuous monitoring strategy	Storage	Host based security
Infrastructure support	Incident response plan	Boundary security	Operating system
Incident responder	Service level agreement	Network Devices	Database
Auditor	Contingency plan	Facility	Security event
Service provider manager	Training plan	End point devices	
Personnel security manager	Change management plan	Public Key Infrastructure	
	Acquisition strategy		
	Risk management plan		
	Physical security		
	Asset management		
	Vulnerability management		
	Patch Management		

3. What are the critical assets of a cloud CSSP?
    a. Answer: The following 16 critical assets were identified and split into four categories (People, Policy, Infrastructure, and Platform):

Table 12. Critical asset summary table

People	Policy	Infrastructure	Platform
Infrastructure support	Continuous monitoring strategy	Storage	Host based security
Incident responder	Incident response plan	Boundary security	Operating system
Service provider manager	Service level agreement	Network Devices	Database
		Facility	Security event
		End point devices	
		Public Key Infrastructure	

4. How do the critical assets rank in respect to the CM mission of a cloud CSSP?
    a. Answer: The weighted average of the estimated time of restoration each for asset was used to rank the critical assets. The following chart presented the results to this question:

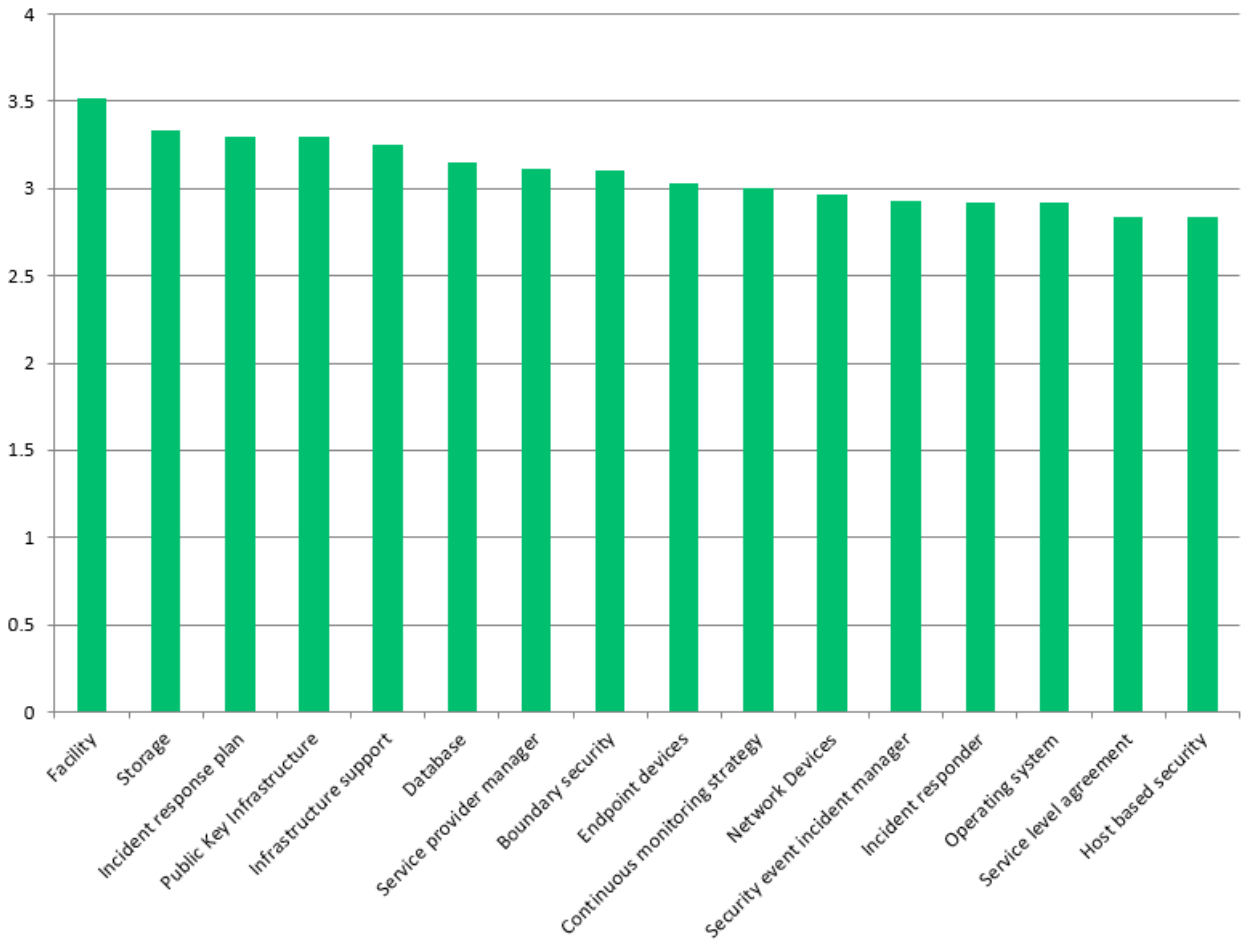

Figure 16. Critical asset ranking

5. What is the terrain analysis of the assets supporting the CM mission of a cloud CSSP?
    a. Answer: The terrain analysis for all 28 assets was accomplished by combining the weighted average identified for each asset's perceived importance with the weighted average identified for each asset's listed ETR. The following figure depicted the results:

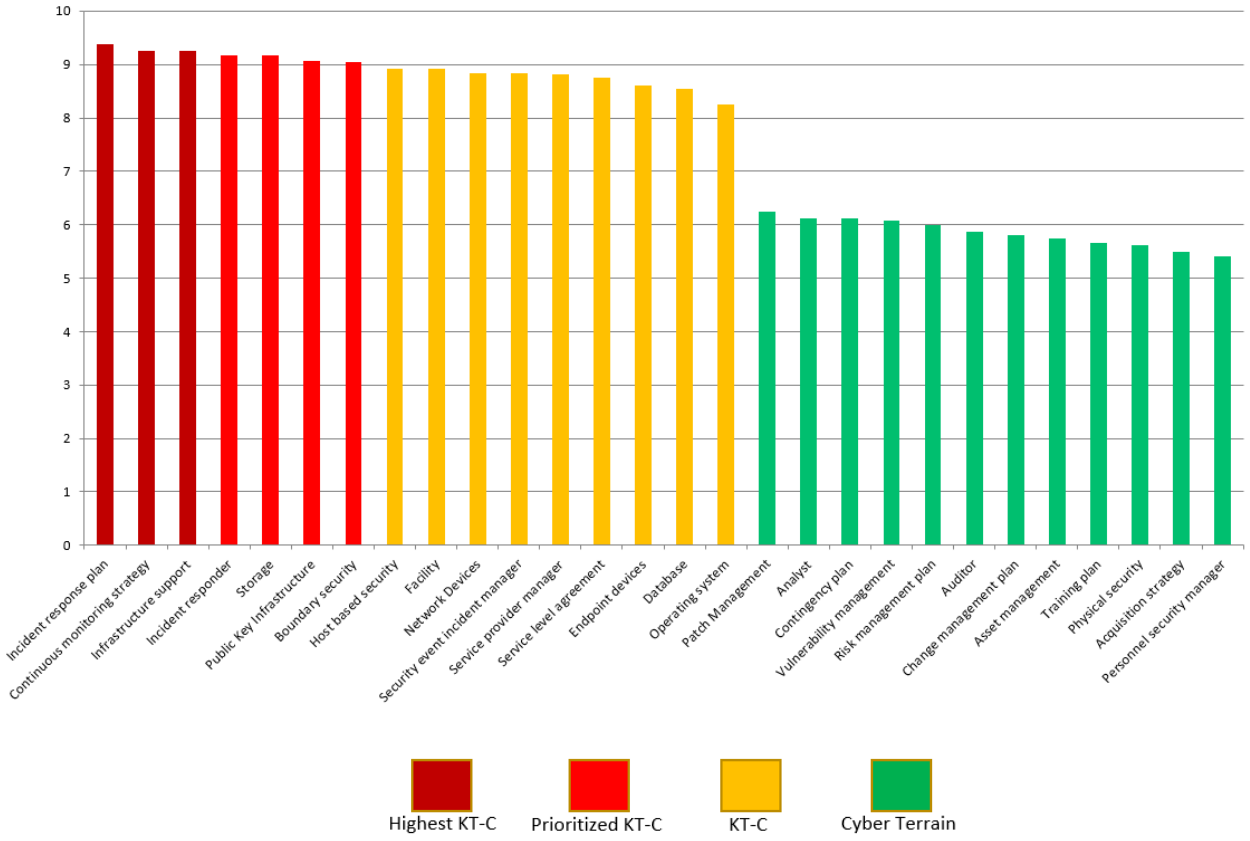

Figure 17. Terrain analysis chart

This research is significant to the cybersecurity community. Researchers are concerned with better understanding ways to effectively map KT-C (Applegate, Carpenter, & West, 2017; Conti, Cross, Nowatkowski & Raymand, 2014; Bodeau, Graubart, & Heinbockel, 2013). This research sort to better understand KT-C and provide an effective way to map KT-C. This study

