Intelligence Agencies' move to the Cloud

Challenges and Opportunities

Karin Säberg

Department of Computer and Systems Sciences

Degree project 30 HE credits
Computer and Systems Sciences
Degree project at the master level
Spring term 2023
Supervisor: Gazmend Huskaj
Swedish title: Underrättelsetjänsters flytt till Molnet – Utmaningar och Möjligheter

Stockholm University

Abstract

Information and data are generated at an unprecedented rate. Previously, intelligence agencies had multiple sources to collect information from and the information was limited. This has changed and information is being created by humans and machines at a pace incomparable to only a few years ago, and intelligence agencies have to gather, process and share this information in a timely, accurate, and actionable manner. The cloud could provide this capability if implemented and used correctly, however, intelligence agencies are keen on information security, making them face challenges if a cloud computing solution were to be adopted. To find some of the challenges and opportunities two research questions of *what challenges do intelligence agencies face when adopting cloud solutions* and *what opportunities does a cloud solution bring to an intelligence agency?* were formulated and answered. A case study research strategy was chosen and conducted, and by using semi-interviews with experts in the field data was called and thematically analysed. The data analysis resulted in 14 main themes and 13 sub-themes. These themes showed that the main challenge is laws and regulations, and the main opportunities are the processing and analytical prowess and information sharing potential. The findings provide some new insights into the field of cloud computing adoption for intelligence agencies.

Keywords: intelligence, intelligence agency, cloud, cloud computing, information security

Synopsis

Background

There is little previous research regarding intelligence agencies and use of the cloud. Most sources on existing examples are news articles and research on cloud use and adoption in governments had to be consulted. One study concerning digital tools use in intelligence processes was heavily referenced but even it lacked insight into cloud computing. It belongs to the information/cyber security and cloud computing area of computer and system sciences.

Problem

Intelligence agencies need to gather, process, and analyse massive amounts of data and the cloud could provide the needed capability and tools for this. Due to the nature of intelligence agencies and the cloud there is likely to be resistance and challenges that need to be considered.

Research Question

Two research questions are posed to discover the challenges and opportunities faced by intelligence agencies.

- *What challenges do intelligence agencies face when adopting cloud solutions?*
- *What opportunities does a cloud solution bring to an intelligence agency*?

These questions will help discover what intelligence agencies have to do to consider cloud solutions as an answer to the problems they face.

Method

A case study research strategy was used. It allows for in-depth research about a specific case, in this case *intelligence agencies move to the cloud*, and to explore the complexities its context brings. Action research and surveys were disregarded as research strategies due to being unfit. Semi-structured interviews with five experts were conducted, three intelligence and two technical. The data was analysed using thematic analysis and resulted in 151 codes, sorted into 24 categories, and gathered into 14 main themes and 13 sub-themes.

Result

The result explains the 14 main themes and their identifying topics. The themes are presented using a mix of quotes from the experts and connecting with previous research. Laws and regulations were found to be the most pressing challenge, with the requirements on information security following closely after. The challenges were mostly dependent on intelligence agency capability and ability, with laws and regulations being outside their direct influence. Opportunities were found to be equally important as the challenges as the capability brought by a cloud are likely to be worth the risk a cloud solution would present.

Discussion

The study is limited to experts in Sweden and only five were interviewed. Due to lack of previous studies, the thesis is exploratory and explanatory, and very broad in topic with some depth. The results are mostly original and present new considerations. Intelligence communities, lawmakers, and researchers can all use the thesis for varying reasons. The societal implications are that the need for changes in laws is highlighted which may lead to higher cloud usage in government agencies.

Acknowledgement

I would like to thank my supervisor, Gazmend Huskaj, for his support during this thesis. He has been invaluable towards getting this research done, both by proposing a topic I would not have found, or considered, myself and his support during it by providing continuous encouragement and resources when I have been stuck. This research would have been impossible without him and the contacts he provided.

I would equally like to thank the experts who took the time to take part in this study and the discussions they provided during the interviews. They all provided me with valuable insight and additional knowledge about the intelligence process I would have missed out on otherwise. The expert who provided a reference to another expert I am extra grateful towards; thank you for introducing me and for said expert to agree as well.

My family has been a great support during this time, Mum especially; thank you for letting me call and discuss a topic you, as you have repeatedly told me, do not understand.

Additionally, I would like to thank my friend Raouf for providing valuable feedback and support, as well as my other friends for allowing me to share the ups and downs of this process.

I have had the honour and opportunity to discuss my research with a great deal of people who have all provided valuable insights and discussions, you are too many to name, but I thank you all.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Artificial intelligence – AI
Machine learning – ML
Central Intelligence Agency – CIA
Open-source intelligence – OSINT
United States of America – US
United Kingdom of Great Britain – UK
Säkerhetspolisen – SÄPO
Information technology – IT
Government Communications Headquarters – GCHQ
National Institute of Standards and Technology – NIST
North Atlantic Treaty Organization – NATO
European Union – EU
International Organization for Standardization – ISO
International Electrotechnical Commission – IEC
Cloud service provider – CSP
Service-as-a-Service – SaaS
Platform-as-a-Service – PaaS
Infrastructure-as-a-Service – IaaS

1 Introduction

The Information Age is in full swing and brings opportunities and challenges. As the name implies, it is an age of information, and enormous amounts of data are being generated daily; every minute 66 thousand photos are shared on Instagram, over 347 thousand tweets are created, 500 hours of video are uploaded to YouTube, and 5.9 million Google searches are done (Domo, 2022). This is but a fraction of the content, and data, generated by users on the Internet. They interact with each other and organisations continuously through social media, online chat solutions, or online shopping; the Internet provides solutions and consequently generates data. This data and information could provide valuable insights if analysed.

Intelligence agencies have used multiple intelligence-gathering methods over the years. These can be grouped into five categories: Human Intelligence, Signals Intelligence, Imagery Intelligence, Measurement and Signatures Intelligence, and Open-Source Intelligence (OSINT) (FBI, n.d.; MI5, n.d.; Säkerhetspolisen [SÄPO], 2022). While MI5 (United Kingdom of Great Britain's (UK) Secret Service) and SÄPO (Swedish Security Service) do not divide their intelligence collection as clearly as the United States of America (US) intelligence community does, their collection methods fit into the categories mentioned above. Of these, open-source intelligence is of interest, especially in today's highly digitalised world. The term open-source intelligence is relatively recent, having been coined in the late 80s by the US military (Schaurer & Störger, 2013) and concerns the collection of data from "publicly available information, as well as other unclassified information that has limited public distribution or access" (North Atlantic Treaty Organization [NATO], 2013). SÄPO exemplifies OSINT using the internet, newspapers, radio and tv (2022).

Considering OSINT, the internet and intelligence agencies need to discover, access, and share critical all-source multi-fused intelligence in a timely, accurate and actionable manner (Palfy, 2015; Schaurer & Störger, 2013); intelligence agencies are presented with two main issues. The "handling" (discovery, access, analysis, sharing) of the data and the security to ensure that the goals can be accomplished. To tackle these issues, the Central Intelligence Agency (CIA) decided to employ cloud solutions for all 17 of the United States intelligence agencies (Konkel, 2014). The deal was for Amazon Web Services (AWS) to provide this solution for ten years, and now a new deal has been completed, this time with AWS, Microsoft, Google, Oracle, and IBM (Konkel, 2020). Little is known about the specifics and requirements that supported the move to the cloud, both in 2014 and 2020, other than a statement from the associate deputy director at CIA's Digital Innovation Directorate, Sean Roche, where he states that "[…] the cloud on its weakest day is more secure than a client service solution" and that government organisations are desperately trying to upgrade legacy information technology (IT) systems (Corrigan, 2018).

With only two found examples of intelligence communities moving to the cloud, the US and UK, and at most some news articles on the topic, there is little previous research on the topic of moving an organisation with such high-security requirements while also needing to access and share the information to the cloud. As noted above, the abundance of data and OSINT mean that intelligence agencies need to adapt to the current age and, similarly to the CIA, consider moving to the cloud. However, this is not problem or challenge-free; information security needs to be considered regarding data access and control and the inherent nature of the cloud. The cloud is a collection of connected but distributed servers providing services to customers, and type can vary, but in practice it means that the customer cannot be sure where the physical hardware is located.

1.1 Problem and Aim

With little available research on moving an intelligence agency's data to the cloud knowledge about the topic is lacking. The US and UK intelligence communities have done it, but little is known about the decision process, security requirements and practical solutions. As such, there are issues with how to approach the security of the physical cloud solution and how to approach information security, as well as the potential resistance to moving to the cloud. To better face these issues and understand what intelligence agencies need to consider to adopt cloud solutions, research is needed into the challenges of moving an intelligence agency's data to the cloud. The aim of the study will be to discover challenges that intelligence agencies face when moving to the cloud to better provide them with tools to utilise available solutions that would benefit them in their work. However, using the cloud will likely bring opportunities and will also be explored.

1.2 Research Questions

The research questions this study aims to answer are:

- *What challenges do intelligence agencies face when adopting cloud solutions?*
- *What opportunities does a cloud solution bring to an intelligence agency*?

With the first aimed at discovering challenges and the second to find out what opportunities a cloud solution could bring.

1.3 Delimitations

The study will be limited in scope and practical application. Due to time and resource limits, the study will be purely theoretical, with no opportunity to be implemented or tested practically; due to secrecy and confidentiality reasons many practical solutions are also not viable to discover beyond what is already considered best practice. The study will also be limited to free and open-source tools and what tools Stockholm University provides its students. The study is further limited in using sources available in Swedish or English.

1.4 Thesis Outline

The study is structured as such; first, a literature review of previous research, starting with identifying literature on intelligence agencies and cloud solutions. The initial concepts are identified in Tables 1, 2 and 3. Chapter 3 provides a detailed look into the methodology used for the thesis. Following this is Chapter 4 with the results and analysis, and Chapter 5 discusses the findings and future studies.

The contribution of this study is that it provides better understanding of the challenges faced by intelligence agencies and their move to the cloud by using interviews with experts in the field.

2 Literature Review

To better understand what challenges moving classified data, information, and processes to the cloud (hereafter: move to the cloud) would present and what requirements an intelligence agency may have on a cloud solution, previous research will be consulted. First intelligence and intelligence agencies will be explained, followed by definitions of *the cloud* and *cloud computing*, and a discussion on the security challenges. Finally, previous research is considered and discussed. The concepts identified are then presented in Table 2 and Table 3.