ascertained how to identify key terrain in a contextual manner by mapping the key terrain that supports the continuous monitoring mission of a cloud CSSP. Pantin noted that a framework or tool to assist in the identification of key terrain in Cyberspace would prove beneficial and is an area of study that not many have attempted (2017). This research has developed a process to implement KT-C mapping in existing risk management frameworks like DoD's RMF.

Appendix A

Qualitative Survey Instrument

Cloud Cybersecurity Service Provider (CSSP): A cloud CSSP can offer a full spectrum of services to the Information System (IS) it supports. These services may include the detection of malicious activity, response to incidents, and sustainment of the mission. The success of an IS's mission is directly dependent upon the success of the cloud CSSP executing its mission. If the cloud CSSP fails its mission, the IS fails and impacts the success of the overall mission it supports. The Department of Defense (DoD) Chief Information Officer (CIO) (2016), has mandated the use of a DoD CSSP by all its networks and systems. As per DoD Instruction 8530.01 (2017), the measurement of the effectiveness of CSSP services is done by reviewing support agreements or contracts. Understanding the key terrain of a CSSP protecting a DoD IS is an additional way to foster confidence in CSSPs supporting DoD's mission. Applegate, Carpenter, and West, (2017) have defined key terrain as any locality, or area, the seizure or retention of will provide a marked advantage to either combatant.

Question 1

In your own words, please describe the continuous monitoring mission of a typical cloud cybersecurity service provider.

_____
_____
_____
_____
_____

Question 2

Please list the assets that support the continuous monitoring mission of a cloud cybersecurity service provider.

_____
_____
_____
_____
_____

Question 3

Of the assets listed in Question 2, list the ones you would consider critical to a cloud cybersecurity service provider's ability to continuously monitor. Continuous monitoring would fail without these assets.

_____
_____
_____
_____
_____

Appendix B

Expert Review Questionnaire

Thanks for participating in this review. Please provide your feedback regarding the research instrument attached. If required, please use additional paper.

1. Are the directions for completing the instrument clear and complete?

YES NO

If no, please explain

_____
_____
_____
_____
_____
_____

2. Do the questions appropriately address the construct?

YES NO

If no, please explain

_____
_____
_____
_____
_____
_____

3. Would you recommend revising anything?

YES NO

If yes, please explain

_____
_____
_____
_____
_____
_____

4. Would you recommend including any additional questions in this proposed instrument?

YES NO

If yes, please explain

_____
_____
_____
_____
_____
_____

GENERAL COMMENTS

_____
_____
_____
_____
_____
_____

Appendix C

Quantitative Survey Instrument

Mapping the Key Terrain that Supports the Continuous Monitoring Mission of a Cloud Cybersecurity Service Provider.

Mapping the Key Terrain that Supports the Continuous Monitoring Mission of a Cloud CSSP

Completing the survey indicates your voluntary participation in the study.

Use the answer keys provided to select the best response to each of the questions in this instrument. There are two sections to the instrument. Section A asks to rank the importance of assets that support the continuous monitoring mission of a cloud cybersecurity service provider (CSSP). Section B asks to identify the estimated time of restoration (ETR) of critical assets that support the continuous monitoring mission of a cloud CSSP.

* 1. **SECTION A**: How important are the identified assets to the continuous monitoring mission of a cloud CSSP?

	Very unimportant	Unimportant	Somewhat unimportant	Neutral	Somewhat important	Important	Very important
Analyst A person who analyzes data	○	○	○	○	○	○	○
Infrastructure support Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software	○	○	○	○	○	○	○
Incident responder Acts in response to realized threats	○	○	○	○	○	○	○
Auditor Determines the effectiveness of systems and their related security components (e.g. procedures)	○	○	○	○	○	○	○
Service provider manager The person responsible for controlling the activities associated with a service provider	○	○	○	○	○	○	○
Personnel security manager Manages the daily activities a personnel security program	○	○	○	○	○	○	○
Continuous monitoring strategy How a system conducts continuous assessments, reporting, and authorization of information systems to monitor security risks	○	○	○	○	○	○	○

Incident response plan An incident response plan is a set of instructions to help IT staff detect, respond to, and recover from network security incidents	○	○	○	○	○	○	○
Service level agreement An agreement between client and provider that outlines the services that will be provided	○	○	○	○	○	○	○
Contingency plan A contingency plan is a plan to recover from a risk should it occur	○	○	○	○	○	○	○
Training plan Guides the planning and delivery of instruction in the form of on the job training and certification requirements	○	○	○	○	○	○	○
Change management plan The process for dealing with changes within the environment	○	○	○	○	○	○	○
Acquisition strategy Describes the acquisition approach that Program Management will follow to manage program risks and meet program objectives	○	○	○	○	○	○	○
Risk management plan A plan on the identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks	○	○	○	○	○	○	○
Physical security Physical/electronic measures designed to monitor people, objects, and control access to property and information	○	○	○	○	○	○	○
Asset management Monitors and maintains things of value	○	○	○	○	○	○	○
Vulnerability management A process to ensure that systems are safe from cyber threats	○	○	○	○	○	○	○

Patch Management A process to update systems to remediate and mitigate vulnerabilities and issues	○	○	○	○	○	○	○
Storage Systems used to store information	○	○	○	○	○	○	○
Boundary security The monitoring and control of communications at the external boundary of an information system to detect and prevent malicious and other unauthorized communication	○	○	○	○	○	○	○
Network Devices Routers, switches, etc.	○	○	○	○	○	○	○
Facility The physical location where the cloud CSSP resides	○	○	○	○	○	○	○
Endpoint devices Computers, monitors, end-user devices, etc.	○	○	○	○	○	○	○
Public Key Infrastructure A system for the creation, storage, and distribution of digital certificate	○	○	○	○	○	○	○
Host based security Anti-virus software, host intrusion detection/prevention, vulnerability scanning software, encryption of data at rest, audit logging	○	○	○	○	○	○	○
Operating system Windows, Linux, etc.	○	○	○	○	○	○	○
Database Oracle, SQL, etc.	○	○	○	○	○	○	○
Security event incident manager Software used for identifying, monitoring, recording and analyzing security events or incidents within a real-time IT environment	○	○	○	○	○	○	○

* 2. **SECTION B**: If the identified critical asset fails, how will it impact the **Estimated Time of Restoration (ETR)** to the continuous monitoring mission of a cloud CSSP?

	ETR < 1 Hour	ETR> 1 Hour < 8 Hours	ETR> 8 Hours < 24 Hours	ETR> 24 Hours < 48 Hours	ETR> 48 Hours < 72 Hours	ETR> 72 Hours < 96 Hours	ETR> 96 Hours
Infrastructure support Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software	○	○	○	○	○	○	○
Incident responder Acts in response to realized threats	○	○	○	○	○	○	○
Service provider manager The person responsible for controlling the activities associated with a service provider	○	○	○	○	○	○	○
Continuous monitoring strategy How a system conducts continuous assessments, reporting, and authorization of information systems to monitor security risks	○	○	○	○	○	○	○
Incident response plan An incident response plan is a set of instructions to help IT staff detect, respond to, and recover from network security incidents	○	○	○	○	○	○	○
Service level agreement An agreement between client and provider that outlines the services that will be provided	○	○	○	○	○	○	○

Storage Systems used to store information	○	○	○	○	○	○	○
Boundary security The monitoring and control of communications at the external boundary of an information system to detect and prevent malicious and other unauthorized communication	○	○	○	○	○	○	○
Network Devices Routers, switches, etc.	○	○	○	○	○	○	○
Facility The physical location where the cloud CSSP resides	○	○	○	○	○	○	○
Endpoint devices Computers, monitors, end-user devices, etc.	○	○	○	○	○	○	○
Public Key Infrastructure A system for the creation, storage, and distribution of digital certificate	○	○	○	○	○	○	○
Host based security Anti-virus software, host intrusion detection/prevention, vulnerability scanning software, encryption of data at rest, audit logging	○	○	○	○	○	○	○
Operating system Windows, Linux, etc.	○	○	○	○	○	○	○
Database Oracle, SQL, etc.	○	○	○	○	○	○	○
Security event incident manager Software used for identifying, monitoring, recording and analyzing security events or incidents within a real-time IT environment	○	○	○	○	○	○	○

Appendix D

Participant Letter for Anonymous Surveys

Participant Letter for Anonymous Surveys
NSU Consent to be in a Research Study Entitled
Protecting the Protector: Mapping the Key Terrain that Supports the Continuous Monitoring Mission of a Cloud Cybersecurity Service Provider

Who is doing this research study?