2.1 Intelligence and Intelligence Agencies

Intelligence is defined slightly differently depending on the source (Bang, 2017, pp. 8–12; Bimfort, 1958; Kent, 1966, p. vii). However, Swedish, UK and US intelligence agencies define it as the collection and analysis of information to provide intelligence to decision and policymakers, often with the goal of protecting the country they operate for (Försvarsmakten, 2020; FRA, n.d.; Office of the Director of National Intelligence, n.d.-b; Secret Intelligence Service MI6, n.d.). When gathered by intelligence agencies, intelligence tends to involve foreign actors. Intelligence can be collected both within and outside the borders of a country.

NATO defines intelligence as “the product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers” (2022), being both more narrow and broader in definition compared to the above-mentioned intelligence agencies’ definitions.

Probst (2006) discusses the need to clearly communicate the findings to the decision-makers. Lahneman (2010) and Palfy (2015) further discuss the importance of turning information into usable intelligence.

By providing timely and accurate intelligence about threats to the country, actions can be taken to mitigate the risk and threats towards the state in question. However, as many intelligence communities in a country are made up of multiple agencies, there is also a need to share information between these agencies while ensuring that secrecy is upheld. The nature of intelligence communities is inherently closed and shrouded in secrecy, with little insight further complicating the issue.

2.2 The Cloud and its Uses

The terms cloud and related terms computer clouds and cloud computing are both easy and complex to define. At its most basic, it is a term that provides computer services over networks using distributed server solutions (Cloudflare, n.d.; IBM, n.d.-a; Marinescu, 2022, p. 1). However, it also covers complex issues such as different deployment models, management solutions and users (Butt et al., 2022; International Organization for Standardization/International Electrotechnical Commission [ISO/IEC], 2021; Jones, 2015; Mell & Grance, 2011), management covering both organisational management and policy management (e.g., risk and access management), while users are an integral part as they will be the ones using it. Even further, definitions of the *cloud* or *computer cloud* appear non-existent; only Microsoft Azure provides one for the *cloud*, while others prefer the term *cloud computing*.

Microsoft Azure provides an easy-to-understand description of the cloud:

> The definition for the cloud can seem murky, but essentially, it's a term used to describe a global network of servers, each with a unique function. The cloud is not a physical entity, but instead is a vast network of remote servers around the globe which are hooked together and meant to operate as a single ecosystem. These servers are designed to either store and manage data, run applications, or deliver content or a service such as streaming videos, web mail, office productivity software, or social media. Instead of accessing files and data from a local or personal computer, you are accessing them online from any Internet-capable device—the information will be available anywhere you go and anytime you need it. (Microsoft Azure, n.d.)

The National Institute of Standards and Technology (NIST) and ISO/IEC provide definitions for cloud computing. NIST's definition also notes that it is a cloud model and includes characteristics, service, and deployment models (Mell & Grance, 2011), thus being more specific in its definition and what is required for something to be considered "cloud computing". ISO/IEC's definition is slightly less specific than NIST's however, ISO/IEC differentiates between cloud computing and cloud service (ISO/IEC, 2021).

With the above definitions in mind, the cloud, or cloud computing, the phrases will be used interchangeably in this study, is a set of pooled resources that allow the users flexible access to these resources using network access, usually the internet. However, this model presents issues, especially with information security in mind. To handle some of these concerns, cloud service providers (CSP) cloud computing is traditionally offered using three different service models and four different deployment models, with newer service and deployment models existing. These services and models offer different solutions, security options and varying levels of control. An overview of the deployment and service models can be found below in Table 1.

Table 1

Overview of Cloud Deployment and Service Models

Deployment Model	**Description**
Community Cloud	Infrastructure and/or resources are shared by a collection of customers who share requirements, goals, policies, and relationships. It can be controlled by a member of the customers or a third party, or a combination of both.
Hybrid Cloud	A combination of any of the other deployment models but remain as unique identities.
Private Cloud	The cloud service is provided to and used by a single customer[a] who also controls the resources. It can be managed, owned, and operated by the organisation, a third party, or a combination. It can be situated on or off-premises.
Public Cloud	The resources and infrastructure are available to, and shared by, any potential customer. It is owned and maintained by the cloud service provider.
Service model	
Service-as-a-Service (SaaS)	Application capability provided to customers using the cloud service provider's infrastructure.
Platform-as-a-Service (PaaS)	The cloud service provider provides a platform for customers to deploy their own applications, created or bought. The underlying infrastructure is in control of the cloud service provider and not the customer.
Infrastructure-as-a-Service (IaaS)	The customer is provided more extensive control over underlying infrastructure, such as operating systems, storage and physical and virtual resources. Limited control over some networking components may also be granted.

Note. Information in the table from ISO/IEC 22123-1 Information technology – Cloud computing (ISO/IEC, 2021), NIST SP 800-145 The NIST Definition of Cloud Computing *(Mell & Grance, 2011)*, and Marinescu (2013, 2022).

[a] The customer can be compromised of multiple units.

2.2.1 Information Security and the Cloud

The cloud, a distributed server solution consisting of information systems, faces security issues (e.g., Alouffi et al., 2021; Balani & Varol, 2020; Bhajantri & Mujawar, 2019; Butt et al., 2022; Wulf et al., 2019). A cloud solution needs to consider the issues with confidentiality, integrity, and availability[1],

[1] *Known as the CIA triad, Confidentiality: protecting information from unauthorised access, Integrity: data are correct, complete, and have not been altered or modified in unintended ways, Availability: data are accessible when needed.*

and includes non-repudiation and authenticity, but should also consider authentication[2] to ensure that the data is kept secure and accurate (Barker et al., 2003, p. 15). A literature review of recent research regarding cloud security threats and challenges provides some insight into current issues. Studies that review previous research were chosen to summarise research findings, and the security concepts identified can be found in Table 3.

To face some of the issues concerning privacy and regulation of information security and the cloud, the European Union (EU) has produced a Cloud Code of Conduct (CoC) (EU Cloud CoC, n.d.-a). This CoC is meant to provide cloud customers with knowledge about CSPs' GDPR (General Data Protection Regulation) adherence. The CSP decides what level of compliance to apply for. At the time of writing, it is interesting that only one of the adherent services has the highest level of competence. Among major CSPs (Google, Azure, IBM, Oracle, AWS, Dropbox, Cisco), AWS is the only non-adherent CSP (EU Cloud CoC, n.d.-b).

2.3 Intelligence Agencies and the Cloud

The only two examples of intelligence communities using the cloud, according to the author's best knowledge, are the UK's GCHQ, MI5, MI6[3], and government departments and the Ministry of Defence (Warrell & Fildes, 2021) and the two deals the CIA have completed on behalf of the US intelligence community[4] (Konkel, 2014, 2020). The CIA cloud deal is slightly more well-reported than the UK one. Most of the reports on the CIA deal can be traced to one news site making information about either deal scarce. Considering the closed nature of intelligence agencies, this is no surprise but means there is precious little facts, information or research regarding the decision process, requirements or anything regarding cloud solutions chosen. There are also worries about choosing a US-based cloud company for UK data, especially considering revelations regarding the possibility of the US government gaining access to these companies (Ball & Rushe, 2013; Gellman et al., 2013; Gellman & Poitras, 2013), the article, however, mentions that all data will be stored within the UK's borders (Warrell & Fildes, 2021).

Despite the rise of cloud computing solutions and the digitalisation of organisations, there is little previous research on intelligence agencies and their approach and view on cloud computing. Their secret nature could explain this. Intelligence concepts regarding the cloud found in this section can be seen in Table 2. Some of these concepts are based on research from adjacent fields, military, and government use of the cloud, to provide some more insight into possible concepts. Many of the concepts found in these studies support the findings of Horlings' (2022), the main source for this section. Horlings suggest, and echoes, looking towards research in other fields as the topic lacks research within intelligence research and applying those findings in intelligence organisations. This suggestion is applied in this study by considering government and military cloud adoption; see Appendix E for an in-depth discussion of the relevant concepts presented in Table 2 and Table 3. The text is excluded from the main part due to not being directly relevant to the topic, but the context is needed.

[2] *Measure to ensure the validity of a transmission, message, or originator, or a means to verify the identity for authorisation* (Barker et al., 2003, p. 13).

[3] *The UK intelligence community consists of GCHQ, MI5 and SIS (MI6)* (MI5, n.d.-b).

[4] *The US intelligence community consists of 18 organisations* (Office of the Director of National Intelligence, n.d.-a).

Horlings' (2022) study is the most comprehensive research on intelligence agencies, the Information Age, and their use of digital tools. The study covers twelve intelligence journals, four professional intelligence journals, and the articles published between 2010 and the Autumn of 2021. In total, 89 articles were included in the study, having been selected using a requirement that "the article should engage in discussion of the implications of the Information Age in the intelligence domain" (p. 3). While the study covers various computer science tools as part of the intelligence process, it does not mention using the cloud or cloud computing.

Horlings (2022) discusses that the traditional, linear intelligence process is not viable anymore with the complexity and quantity of data available today. She notes that it is no longer about monitoring and researching what is not known or searching for what is known in unknown locations. It has changed to searching for both information and locations that are unknown. The findings include that the new intelligence process model builds on the access to meta-tagged data available for analysis to create knowledge to base decisions on. Collecting as much data as possible and making it accessible for the intelligence process is important and highlights the need for unprecedented storage capacity.

Over a decade ago, Lahneman (2010) discussed that intelligence analysts need to understand global dynamics and that organising and sharing information will become paramount in intelligence communities. Intelligence sharing can be divided into three levels: intra-agency, national intelligence community, and international, with different challenges to sharing present at each level; intra-agency sharing faces social barriers, national intelligence agency sharing has standardisation issues, and international sharing is a matter of trust (Horlings, 2022).

With the complexities and volumes of data and information available to intelligence communities, a need to move from data management to data governance is evident (Palfy, 2015).

Horlings (2022) identified two challenges regarding data processing: information overload and processing gap. Big data analytics and AI are presented as a tool to support the human analyst in the face of these challenges. Scalability is suggested to meet the needs of data governance and big data, especially regarding storage, manipulation, and analysis requirements. Proper data governance and the employee skill to upkeep the big data are also important. Organisation culture and failure to have the IT tools meeting the business needs is pointed out as a challenge towards data science integration (Horlings, 2022).