The person doing this study is Chris Bush with the College of Engineering and Computing. He will be helped by Dr. Trudy Abramson.

Why are you asking me to be in this research study?

You are being asked to take part in this research study because you have been identified as an expert in supporting the mission of a cybersecurity service provider.

Why is this research being done?

The purpose of this study is to find out an effective way to map Key Terrain in Cyberspace (KT-C) through a contextual approach that focuses on a specific objective or mission within cyberspace. Each context can be used as modules that fit together to form the big picture. This research is focused on the continuous monitoring mission of a cloud cybersecurity service provider.

What will I be doing if I agree to be in this research study?

You will be taking a one-time, anonymous survey. The survey will take approximately 10 – 15 minutes to complete.

Are there possible risks and discomforts to me?

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

What happens if I do not want to be in this research study?

You can decide not to participate in this research, and it will not be held against you. You can exit the survey at any time.

Will it cost me anything? Will I get paid for being in the study?

There is no cost for participation in this study. Participation is voluntary, and no payment will be provided.

How will you keep my information private?

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. This research will not collect any personal identifiable information (PII) associated with any participant. PII is not significant and has no bearing on the findings of this research. Therefore, if the data has a compromise of confidentiality, the participants will be assured that their anonymity is protected. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any granting agencies (if applicable). All confidential data will be kept securely offline in a Federal Information Processing Standards (FIPS) 140 approved encrypted external HD. All data will be kept for 36 months from the end of the study and destroyed after that time by wiping the drive with BleachBit.

Who can I talk to about the study?

If you have questions, you can contact Chris Bush at 757-570-7766 and Dr. Trudy Abramson at (954) 262-207.

If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll-free at 1-866-499-0790 or email at IRB@nova.edu.

Do you understand and do you want to be in the study?

If you have read the above information and voluntarily wish to participate in this research study, please https://www.surveymonkey.com/r/DQGMVM6.

NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Chris Bush**

From: **Ling Wang, Ph.D.,**
Center Representative, Institutional Review Board

Date: **January 16, 2019**

Re: **IRB #: 2019-26; Title, "Protecting the Protector: Mapping the Key Terrain that Supports the Continuous Monitoring Mission of a Cybersecurity Service Provider"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Gertrude Abramson, Ed.D.
Ling Wang, Ph.D.

References

Abdulraza, N., & Zakari, R. Y. (2016). Computer security: a literature review and classification. *International Journal of Computer Science and Control Engineering.* Vol. 4, No. 2, pp. 6-13.

Applegate, S. D., Carpenter, C., & West, D. C. (2017). Searching for digital hilltops: A doctrinal approach to identifying key terrain in cyberspace. *Joint Force Quarterly* 84.

Bambauer, D. (2010, July). The enigma of Internet freedom. *Ejournalusa*. http://www.america.gov/st/democracyhr-english/2010/July/20100727141139enelrahc0.947201.html

Barlow, J. P. (1996). Declaration of independence in cyberspace. http://homes.eff.org/~barlow/Declaration-Final.html

Bodeau, D., Graubart, R., & Heinbockel, W. (2013). Mapping the cyber terrain: Enabling cyber defensibility claims and hypotheses to be stated and evaluated with greater rigor and utility. *MITRE Technical Report* MTR130433.

Booth, H., Feldman, L., McBride, T., Mell, P., Ouyang, A., Ragland, Z., & Waltermire, D. (2012). CAESARS framework extension: An enterprise continuous monitoring technical reference model. *NIST interagency report* 7756 (second draft).

Chawla, N., Dempsey, K., Johnson, A., Johnson, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. (2011). Information security continuous monitoring (ISCM) for federal information systems and organizations. *NIST special publication* 800-137 revision 1.

Collins, J. M. (1998). Military geography for professionals and the public. *An AUSA Institute of Land Warfare book*. Washington D.C.