Horlings' (2022) findings show that cultural aspects and organisational readiness affect data science solution adoption. Organisational readiness, and management support, as a cloud computing adoption enabler, is supported by research in other fields (El-Gazzar et al., 2016; Jones, 2015; Liang et al., 2017; Oliveira et al., 2014; Porrawatpreyakorn et al., 2019). Organisational factors such as how resistant to change and general organisational inertia can further influence the cloud adoption process and decision-making (Koç et al., 2022; Liang et al., 2017).

Privacy and legalisation are discussed and cover topics such as the bulk collection of data from citizens, the Edward Snowden leaks, and that legalisation tends to lag behind technological advances (Horlings, 2022). The complexity of threats and environments is discussed and brings up the issue of technological advancement bringing more complexity to the intelligence gathering process.

To summarise the previously available research, while adapting and considering data science solutions in intelligence agencies is discussed, at no point is the cloud as a solution or alternative brought up. This is surprising, considering many articles focus on AI, big data, and data science applications. One of the articles explicitly mentions “scalable architecture for efficient storage, manipulation, and analysis” (Horlings, 2022, p. 13), something that should bring cloud computing to mind immediately.

Table 2

Overview of Intelligence Concepts

Source **Concept**	**El-Gazzar** (2014)	**Zwattendorfer et al.** (2013)	**Horlings** (2022)	**Jones** (2015)	**Lahneman** (2010)	**Palfy** (2015)	**El-Gazzar et al.** (2016)	**Oliveira** (2014)	**Liang et al.** (2017)	**Tweneboah-Koduah et al.** (2014)
Big data and AI			X							
Privacy and legalisation	X	X	X	X					X	X
Information sharing			X		X					
Data governance			X			X				
Information overload			X			X				
Processing gap			X			X				
Organisational readiness			X	X			X	X	X	X
Financial factors		X		X						X
Management commitment			X	X			X	X	X	

Note. See Appendix D for detailed concept descriptions.

Table 3

Overview of Cloud Security Concepts

Source Concept	**Alouffi et al.** (2021)	**Balani & Varol** (2020)	**Bhajantri & Mujawar** (2019)	**Butt et al.** (2022)	**El-Gazzar** (2014)	**Verma & Adhikari** (2020)	**Wulf et al.** (2019)	**Zwattendorfer et al.** (2013)	**Jones** (2015)	**Tweneboah-Koduah et al.** (2014)
Data security	X		X	X	X	X		X	X	X
Data loss		X	X	X						
Regulation and legal compliance		X	X		X	X		X	X	X
Loss of control	X		X		X	X			X	X
Employee expertise		X	X		X	X				
Compromised accounts and insider threats			X	X		X				
Business continuity and service	X	X				X			X	X
Lack of interoperability and portability	X				X	X		X	X	
Secure communications between cloud	X	X				X				X
Event logs		X				X				
User access control		X		X		X		X		
Insecure APIs and interfaces				X						
Data location		X			X				X	X
Data segregation		X		X						X
Audits					X		X	X		X

Note. See Appendix D for detailed concept descriptions.

3 Methodology

This chapter will present the chosen research strategy, data collection method and process, as well as ethical concerns. As there are no other similar studies on the topic of intelligence agencies' move to the cloud no comparison to previous studies can be made in methodology choice. This study will thus be both exploratory and explanatory.

3.1 Research Strategy

3.1.1 Case Study

Case studies aim to understand social phenomena where it is of interest to study a specific thing in-depth by using different data and research methods (Denscombe, 2014; Yin, 2018). This study is both exploratory and explanatory, and case studies lend themselves well for both types (Yin, 2018). This study's aims and research question is phrased using what but truly explore the reasoning and whys behind intelligence agencies moving to the cloud. Case studies work well to explain and understand how different facets affect the case (Denscombe, 2014), and to explore current events (Yin, 2018), in this case the lack of research concerning the intelligence community and the cloud. Furthermore, case studies allow the study of the context the case is placed in and how the context affects the case (Yin, 2018). Thus, a case study is an excellent choice to understand the hows and whys concerning intelligence agencies moving to the cloud. Thus, case study is the chosen research strategy.

3.1.2 Alternative Strategies

Action Research

Action research aims to deal with practical, real-world problems and includes factors such as change and a cyclical process to get feedback and prompt change, and requires people to actively participate (Denscombe, 2014). However, this means that research must be done practically directly involving the practice itself (Denscombe, 2014), something that is impractical for the resources available to this study, and thus action research as a strategy is discarded.

Surveys

Surveys offer similar benefits as case studies, it allows issues studying in-depth by varying data collection methods, mostly by questionnaires and interviews (Denscombe, 2014). They are also useful for creating a snapshot of current events and the in-depth studies tend to be exploratory and the discovery of new ideas (Denscombe, 2014). Surveys are also likely to struggle with contextual conditions (Yin, 2018), and for this study, the context is likely to play a significant role in answering the research question, causing surveys to be discarded as a research strategy.

3.2 Research Process and Case Planning

Runeson and Höst (2009) propose a five-step process when conducting a case study, presented in Table 4 below with the application in this study included.

Table 4

Overview of the Case Study Design Process and its Application in this Study

Step	Process step	Application in this study
1	Case study design	Planned the thesis and research.
2	Preparation for data collection	Literature review leading to conceptualising. Interview questions based on concepts. Reviewed Denscombe (2014) and Yin (2018) for case study design.
3	Collecting evidence	Semi-structured interviews ca 90 minutes long with experts in the field. See Appendix A-C.
4	Analysis of collected data	Thematic analysis according to Braun and Clarke (2022) and Denscombe (2014), see Appendix F.
5	Reporting	Writing the thesis.

This process will be followed in this study.

3.2.1 Case Study Design

Runeson and Höst (2009) cite Robson (2002) on six elements that should be included in a case study plan. These are: objective, the case, theory, research questions, methods, and selection strategy, all of which can be found in the Introduction, Literature Review, or this section.

The case is to understand what challenges intelligence agencies face moving to the cloud. To achieve this, experts with experience in the field will be interviewed.

3.2.2 Sampling Method

Purposive sampling was used to select experts who possess the necessary knowledge to answer the questions asked, as the relevance and knowledge of the topic needed for the case (Denscombe, 2014). The interviewees were chosen based on their knowledge and experience in the intelligence community and willingness to participate. The experts were contacted through email introductions via the study supervisor, and in one case a reference by another expert.

3.2.3 Preparation for Data Collection

As part of the preparation for data collection a case study protocol is produced and includes the interview questions and the procedure to follow when using the protocol (Yin, 2018). The case study protocol sections somewhat overlap with the general outline of this study, such as relevant literature and objectives of the study, data collection procedures, interview questions, and general information about presentation about the results and bibliographic information (Yin, 2018). However, the case study protocol will also include parts about the interview subjects that will not be published, yet need to be tracked during the research; see Appendix A-C for consent form, interview form, and interview questions.

Regarding the creation of interview questions, they are based on the previous literature presented above and covering topics that have not been extensively addressed in previous research. There are two sets of interview questions, one aimed at a more technical aspect of challenges and requirements, and one aimed at the organisational, cultural, and otherwise intelligence community issues. With five interviews to be completed, two will be of the technical type and three covering intelligence community issues. This is based on the findings where the technical challenges appear to be the same or mostly similar independent on who is using the cloud and for what purpose, only varying degrees of security implementation appears to be present, while the arguments and challenges faced by intelligence agencies are nearly completely unaddressed. The lack of cultural and organisational influence on cloud adoption is further supported by the literature in 2.3. This leads to the argument that the intelligence community's view on challenges on cloud solutions adoption are more relevant than addressing an already well-research area.

An informed consent form is produced and communicated to the interviewees to ensure they are informed about what the interview will entail and cover.

3.2.4 Collecting Evidence

To sufficiently be able to address the research question data about the topic is required and as there is a noticeable lack of document sources about the topic human sources will be used. The data collection will be done through semi-structured interviews.

Interviews are best utilised when the goal is to "explore complex and subtle phenomena … such as:

- Opinions, feelings, emotions and experiences, …
- Complex issues, …
- Privileged information …" (Denscombe, 2014, p. 186).

Yin (2018) also argues for interviews as a suitable way to collect data in case studies as they allow the researcher to target specific topics and allows for insights and explanations by and from the interviewee.

There are three structures to interviews, structured, unstructured, and semi-structured (Denscombe, 2014). Structured interviews are akin to questionnaires with limited answer options, while unstructured interviews introduce a topic that the interviewee expands upon and discusses their thoughts and ideas. Semi-structured interviews strike a balance between these two by asking open-ended questions where the interviewee can answer and expand as they wish, while also allowing the researcher to ask further questions for clarification and elaboration. Semi-structured interviews will thus be used in this study.

Interviews can be done in groups or in one-to-one sessions, while group interviews provide the advantage of being able to include more participants and allow for group discussions bringing new points to light (Denscombe, 2014). However, intelligence is a rather sensitive topic, and five interviews are intended to be completed for this research, and thus one-on-one interviews will be the chosen method. Five interviews were chosen to cover both the technological and intelligence concepts while also being manageable within the time and scope allowed this research.

The interviewees were experts within the field of intelligence in Sweden, with at least 10 years of experience, and have some working experience with cloud solutions, with two working to either procure or develop cloud solutions. Experts 1, 2 and 5 were asked the intelligence questions, and experts 3 and 4 were asked the technical questions. Due to the nature of the study and field no more information about the interviewees will be divulged.

Interviews were, when approved and agreed upon with the interviewee, performed and notes were taken during them. In two cases the interviewees agreed to audio recordings to ease the transcription process. When needed for clarification, the interviewer asked questions, or for the interviewee to repeat themselves. Four interviews were done in person and one using Zoom.

3.2.5 Alternative Data Collection

One alternative data collection method would be questionnaires. The purpose of questionnaires is to discover things by asking people about the research topic, and consist of written questions (Denscombe, 2014, p. 166). While questionnaires are easy to distribute and provide options for depth with open-ended questions, they also come with issues such as the lack of potential to ask follow-up or clarifying questions, respondents not being motivated to answer truthfully or at all, and that the information asked about should be straightforward (Denscombe, 2014). As the research topic is complex in nature and require depth to the answers questionnaires are discarded as a data collection method.