Committee on National Security Systems. (2015). Committee on National Security Systems (CNSS) Glossary. *CNSS Instruction* No. 4009.

CompTIA. (2016). International trends in cybersecurity. *Research – premier content. CompTIA, Inc.* https://www.comptia.org/resources/international-trends-in-cybersecurity

Conti, G., Cross, T., & Nowatkowski, M., Raymond, D. (2014). Key terrain in cyberspace: seeking the high ground. *Proceedings of the 6th International Conference on Cyber Conflict* pp. 287 - 300. NATO CCD COE Publications.

Creswell, J. (2013). Qualitative Inquiry and Research Design: Choosing Among Five Approaches (Kindle Locations 1027-1030). SAGE Publications. Kindle Edition.

Creswell, J. (2003). Research design: Qualitative, quantitative, and mixed methods approaches (2nd ed.). Thousand Oaks, CA: Sage.

Crovitz, L. G. (2011, August 15). Techno-utopians are mugged by reality: Shutting down social media to prevent violence does not violate free speech. *Wall Street Journal* (2011, August 15).

Department of Homeland Security. (2018). Cybersecurity strategy. *Department of Homeland Security publications.* https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

Department of Homeland Security. (2016). Grizzly steppe – Russian malicious cyber activity. *NCCIC Joint analysis report.* Reference Number: JAR-16-20296.

Department of Defense. (2003). Computer Network Defense (CND) service provider certification and accreditation program. *DoD Instruction* O-8530.1-M.

Department of Defense. (2017). Cloud computing security requirements guide (SRG). *Defense Information Systems Agency*. Version 1, Release 3.

Department of Defense. (2014). Cybersecurity. *DoD Instruction* 8500.1.

Department of Defense. (2016). Cybersecurity activities support to DoD information network operations. *DoD Instruction* 8530.1.

Department of Defense. (2014). DoD Chief Information Officer, updated guidance on the acquisition and use of commercial cloud computing services. *DoD CIO*. http://iase.disa.mil/Documents/commercial_cloud_computing_services.pdf

Department of Defense. (2015). The department of defense cybersecurity strategy. *DoD strategy.* Washington, DC. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Department of Defense. (2015). Cybersecurity discipline implementation plan. DoD Instruction. DoD CIO.

Department of Defense. (2013). Cyberspace operations. *Joint Publication 3-12*. Washington, DC. http://www.dtic.mil/doctrine/new pubs/jp1 02.pdf

Dodge, M., & Kitchin, R. (2003). Mapping cyberspace. *London: Routledge.*

Eisenmann, C., Gullestrup, P., Nolan, R., & Stephenson, P. (2009). When Hackers Turn to Blackmail. *Harvard Business Review*, 87(10), 39-48. Retrieved from Business Source Complete database.

Fink, A. (2003). The Survey Kit, 2nd ed. Thousand Oaks, CA: Sage.

Federal Risk Management Authorization Program. (2011). Security authorization of information systems in cloud computing environments. *FedRAMP policy memorandum.*

Finstad, K. (2010). Response interpolation and scale sensitivity: Evidence against 5-point scales. *Journal of Usability Studies, 5*(3), 104-110.

Bougie, R., & Sekaran, U. (2016). Research Methods for Business: A Skill-Building Approach (Kindle Location 11188). Wiley. Kindle Edition.

Fowler Jr, F. J. (2013). Survey research methods. *Sage publications*.

Gabel, Detlev., Liard, B., & Orzechowkis, D. (2015). Why cyber security is important. *White & Case LLP*.

Galliers, R. D. (1992). Choosing information systems research approaches. *Information Systems Research: Issues, Methods, and Practical Guidelines*, R. D. Galliers (ed.), Oxford, England: Blackwell Scientific Publications, pp. 144-162.

Geller, E., Overly, S. (2020). White house drafts executive order that could restrict global cloud computing companies. *Politico.* Retrieved from https://www.politico.com/news/2020/12/04/trump-cloud-computing-executive-order-442918

Grau, L., Kipp, J., Prinslow, K., & Smith, D. (2006). The human terrain system: a CORDS for the 21st Century. *Military Review*. pp. 8-15.

Gondree, M., Leyba, N., Parker, T., Price, P., Staples, Z. (2017). Asset criticality in mission reconfigurable cyber systems and its contribution to key cyber terrain. *Hawaii International Conference on System Sciences (HICSS).* Retrieved from http://hdl.handle.net/10125/41893

Guion, J., Reith, M. (2017). Cyber terrain mission mapping: tools and methodologies. *International Conference on Cyber Conflict (CyCon U.S.)*

Jakobson, G. (2013). Mission-centricity in cyber security: architecting cyber attack resilient Missions. *Proceedings of the 5th International Conference on Cyber Conflict (CyCon).* IEEE pp. 1–18.

Joint Task Force Transformation Initiative Interagency Working Group. (2013). Security and privacy controls for federal information systems and organizations. *NIST special publication* 800-53 revision 4.

Kramer, F. D. (2009). From Cyberspace to Cyberpower: Defining the Problem. In Kramer F., Starr S., & Wentz L. (Eds.), *Cyberpower and National Security* (pp. 24-42). University of Nebraska Press. Retrieved from http://www.jstor.org/stable/j.ctt1djmhj1.7

Kryger, M., & Lillemose, J. (2015). The (re)invention of cyberspace. *Kunstkritikk.* http://www.kunstkritikk.dk/kommentar/the-reinvention-of-cyberspace/.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In Kramer F., Starr S., & Wentz L. (Eds.), *Cyberpower and National Security* (pp. 24-42). University of Nebraska Press. Retrieved from http://www.jstor.org/stable/j.ctt1djmhj1.7

Lewis, J. A. (2013). The Economic impact of cybercrime and cyber espionage. *Center for Strategic and International Studies (CSIS).*

Nardi, P. (2003). Doing survey research: A guide to quantitative methods. Boston, MA: Pearson.

National Institute of Standards and Technology. (2004). Federal information processing standards publication (FIPS-199) standard for security categorization of federal information and information systems. *FIPS PUB 199.*

National Institute of Standards and Technology. (2011). Guidelines on security and privacy in public cloud computing, dated December 2011. *NIST Special Publication 144*. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. *NIST* version 1.1. https://www.nist.gov/cyberframework

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity. *NIST* version 1.0.

National Institute of Standards and Technology. (2018) NIST releases version 1.1 of its popular cybersecurity framework. *NIST*. https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

National Institute of Standards and Technology. (2011). The NIST definition of cloud computing. *NIST Special Publication 800-145*. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

National Institute of Standards and Technology. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication 800-181*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf?trackDocs=NIST.SP.800-181.pdf

National Institute of Standards and Technology. (2020). Workforce framework for cybersecurity (NICE Framework). *NIST Special Publication 800-181 revision 1*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Niles, R. (2018). Survey Sample Sizes and Margin of Error. Retrieved on 11 November 2018 from https://www.robertniles.com/stats/margin.shtml

Paganini, P. (2014). NATO officially recognizes cyberspace a warfare domain. *Security Affairs – NATO, Information Warfare.*

Pantin, N. T. (2017). Key terrain: application to the layers of cyberspace. *Naval Postgraduate School*, Monterey, California. http://hdl.handle.net/10945/53030.

Pathirana, P. (2017). Hiring a competent cybersecurity service provider. *The Associated Newspapers of Ceylon Ltd.*

Pingel, J. T. (2003). Key defensive terrain in cyberspace: a geographic perspective. *Department of Geography*, University of California Santa Barbara, CA 93106-4060, USA

President of the United States Executive Office. (2017). Presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure. *Whitehouse.gov*. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

President of the United States Executive Office. (2009). The comprehensive national cybersecurity initiative. *Whitehouse.gov*. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative/.

Shank, G. (2006). Six alternatives to mixed methods in qualitative research. *Qualitative Research in Psychology, 3*(4), 346-356.

SurveyMonkey Inc. (2020). www.surveymonkey.com San Mateo, California, USA

Thil, S. (2009). March 17, 1948: William Gibson, father of cyberspace. *WIRED.* *https://www.wired.com/2009/03/march-17-1948-william-gibson-father-of-cyberspace-2/*

United States. Dept. of the Army. (1986). Department of the army field manual. *Headquarters Dept. of the Army.* Washington DC.

Whittaker, J. (2004). The cyberspace handbook. *London: Routledge.*

Wynne, M. W. (2006). Cyberspace as a domain in which the Air Force flies and fights. *C4ISR Integration Conference.* Crystal City, VA.