3.2.6 Data Analysis

Qualitative thematic data analysis will be performed on the data collected from interviews. By using Braun and Clarke (2022) for deeper understanding of the process while using Denscombe's (2014, pp. 247–248) five-stage data analysis process:

Table 5

Overview of Data Analysis Process and its Application

Step	Five-stage data analysis	Application in this study
1.	Data preparation – Transcribe the text, cataloguing or loading to software,	Notes from interviews are transcribed
2.	Initial exploration of the data – Look for themes, add notes and write memos,	1st (initial) iteration
3.	Analysis of the data – Code the data, group the data into categories, compare categories, further group them into concepts,	Two iterations planned
4.	Presentation and display of the data – Written interpretation of the findings, illustrate with quotes, use visual means of presentation,	Present final iteration themes
5.	Validation of the data – Data and method triangulation, alternative explanations comparison.	Compare to previous research etc.

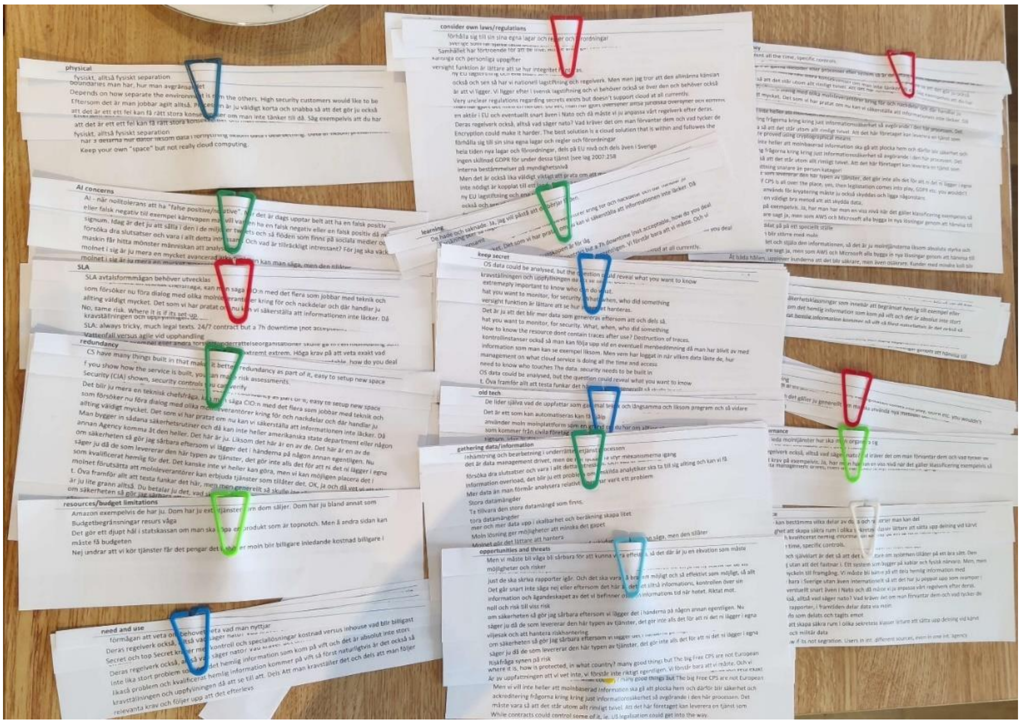
The data analysis followed these steps to reach results attempting to answer the research question; step 1-3 especially is of value when doing thematic analysis. During this process categories will be used for the second coding iteration with themes (concepts in Table 5) being the final products.

Three software were used during the coding process, step 1 used Microsoft Office Word to transcribe, step 2 used Taguette[5], an open-source tagging tool that allowed tying codes to relevant text and exporting these, and step 3 used FreeMind[6], an open-source mind mapping tool, to easily group the categories found into themes.

The interviews were transcribed as soon as possible after completion (step 1), and initial notes were taken during this process as well (step 2). Step 3 started with coding each interview, no codes were predetermined and instead decided on during the process. The codes were, however, influenced by the notes from step 2 and the knowledge of the previous research. 151 codes were identified during the first iteration. After the five interviews had been coded the codes and related text was printed and sorted into piles, see Figure 1, the number of codes and similarity between some of them did not allow for easy sorting using a computer which is why this approach was used. 150 codes (1 was removed during the process after being considered irrelevant) were sorted into 24 categories during the second iteration.

Figure 1

Picture of the Piles of Sorted Codes as Part of Iteration 2


physical
AI concerns
SLA
redundancy
resources/budget limitations
need and use
consider own laws/regulations
learning
keep secret
old tech
gathering data/information
opportunities and threats

The sorted codes and categories were entered into FreeMind and then sorted again into themes as FreeMind allowed an easy overview. The result of themes, and sub-themes, can be seen in Figure 2.

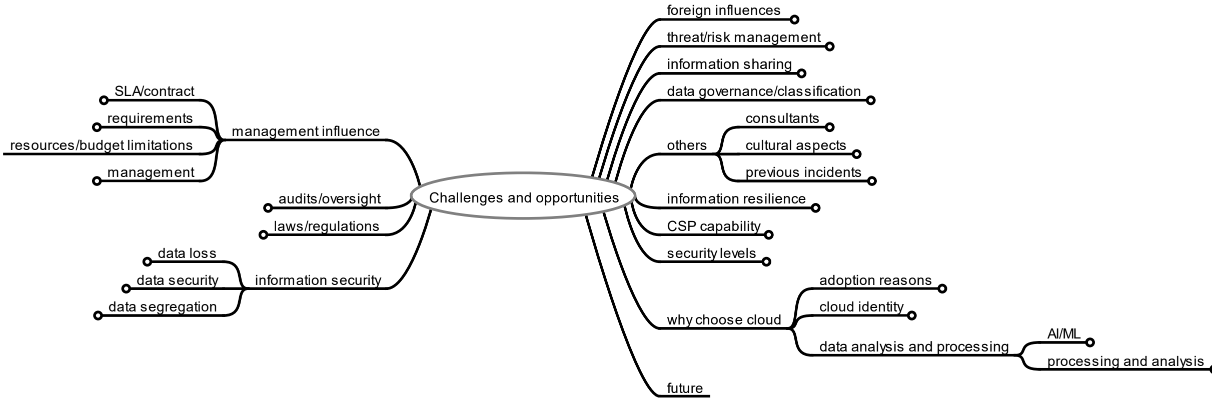
[5] *https://www.taguette.org/*

[6] *https://freemind.sourceforge.net/wiki/index.php/Main_Page*

The main themes are the branches closest to the middle, and the sub-themes the branches branching off the main themes. 14 main themes were identified during this step with 13 sub-themes. These are more than the previously identified categories because some categories become themes and include both their own codes and other categories, thus needing another sub-theme name to allow this presentation. For example: *data analysis and processing* was identified as a category, but had to include both its own codes and *AI/ML* (artificial intelligence/machine learning) codes, thus another sub-theme heading was added to visualise this properly.

Figure 2

Figure made in FreeMind Representing Thematic Analysis Results, 14 Themes and 13 Sub-themes



Note. CSP = Cloud service provider, *Security levels* is renamed to *security clearance level* in the text

The total result with codes can be seen in Appendix F. As part of the final iteration categories with similar themes were combined into one theme, i.e., *data loss* and *data segregation* were combined with the *data security* category to create the *information security* theme. Groupings mainly related to *management* and *why choose cloud* was treated the same way. Three groupings, *consultants, cultural aspects,* and *previous incidents* were put into an *other* theme as they were deemed important enough to be considered but not enough to warrant their own separate themes.

3.2.7 Results

The results will be presented in the Results chapter, and further discussed in the Discussion chapter. Steps 4-5 from the data analysis step will be utilised in for these two chapters.

3.3 Ethical Considerations

No specific ethical considerations are of concerns for this study. The only concern identified is the anonymity of the interviewees, especially as the study concerns a sensitive and secretive topic. As mentioned above, an informed consent form is produced and communicated to the interview participants, as well as a guarantee of their anonymity. This is by recommendation of Denscombe (2014, pp. 309–324), where he further provides guidelines that will be followed on what to include in the informed consent form, see Appendix A for consent form. No vulnerable groups are involved in the research, neither is any harm expected to come to the participants. The identifying information of participants will not be kept beyond what is needed to initially to identify them, nor will any personal data questions be asked. This study's research and data collection followed the recommendations from Stockholm University (n.d.), Vetenskapsrådet (2017) and Swedish Law. The interview transcripts will only be available to the researcher and relevant supervising persons.

3.4 Validity and Reliability

The reliability of this research is high, to the extent it can be measured for qualitative research (Denscombe, 2014, p. 297), experts in the field were chosen and confirmed to have many years of experience within the field of research. Their experience with the cloud was asked about and noted, and while some lacked some experience working with it, they had done related research concerning it. As interviews were chosen the exact same results are unlikely to be reproduced, and even within the five experts there were differing opinions regarding certain topics and solutions.

The validity of the research is easier to confirm, the interview questions were based on previous research, and five experts were interviewed to allow differing opinions to be expressed. Three experts within the intelligence field were chosen versus two in the technological field to allow for the discrepancy found during previous research that the intelligence field was the one lacking.

To further increase the validity and reliability of the research the same procedure was followed in all interviews, and any terms or concepts used was defined by referring to Appendix D. While it would be ideal to allow for the interviewees to validate the statements and results this is not possible due to time constraints.

4 Results

The thematic analysis resulted in 14 main themes which will be explained in this chapter. While some are in line with previous research others are not. The themes identified, in no specified order, are as follows:

1. Management influence
2. Audits/oversight
3. Laws/regulations
4. Information security
5. Foreign influence
6. Threat/risk management
7. Information sharing
8. Data governance/classification
9. Others
10. Information resilience
11. Cloud service provider capability
12. Security clearance levels
13. Why choose cloud
14. Future

All statements made by experts are to a degree paraphrased and, excluding Expert 4, translated by the author. This is due to the notes the statements are based on; experts 3 and 5 allowed for the interviews to be recorded and thus contain more detailed answers. Expert 4 provided answers in English and thus required no translation. When discussing a theme, the name will be *italicised* to allow for differentiating from concepts using the same name.

Management Influence

This theme includes four sub-themes:

1. SLA/contract
2. Requirements
3. Resources/budget limitations
4. Management

This theme concerns, as indicated by the name, the effect that management has on cloud adoption and usage. While the first three sub-themes are clearer in what they include *management* includes management-related topics that do not fit with the others.

SLA/contract regard issues such as management’s ability to negotiate appropriate contracts, which also includes the issue found in Chapter 2 regarding cloud location. While the interviewees mostly agreed that knowledge of where the data is stored is important but could be mostly mitigated by ensuring the data is encrypted, it was also argued that if it were to be an issue it would be negotiated in the contract to become a non-issue.

Expert 4 expressed that, paraphrased, “if the CSP is all over the place then legalisation comes into play, GDPR, and that you wouldn’t really be able to control [the data location in the cloud]” and that “encryption would make it harder, but the best solution is a cloud solution that is within and follows the same jurisdiction.”

However, the experts were split on the expertise regarding SLA management and procurement. Expert 1 stated that “contractual capacity [for SLAs] needs to improve,” Expert 4 somewhat echoes this with that SLAs are always tricky and contain much legal text, and that the technical and legal staff lack knowledge of each other’s fields which causes issues. Meanwhile, Expert 3 states, “I think this is something that they’ve been doing a long time. Set requirements and such,” implying a certain degree of knowledge and expertise in the area.

The *requirements* sub-theme is related to the *SLA/contract* sub-theme but concerned slightly different topics such as being able to properly measure how much usage of a cloud service is needed. Requirements can also differ between groups, as Expert 5 put it “being part of the EU, and potentially soon NATO we need to adapt our regulations to them,” showing that an organisation is unlikely to exist in a vacuum needing to consider outside requirements as well.

While the interviewees agreed that adopting the cloud would be expensive there were some statements indicating that “intelligence agencies get the money they need” (Expert 2). However, this was also contradicted by statements about looking at the budget that Swedish intelligence agencies are granted, suggesting that *budget and resources* are likely to be a, at the very least, initial concern. This was also supported by statements by Expert 2 who followed with “there will be an initial bump,” and Expert 1 who said, “secret and top secret [data] requires more control and tailored solutions,” and continued that it needs to be compared to having an in-house solution cost wise.

To expand on the *management* sub-theme, it concerns topics such as the lack of knowledge regarding the cloud in management, but also how they are learning and building expertise. However, employees and their level of expertise and the education of them are also included here as this was judged to be a management issue. The theme further includes that there is support for the cloud and that they understand the need for cloud computing even if a level of distrust, most likely based on lack of knowledge, is present.

The *management influence* theme shows that management is integral for cloud adoption and without it little will happen; they decide what can be included and if the money and resources needed shall be directed towards it.

Audits/oversight

This theme is based on the need for audits and oversight; while not immediately connected they do concern the same thing: tracking of actions taken. During the interviews the possibility and need to be able to track actions both from within the organisation and the cloud service provider was noted. It was mentioned that adopting cloud solutions could allow for better oversight especially with the need for audits compared to current solutions not having changed.

Experts 1 and 5 both said that oversight is likely to become easier by logging every action in a cloud environment, while Expert 4 supports this by saying that “it is extremely important to know who can do what” and “what, when, and who did something.”

Some issues, but also opportunities, regarding audits and logs were noted but are more in the realm of practical information security implementation and outside the scope of this study.

One part of the *audit and oversight* theme is the need to continuously follow up and evaluate the cloud service to ensure that contracts and requirements are being followed and upheld. This ties into the theme of *management influence* and their ability to negotiate contracts with appropriate audit and logging requirements. Audits and oversight, when utilised correctly, can bring improved information security capability.

Laws/regulations

When laws and regulations were brought up during the interviews it was often in relation to how they are lagging behind the digital and technological evolution and the needs that have come with it. It was also noted that the laws are improving and are being worked on, but currently the fact is that they hinder intelligence agency use of the cloud. Other than this, Expert 5 brought up issues regarding privacy and the trust that intelligence agencies act as intended. This ties into the *audits/oversight* theme and that oversight will be easier in a cloud solution, hopefully increasing trust in intelligence agencies.

The need to first and foremost consider laws and regulations concerning oneself (Expert 3) was also brought up, and ties into issues that Swedish government agencies are very autonomous meaning that different agencies can have different rules concerning cloud usage. As mentioned in the *management* theme's sub-theme *requirements*, an organisation is unlikely to exist in a vacuum and thus needs to conform to outside laws and regulations as well, one example being the GDPR from the EU. Also from the *management* theme is the *SLA/contract* sub-theme where Expert 4 said that "SLAs are tricky, [there are] many legal texts," further showing the importance of regulations and laws for cloud usage but also the need to understand these to be able to use these services.

Furthermore, the regulations regarding secret and top secret classified information are unclear, and "doesn't support cloud at all currently" (Expert 4), showing that while cloud could be used for some purposes if the most important pieces of data and information must be stored off cloud and cannot be processed in the cloud, the purpose of cloud adoption is somewhat lost.

Information security

This is the most extensive of the themes with the most codes included. It has three sub-themes:

1. Data loss
2. Data security
3. Data segregation

The findings in this theme are not surprising, agreeing with general best practices within information security solutions and previous research. Within *data security* the most surprising was the consensus of the need for encryption, this was in response to both data security concerns but also potential issues with cloud service provider data access, as well as in-transit data security. Other than that, the issues related to *data security* are expected from any information system, however with higher demands on fulfilling information security requirements, as Expert 5 expresses, paraphrased: that if Swedish intelligence agencies would move to the cloud, they would have extremely high requirements regarding information security such as location and data access. The requirements would be "shall requirements" (Swedish: skall-krav"), wherein it must be fulfilled to even be considered.

Data security for intelligence purposes is likely to be held to a higher standard due to the sensitive nature of the data and information handled. During the interviews many different data security topics were brought up, from the CIA-triad components to the need for strong encryption and encryption key management, but also that the newest latest technology and methodology perhaps is not always the best, supported by this statement from Expert 3 “it’s a security to not jump on the newest, I usually say that if the methods or processes are a few years old they are well tried.”

Experts 3 and 4 expressed the need to implement a two-man rule, a security mechanism that requires two or more authorised persons to execute an action, the need for a jump server, a single-entry point for cloud service users, and the use of zero trust environments. Zero trust environments as a solution cover most of the issues brought up within the *data security* sub-theme; it builds on proven identities for each session, all communication to be secured, and access is granted on a least-privilege basis needed to complete the task, no more access than what is needed is granted and more (IBM, n.d.-b; Microsoft, 2021; Rose et al., 2020).

Data loss comparatively brings up some cloud-specific issues. One is the issue of the cloud service provider disappearing, and another is the need to plan to not lock solutions into a specific provider making data migration more complicated.

The most cloud-specific issue is the *data segregation* sub-theme; while the shared use of resources is integral for a cloud solution it also presents issues for intelligence use. Data needs to be segregated and boundaries established to ensure security, but it also limits the cloud possibilities. Tied to this, but also the *audits/oversight* theme, is the question of traces left behind by queries; if this is not properly secured leaks may happen.

The *information security* theme captures some of the many challenges in moving to the cloud, it will need careful planning and implementation to ensure that the security is kept up while also allowing important functions such as audits and information sharing to occur.

Foreign influences

This theme covers several topics that boil down to that influence from foreign actors cannot be disregarded. Mainly it concerns the influence US companies and government have on the cloud solution adoption, part of this is the genuine issue of US government access to US company data. Expert 1 expressed “a government’s right to access and right to take part [of data] versus ability [to do so]”, which further highlights the problem, can a foreign government entity legally access the data and if they have the ability to do so. There is also the influence brought on by allies using cloud solutions, it can be compared to group pressure wherein not using a technology would exclude you.

Experts 1, 3, 4 and 5 expressed concerns regarding US-based companies as cloud hosts for intelligence purposes, either due to US laws and regulations, the established risk of US government access to the data, or the potential of being denied access to one’s own data.

The most common issues noted in this theme were regarding the fact that most cloud service providers are from the US and are subject to US law presenting security concerns. As such being aware of the *foreign influence* when choosing a cloud solution is of importance.

Threat/risk management

To dare take risks and balance the threats and opportunities was brought up multiple times as something that needs to be done to adopt a cloud solution. Expert 5 summed up the problem well with “but we need to dare be vulnerable to be effective, and that is an equation that needs to work in the end.” Putting the data and information on the Internet is a risk, but it would allow for many opportunities and the ability to balance and consider these are of importance to adopting a cloud solution. Experts 2, 4 and 5 all express the need to take risks and manage these, and that a zero-risk approach is no longer viable for cloud solutions. Risks need to be taken to be able to utilise these new tools.

Information sharing

The ability and need to share information were found to be of importance, the interviews indicated that this would likely be made easier using cloud solutions and is likely to become a necessity. Expert 2 said "today you exchange reports, in the future the data can be shared using the cloud." But information sharing is not done just between different intelligence agencies (externally) but also within different departments and intelligence agencies within the same community (internally) which needs to be improved, as exemplified by Expert 4, paraphrased, that "[the US] had data on 9/11 available but at different agencies and not in a way that let them know it was going to happen," showing that if the data is spread out it cannot be utilised for its intended purpose. Expert 5 also expresses the need to improve intelligence and information sharing among intelligence communities.

However, issues were noted as well, such as setting up appropriate security controls, using security layers and clearance to control who can access what. *Information sharing* is closely connected to the *security clearance levels* theme in parts, information sharing in this case is built upon the components of security clearance. The experts noted that by utilising cloud solutions it would be easier to share data and information while having high control over who can access it.

This theme could also be considered to belong to the *information security* theme but based on previous research and the comments made by the interviewees it needs its own theme. This is partly due to the issues it will face but more so for the potential it has to speed up and ease information sharing both internally and externally.

Data governance/classification

This theme comes partly from the previous research regarding the move from data management to data governance but also relates to *information sharing*. Part of this is that currently different intelligence communities use different classifications of the same kind or even the same data meaning that the same pieces of data or information can have different classifications depending on agency (Expert 5), but also the different classifications require different levels of data security, i.e., encryption (Expert 3). This can cause potential issues both when sharing information between two agencies but also if they were to use the same cloud. If they have the same information but different classifications, this could cause unintended issues. As such the need to unify and use the same classification and thus governance would be important in a cloud adoption scheme, even more so if multiple intelligence agencies were to use the same space.

Expert 5 expresses that the current state of Swedish intelligence agencies is data management driven but a shared classification is needed and that governance mechanisms are underway.

Others

This theme contains three sub-themes of importance that are not big enough to warrant their own themes:

1. Consultants

2. Cultural aspects
3. Previous incidents

Consultants concern both the risk and opportunities consultants and third-party actors can bring to an organisation wishing to adopt cloud solutions and should be regarded as such. This sub-theme also brings up that independent actors can provide valuable services such as audits.

Cultural aspects regard organisational culture, something that was brought up in Chapter 2 as a possible challenge towards digitalisation and has been found, in this study, to be a possible challenge towards cloud adoption. However, there are also groups not resistant towards cloud adoption who would support it.

Last of this theme is *Previous incidents*, a sub-theme concerning previous cases of (failed) outsourcing attempts, one that many Swedes may remember is the Transportstyrelsen incident where personnel without an appropriate security clearance was allowed access to personal and classified data (Olsson & Strengbom, 2017). Attempts that have failed due to mismanagement and a "you get what you pay for" attitude can work against future cloud adoption attempts and proposals, but can, and should, be learnt from to understand what went wrong.

Information resilience

The name of this theme comes from one of the experts interviewed, the concept was apt enough to be included as a theme as it covers potentially important factors, especially for cloud adoption for military use.

> How do we guarantee that we can don't make ourselves vulnerable by using data centres that can be bombed? How do we create resilience if we are attacked? If Russia was to wage an offensive war on Sweden and step into our borders, then they shouldn't be able to steal information. How do we face that and create resilience? By exporting servers abroad and by putting our data on the cloud that cannot be penetrated by foreign powers. That is information resilience. (Expert 5)

As seen in the quote by Expert 5 *information resilience* concerns the capability to keep working in crisis and war, and the cloud can prove to be an important tool for this. By not being bound by physical places that can be destroyed military capability can be ensured no matter where the persons are and the situation around them. It also includes the concept of digital sovereignty, a nation's ability to control its digital tools and data (Couture & Toupin, 2019; Floridi, 2020).

As with any new implementation of digital tools it is a balance between risk and gain, perhaps even more so for cloud adoption for intelligence use. Intelligence would rather not have anything on the Internet while the gains could be enormous, as such it becomes a question of how much risk the organisation is willing to take to gain the benefits.

Cloud Service Provider capability

This theme concerns what the CSP is capable of, such as their ability to ensure redundancy and provide security options like encryption. It also includes facts such as that most big CSPs are focused on providing cloud services and thus can put the resources towards it, compared to a government agency hosting a cloud solution themselves. On the other hand, topics such as that different CSPs provide different services are mentioned here, as well as that it is important to not lock oneself in with CSP-specific solutions.

It was noted during the interviews that if even the US, with resources and money incomparable to smaller countries, chose to use CSPs to deliver the cloud solutions a smaller country is unlikely to be able to host their own cloud. It can thus be concluded that considering the CSP and its capabilities are important when choosing a cloud adoption, no matter on what scale and for what purpose, especially important for intelligence agencies are the CSPs' proven capability when it comes to data and information security aspects.

Security clearance levels

Security clearance levels are an important part of an organisation, even more so for organisations handling information, data and intelligence concerning the safety of a nation. As such the implementation, planning and consideration of how to handle *security clearance levels* of data and information should be considered when choosing and planning a cloud solution, even more so if it is meant to be shared between multiple intelligence agencies and government bodies.

This is mostly aimed at classifying data and information correctly and some of the personnel security clearance, however security clearance is (presumably) already well practiced and not a cloud-specific issue.

Why choose cloud

This is the second most extensive theme counting the number of codes included, as well as sub-themes. It concerns reasons as to why one would choose a cloud solution and the benefits it can bring an organisation; however, it is not without challenges, especially regarding *AI/ML*.

The sub-themes included are:

1. Adoption reasons
2. Cloud identity
3. Data analysis and processing
    a. AI/ML
    b. Processing and analysis

As can be seen, the third sub-theme has two additional sub-themes to further highlight a division within the *data analysis and processing* sub-theme. This is due to *AI/ML* being brought up with important points but not to the degree it warrants its own theme, or even sub-theme, and better connects with the *data analysis and processing*.

The *adoption reasons* sub-theme concern straightforward reasons as to why one should adopt a cloud solution such as the current use of slow and old technology, its ability to facilitate automation, and allow staff to work with modern tools. It was noted during the interviews that working with old and slow technology may be off-putting for personnel and leads to a lack of knowledgeable and experienced employees.

Cloud identity includes anything that defines a cloud, its ability to allow sharing of systems and resources, scalability, data format, the different cloud deployment models, see Table 1, and similar topics. The sub-theme sums up technological reasons why a cloud solution should be considered while also noting the different options and some things to consider, i.e., cloud deployment mode, or even in-house or local solutions.

The *data analysis and processing* sub-theme is the most extensive of the sub-themes, as the name implies it brings up the possibilities a cloud solution can bring regarding the analysis and processing of data. While information overload and the processing gap were noted in previous research as a possible challenge the findings of this study do not find it as problematic. Expert 1 expressed that a cloud solution "gives [one] tools to handle data." Expert 5 said "that the cloud allows information processing, information analysis and data processing at a higher, faster pace and more efficient." Expert 2 noted that information overload has long been a problem while the opinion of Expert 5 is that it is mitigated using data models and AI-driven technology allowing for analysing bigger amounts of data. Expert 5 further notes that it becomes an issue if a single analyst tries to analyse all the data by themselves and that technology can help.

Experts 1, 2, 4 and 5 all expressed their support for the increased capabilities of processing data using a cloud solution and Experts 1 and 5 noted that AI/ML tools can help with this. Expert 5 further commented that AI/ML use could help find new views and help keep a neutral opinion.

However, Experts 1 and 2 both expressed concerns that AI should be a tool with human oversight, and it is important to understand the decisions made as well as not letting AI make just any decision.

Future

This theme is unique compared to the rest, while the other themes touch upon more specific challenges and opportunities this theme regards the findings that the cloud is the future within intelligence communities. Partly because of the themes presented above, such as *why choose cloud*, *foreign influences*, and *information sharing*, but even more so due to the many opportunities it can bring an organisation, especially one handling such massive amounts of data as an intelligence agency. The need to be able to analyse and process such amounts need to be supported by appropriate tools and cloud computing is such a tool that is also available.

All five of the interviewed experts expressed that the cloud is the future, their reasons may have varied but the result is the same: the cloud is the future. The experts expressed varied and multiple reasons that tie into the above-presented themes. "Others are using the cloud" (Expert 2), "we need it to keep up, the potential oversight and processing capability cannot be overlooked" (Expert 5), and "many tools developed are aimed at cloud solutions" (Expert 3), these are just some of the comments about the cloud as the future made by the experts.

It is also worth noting that the cloud is already being used for intelligence purposes by Google, as Expert 4 put it, what is Google doing using their data, cloud computing and analysing power to predict our needs to direct advertisements at users if not intelligence? And it is correct, Google is using the cloud to produce intelligence about their customers that is used to direct relevant advertisements at them. The cloud is used as part of intelligence processes is thus already happening every day, every minute, and this is an argument to consider well before dismissing or considering the possibilities of the cloud.

5 Discussion

The two research questions this study aims to answer are: *What challenges do intelligence agencies face when adopting cloud solutions?* and *What opportunities does a cloud solution bring to an intelligence agency*?

The findings of this study show that the challenges faced by intelligence agencies moving to the cloud are many, one of the biggest issues is *information security* and *cloud service provider capability*. The demanding requirements on information security to ensure that the data in the cloud is only accessible by those authorised means that a CSP need to prove their capability to provide these services. The fact that many, if not most, of the big CSPs are US based and subject to US legalisation was also one major issue brought up. While encryption was proposed as one solution to mitigate this it also requires trust that the CSP delivers the encryption and services as promised, if this cannot be guaranteed it is unlikely that an intelligence agency would even consider choosing a US-based CSP. While previous research, see Chapter 2, touched on the data security of information security it did so in more general terms and discussed data security broadly rather than its components which, considering the selection of previous research for this study is logical, as there are plenty of studies that discuss specific data security controls. CSP's capabilities was found in parts in Chapter 2, the lack of interoperability and portability, while the other challenges found by this study such as CSPs' ability to provide information security solutions are new.

The issues brought by US legalisation are tied to the *foreign influences* theme where there is both the challenge of foreign legalisation, but also how their use of the cloud currently means they are getting ahead in the intelligence game. The previous research regarding *foreign influence* does not mention the same concerns here but rather that they are already using cloud solutions and can thus reap the benefits of it already. To be able to keep up the adoption of cloud solutions is likely to be needed, and this is expressed multiple times by the experts interviewed.

While audits were noted as a possible challenge in previous research (El-Gazzar, 2014; Tweneboah-Koduah et al., 2014; Wulf et al., 2019; Zwattendorfer et al., 2013) this was not the case here, rather the possibility for improved oversight and log management (part of audits and tracking actions) was the main point.

One finding of interest is the *management influence* theme. Management is, in previous research (El-Gazzar et al., 2016; Horlings, 2022; Jones, 2015; Liang et al., 2017; Oliveira et al., 2014; Porrawatpreyakorn et al., 2019), commonly brought up as a supporting and driving factor in adopting new technology and solutions and it is usually the education and expertise of the employees that can be noted as a future and further challenge. This study found that while some employees may lack knowledge and expertise in using the cloud it is the management's lack of knowledge that is the big hinder. They are not aware of its many uses, abilities, and risks, and are the ones who need to learn more.

Employees are, in private companies, more likely than not to use cloud solutions (Eurostat, 2021; Galov, 2023; Lukehart, 2022) and thus more likely to possess knowledge about its use. Management, especially in intelligence communities, appears to have been using old and outdated technology for a long time and thus lack the necessary experience with cloud solutions. The findings of this study are that management is more likely to need to learn about the benefits, uses, and nuances of cloud computing rather than employees. This is not to say they completely lack this knowledge, they are learning and slowly understanding the need for the cloud.

Another challenge noted, and supported by previous research, is the *laws/regulations* theme. Previous research noted how laws and regulations have not kept up with the technological advances and need to be updated and revised to better reflect the current digital environment. The findings in this study support this, and that intelligence agencies often face even more complex issues as, in the case of Sweden, the legalisation does not support moving top secret and secret classified information and data to the cloud, and in some cases outside the borders at all. Laws and regulations need to be updated and allow for moving highly classified information outside the borders for clouds to become a viable option. If the limit of keeping the information within the borders stays it brings up the issue of *information resilience*, wherein the continued operability and capability would be hindered if the cloud premises were to be placed within a country. By limiting where the cloud is physically placed one of the major benefits of using a cloud solution is negated, the potential to have the data stored far away protects it in the case of local crisis, both natural and manmade.

While many of the themes found presented challenges, they are of the type to be considered when choosing what and how a cloud should be implemented, such as planning for *data governance/classification*, *information sharing*, *security clearance levels*, and *threat/risk management*. These are considerations to mind for any new system to be implemented, especially for organisations with high-security demands. While some of these themes are supported by previous research *threat/risk management* was not one of these. However, it should be part of any security process to consider the threats and risks when adopting new solutions and such research can be referenced if needed. As Lahneman (2010) noted information sharing will be required and the results support this, Horlings' (2022) findings regarding the difficulties in information sharing can, by using a cloud solution, be mitigated. Palfy (2015) and Horlings (2022) both noted the need for data governance which the findings of this study support. No previous research regarding *security clearance levels* was found as part of the literature review and is a new finding.

The *others* theme presents some considerations to be made regarding previous incidents and how to handle cultural aspects which also should be noted. The *cultural aspects* of this theme is supported by earlier findings (Horlings, 2022; Koç et al., 2022; Liang et al., 2017), while the *previous incidents* are not and should be considered new knowledge to the field.

The themes that can be classified as opportunistic in nature, to answer the question *What opportunities does a cloud solution bring to an intelligence agency*? are: *why choose cloud* and *future*. However, the themes: *information sharing, information resilience*, and *audits/oversight* also include many opportunities.

Why choose cloud and *future* both note reasons as to why one should use the cloud, especially the analytical and processing benefits. The opportunities that can be found in the other three themes are perhaps less obvious but nonetheless as important. The potential to share information easily and control who has access to what while ensuring secure sharing cannot be dismissed, just as the ability for improved oversight cannot be overlooked. Improved oversight of data and information access was noted by the experts to be one big potential change and benefit to using a cloud solution. This would allow for easier tracking of who has accessed and viewed what meaning that information security can be improved. The *information resilience* theme is one of the most opportunistic in nature, it would allow for continued operationality and capability in case of crisis. If the data and systems were cloud-based, then personnel would be able to keep working no matter what happens to their physical workplace. Cloud solutions for military use would likely benefit the most of this, even if the country of operations were to be attacked, they could continue their intended operations. During the interviews the war in Ukraine was brought up as an example of how the cloud can support and benefit a country at war, but the details are outside the scope of this study. Furthermore, *information resilience* was not one of the concepts found during the previous research review and thus provided some interesting insight into intelligence-specific challenges not found in other organisations.

5.1 Conclusion

There are many challenges and opportunities to consider if intelligence agencies are to move to the cloud. While the challenges are complex the possible opportunities cannot be forgotten and should be weighed equally, without risk no gains can be made. The findings of this study tentatively suggest that the opportunities and benefits brought by cloud computing solutions may outweigh the risks if managed properly. However, the biggest challenge appears to lie in issues beyond the intelligence communities' direct influence: laws and regulations. This applies to both local and foreign laws and regulations. Local laws limit cloud use while foreign, especially US laws, mean that foreign CSPs may be subject to laws incompatible with the requirements of an intelligence agency.

The other themes are highly influenceable by the intelligence agency and community themselves and depend on their own implementation ability and capability. Laws and regulations are often written by those lacking appropriate technical knowledge and create a gap between the technological and legal requirements.

To answer the research question: *What challenges do intelligence agencies face when adopting cloud solutions?* the answer is that the biggest challenge is laws and regulations.

And to answer the sub-question: *What opportunities does a cloud solution bring to an intelligence agency*? the answer is the analytical and processing, and information sharing potential brought by a cloud solution.

5.2 Limitations

Due to limit in time, scope, and manpower, only five interviews were conducted, and only Swedish experts were interviewed. This means that their experience is wholly from the Swedish intelligence community perspective and that findings in other intelligence communities could differ. Furthermore, no specific challenges or requirements on a cloud solution could be discussed. The research, knowledge, and current implementation of possible cloud solutions or related tools are, as indicated during interviews and discussions with the interviewees, secret and confidential and cannot be revealed. As such many of these challenges are general in nature due to the secrecy involved in intelligence agencies.

5.3 Future Work

Due to this study being a master thesis and limited in both time, manpower, and potential to allow for a complete discussion on the many facets of the intelligence field the author recommends future studies to choose one field of intelligence to better narrow the use. This could be military, internal, or foreign intelligence. Other potential fields to consider would be individual/analytic, governance and management, advantages and disadvantages, and operational capability. While some of these topics were touched upon, they could benefit from more in-depth studies focused on these specific topics.

Furthermore, due to the nature of this study a discussion regarding the threat scenario and the political environment is lacking and a study discussing the influences these factors have on intelligence use of digital tools would be beneficial. A study concerning cloud and digital tools used for intelligence using the war in Ukraine and their implementation could be especially valuable. Ukraine is being mentioned specifically due to the current situation where they are actively being tested in concepts such as information resilience and having had to adopt cloud and digital tools quickly.

This study used semi-structured interviews which worked for an exploratory study, a future study could use unstructured interviews to allow experts to discuss the topic freely with some guidance from the interviewer.

As laws and regulations were found to be the biggest challenge an in-depth study of the specific laws hindering appropriate digital and cloud tool adoption is also recommended.

References

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, *9*, 57792–57807. https://doi.org/10.1109/ACCESS.2021.3073203

Balani, Z., & Varol, H. (2020). Cloud Computing Security Challenges and Threats. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)1*, 1–4. https://doi.org/10.1109/ISDFS49300.2020.9116266

Ball, J., & Rushe, D. (2013, June 6). *NSA Prism program taps in to user data of Apple, Google and others | US national security | The Guardian*. The Guardian. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Bang, M. (2017). *Military Intelligence Analysis: Institutional Influence* [Doctoral dissertation].

Barker, W. C., Evans, D. L., Bond, P. J., & Bement, A. L. (2003). *Guideline for Identifying an Information System as a National Security System Guideline for Identifying an Information System as a National Security System* . https://doi.org/10.6028/NIST.SP.800-59

Bhajantri, L. B., & Mujawar, T. (2019). A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures. *Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019)*, 376–380.

Bimfort, M. T. (1958). A Definition of Intelligence. *Studies in Intelligence*, *2*(4), 75–78.

Braun, V., & Clarke, V. (2022). *Thematic Analysis*. SAGE.

Busch, P., Smith, S., Gill, A. Q., Harris, P., Fakieh, B., & Blount, Y. (2014). A Study of Government Cloud Adoption: The Australian Context. *25th Australasian Conference on Information Systems, ACIS 2014*.

Butt, U. A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M. T., & Albaqami, N. (2022). Cloud Security Threats and Solutions: A Survey. In *Wireless Personal Communications*. Springer. https://doi.org/10.1007/s11277-022-09960-z

Cho, S., Hwang, S., Shin, W., Kim, N., & In, H. P. (2021). Design of military service framework for enabling migration to military saas cloud environment. *Electronics (Switzerland)*, *10*(5), 1–18. https://doi.org/10.3390/electronics10050572

Cloudflare. (n.d.). *What is the cloud? | Cloud definition*. Retrieved 3 March 2023, from https://www.cloudflare.com/learning/cloud/what-is-the-cloud/

Corrigan, J. (2018). *CIA Official: Cloud Is More Secure Than Old Tech, Less 'Soul-Crushing'*. Nextgov. https://www.nextgov.com/it-modernization/2018/06/cia-official-cloud-more-secure-old-tech-less-soul-crushing/149211/

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media and Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Denscombe, M. (2014). *The Good Research Guide For small-scale social research projects Open UP Study Skills*.

Domo. (2022). *Data Never Sleeps*. https://www.domo.com/data-never-sleeps#

El-Gazzar, R. (2014). An overview of cloud computing adoption challenges in the norwegian context. *Proceedings - 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014*, 412–418. https://doi.org/10.1109/UCC.2014.52

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software*, *118*, 64–84. https://doi.org/10.1016/J.JSS.2016.04.061

EU Cloud CoC. (n.d.-a). *About EU Cloud CoC: EU Cloud CoC*. Retrieved 28 February 2023, from https://eucoc.cloud/en/about/about-eu-cloud-coc

EU Cloud CoC. (n.d.-b). *List of adherent services: EU Cloud CoC*. Retrieved 28 February 2023, from https://eucoc.cloud/en/public-register/list-of-adherent-services

Eurostat. (2021). *Cloud computing - statistics on the use by enterprises - Statistics Explained*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises

FBI. (n.d.). *Types of Intelligence Collection - Intelligence Studies - LibGuides at Naval War College*. Retrieved 30 January 2023, from https://usnwc.libguides.com/c.php?g=494120&p=3381426

Federal Trade Commission. (2016, July 25). *U.S.-EU Safe Harbor Framework | Federal Trade Commission*. https://www.ftc.gov/business-guidance/privacy-security/us-eu-safe-harbor-framework

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy and Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Försvarsmakten. (2020, May 7). *The Intelligence and Security Service - Swedish Armed Forces*. https://www.forsvarsmakten.se/en/about/organisation/the-intelligence-and-security-service/

FRA. (n.d.). *Underrättelser - FRA*. Retrieved 12 February 2023, from https://www.fra.se/underrattelser.4.55af049f184e92956c42bab.html

Galov, N. (2023). *Cloud Adoption Statistics for 2023*. Web Tribunal. https://webtribunal.net/blog/cloud-adoption-statistics/

Gellman, B., & Poitras, L. (2013, June 7). *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program - The Washington Post*. The Washington Post. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Gellman, B., Soltani, A., & Peterson, A. (2013, November 4). *How we know the NSA had access to internal Google and Yahoo cloud data - The Washington Post*. The Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/

Horlings, T. (2022). Dealing with data: coming to grips with the Information Age in Intelligence Studies journals. *Intelligence and National Security*. https://doi.org/10.1080/02684527.2022.2104932

Huskaj, G. (2017). *Cyber Deterrence An Illustration of Implementation* [MSc].

IBM. (n.d.-a). *What is cloud computing?* Retrieved 3 March 2023, from https://www.ibm.com/topics/cloud-computing

IBM. (n.d.-b). *What is Zero Trust? | IBM*. Retrieved 27 April 2023, from https://www.ibm.com/topics/zero-trust

International Trade Administration. (2020). *Privacy Shield Program Overview | Privacy Shield*. https://www.privacyshield.gov/Program-Overview

ISO/IEC. (2021). *ISO/IEC 22123-1 Information technology - Cloud computing - Part 1: Vocabulary*.

Jasper, M., & Konkel, F. (2021, July 6). *Pentagon Cancels JEDI Cloud Contract - Nextgov*. Nextgov. https://www.nextgov.com/it-modernization/2021/07/pentagon-cancels-jedi-cloud-contract/183077/

Jones, S. (2015). Cloud computing procurement and implementation: Lessons learnt from a United Kingdom case study. *International Journal of Information Management*, *35*(6), 712–716. https://doi.org/10.1016/j.ijinfomgt.2015.07.007

Kent, Sherman. (1966). *Strategic intelligence for American world policy*. https://www-jstor-org.ezp.sub.su.se/stable/j.ctt183q0qt

Koç, B., Şener, U., & Eren, E. P. (2022). Determinative Factors of Cloud Computing Adoption in Government Organizations. *2022 3rd International Informatics and Software Engineering Conference (IISEC)*. https://doi.org/10.1109/IISEC56263.2022.9998286

Konkel, F. (2014, July 17). The Details About the CIA's Deal With Amazon. *The Atlantic*. https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/

Konkel, F. (2020, November 20). *CIA Awards Secret Multibillion-Dollar Cloud Contract* . Nextgov. https://www.nextgov.com/it-modernization/2020/11/exclusive-cia-awards-secret-multibillion-dollar-cloud-contract/170227/

Konkel, F. (2022, December 7). *Pentagon Awards $9B Cloud Contract to Amazon, Google, Microsoft, Oracle - Nextgov*. Nextgov. https://www.nextgov.com/cxo-briefing/2022/12/amazon-google-microsoft-oracle-awarded-9b-pentagon-cloud-contract/380596/

Lahneman, W. J. (2010). The Need for a New Intelligence Paradigm. *International Journal of Intelligence and CounterIntelligence*, *23*(2), 201–225. https://doi.org/10.1080/08850600903565589

Liang, Y., Qi, G., Wei, K., & Chen, J. (2017). Exploring the determinant and influence mechanism of e-Government cloud adoption in government agencies in China. *Government Information Quarterly*, *34*(3), 481–495. https://doi.org/10.1016/j.giq.2017.06.002

Lukehart, M. (2022). *Cloud Computing Statistics (2023) - Parachute*. Parachute. https://parachute.cloud/cloud-computing-statistics/

Marinescu, D. C. (2013). Cloud Computing: Theory and Practice. In *Cloud Computing: Theory and Practice*. Elsevier Inc. https://doi.org/10.1016/C2012-0-02212-0

Marinescu, D. C. (2022). Cloud Computing: Theory and Practice. In *Cloud Computing: Theory and Practice*. Elsevier. https://doi.org/10.1016/C2020-0-02233-4

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-145

MI5. (n.d.-a). *Gathering Intelligence | MI5 - The Security Service*. Retrieved 30 January 2023, from https://www.mi5.gov.uk/gathering-intelligence

MI5. (n.d.-b). *National Intelligence Machinery | MI5 - The Security Service*. Retrieved 3 March 2023, from https://www.mi5.gov.uk/national-intelligence-machinery

Microsoft. (2021). *Evolving Zero Trust How real-world deployments and attacks are shaping the future of Zero Trust strategies*.

Microsoft Azure. (n.d.). *What is the Cloud - Definition | Microsoft Azure*. Retrieved 31 January 2023, from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-the-cloud

NATO. (2013). *NATOTermOTAN*. https://nso.nato.int/natoterm/Web.mvc

NATO. (2022). *NATOTermOTAN*. https://nso.nato.int/natoterm/Web.mvc

Office for Research, E. and I. S. (n.d.). *Stockholm University's research integrity and ethics policy*. Retrieved 15 February 2023, from https://www.su.se/staff/organisation-governance/governing-documents-rules-and-regulations/research/stockholm-university-s-research-integrity-and-ethics-policy-1.540778

Office of the Director of National Intelligence. (n.d.-a). *Members of the IC*. Retrieved 3 March 2023, from https://www.dni.gov/index.php/what-we-do/members-of-the-ic

Office of the Director of National Intelligence. (n.d.-b). *What is Intelligence?* Retrieved 12 February 2023, from https://www.dni.gov/index.php/what-we-do/what-is-intelligence

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information and Management*, *51*(5), 497–510. https://doi.org/10.1016/j.im.2014.03.006

Olsson, K., & Strengbom, I. (2017, July 24). Turerna kring Transportstyrelsen – detta har hänt - Nyheter (Ekot) | Sveriges Radio. *Sveriges Radio*. https://sverigesradio.se/artikel/6741346

Palfy, A. (2015). Bridging the gap between collection and analysis: Intelligence information processing and data governance. *International Journal of Intelligence and CounterIntelligence*, *28*(2), 365–376. https://doi.org/10.1080/08850607.2015.992761

Peters, H. M. (2019). *The Department of Defense's JEDI Cloud Program*. https://go.usa.gov/xymbk.

Porrawatpreyakorn, N., Tangprasert, S., Nuchitprasitchai, S., Chaipunyathat, A., & Viriyapant, K. (2019). Understanding Key Enablers of Cloud Computing Adoption and Acceptance Over Time. *2019 Research, Invention, and Innovation Congress (RI2C)*.

Probst, Reed. R. (2006). Clausewitz on Intelligence. In R. Z. George & R. D. Kline (Eds.), *Intelligence and the National Security Strategist: Enduring Issues and Challenges* (pp. 3–10). Rowman & Littlefield.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *NIST Special Publication 800-207 Zero Trust Architecture*. https://doi.org/10.6028/NIST.SP.800-207

Runeson, P., & Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering*, *14*(2), 131–164. https://doi.org/10.1007/s10664-008-9102-8

SÄPO. (2022). *Underrättelsearbete - Säkerhetspolisen*. https://sakerhetspolisen.se/verksamheten/underrattelsearbete.html

Schaurer, F., & Störger, J. (2013). The Evolution of Open Source Intelligence (OSINT). *The Intelligencer Journal of U.S. Intelligence Studies*, *19*(3), 53–56. http://blogs.ethz.ch/osint/files/2010/08/nato-osint-handbook-

Secret Intelligence Service MI6. (n.d.). *SIS | About Us*. Retrieved 12 February 2023, from https://www.sis.gov.uk/about-us.html

Tweneboah-Koduah, S., Endicott-Popovsky, B., & Tsetse, A. (2014). Barriers to Government Cloud Adoption. *International Journal of Managing Information Technology*, *6*(3), 1–16. https://doi.org/10.5121/ijmit.2014.6301

Verma, G., & Adhikari, S. (2020). Cloud Computing Security Issues: a Stakeholder's Perspective. *SN Computer Science*, *1*(6). https://doi.org/10.1007/s42979-020-00353-2

Vetenskapsrådet. (2017). *God forskningssed*. Vetenskapsrådet.

Warrell, H., & Fildes, N. (2021, October 26). Amazon strikes deal with UK spy agencies to host top secret data: Cloud services to boost analytics Contract worth up to £1bn Security fears raised. *Financial Times*, 1. https://www.proquest.com/docview/2601746909/citation/EDD5BD10ABC2411FPQ/4?accountid=38978

Wulf, F., Strahringer, S., & Westner, M. (2019). Information security risks, benefits, and mitigation measures in cloud sourcing. *Proceedings - 21st IEEE Conference on Business Informatics, CBI 2019*, *1*, 258–267. https://doi.org/10.1109/CBI.2019.00036

Yin, R. K. (2018). *Case Study Research and Applications Design and Methods* (Sixth). SAGE.

Zwattendorfer, B., Stranacher, K., Tauber, A., & Reichstädter, P. (2013). Cloud Computing in E-Government across Europe A Comparison. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, A. Kobsa, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. P. Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, & G. Weikum (Eds.), *Lecture Notes in Comptuer Science* (Vol. 8061, pp. 181–195). Springer.

Appendix A Informed Consent Form

Adapted from Huskaj's (2017) consent form.

Informed Consent Form

Title of Project: Intelligence Agencies move to the Cloud: Challenges and Requirements
Researcher name: Karin Säberg
Contact details: kasa2167@student.su.se
Sponsoring organisation: Stockholm University

Part 1 Information Sheet

1. Introduction

The cloud and its ability to provide flexible and powerful computing capabilities is widespread in private organisations with government agencies starting to adopt them more. With the enormous amount of data and information being generated daily, and the increased use of open-source intelligence it is likely that intelligence agencies could benefit as well. However, this is not without issues as the cloud present unique challenges towards information security.

2. Purpose of the Research

The purpose of this study is to understand what challenges an intelligence agency face when moving to the cloud, and what information security requirements this puts on the cloud.

3. Type of Research Intervention

The data will be collected using semi-structured interviews estimated to take 90-120 minutes. The researcher will take notes during the interviews.

4. Participant selection

Personal contacts of the supervisor were used to find participants in possession of the needed experience and knowledge. No personal data will be collected during this research.

5. Benefits

The intelligence community is expected to gain much from this as it is the only research of its type, to the best of the author's knowledge, to interview experts within the Swedish Intelligence Community. No benefit will be provided directly to the participants.

6. Risks

No risks are associated with this study and the participant can withdraw their consent at any time, and no questions will be asked. The participant can choose to not answer questions at their discretion as well.

7. Use of data

The data is part of a thesis with the purpose listed in point 2. Data collected will be thematically analysed and made anonymous. Once the thesis is finished the data will be destroyed.

8. Confidentiality

Data will be anonymised, meta-data and any other potentially identifying information removed, and data will be filtered. If the participant wishes the signed Informed Consent form can be disregarded, however the Researcher is still ethically obliged to ensure that Informed Consent has occurred. In this case an unsigned copy of this document will be provided to the participant.

9. Security of the data

The data will be kept available only to the Researcher. Security can be further enhanced if needed by filtering information and correspondence deleted.

Part 2 Certificate of Consent

I confirm that I have read the Informed Consent Form for this study. I have had the opportunity to consider the information, ask questions and have these answered satisfactorily. I agree to take part in the above study.

Print Name of Participant	Date	Signature

I, Karin Säberg, confirmed that the Participant had the opportunities to ask questions about the research. If there were questions asked, I confirm that I answered correctly and to my best ability. I validate that the Participant was not forced into signing this consent form.

Print Name of Researcher	Date	Signature

1 copy for the participant, 1 copy for the researcher (original).

Appendix B Interview Form

1. Greeting, and thanks for taking part and being interviewed.
2. Explain the study:
    a. The information and data available to intelligence agencies increases daily, this requires both data storage and processing power, and the cloud could provide a solution to this.
    b. The purpose of the study is to understand what challenges this presents, and what information security requirements this puts on a cloud solution.
    c. The questions this study aim to answer are:
        i. What challenges do intelligence agencies face when adopting cloud solutions?
        ii. What information security requirements does this put on the cloud solution?
3. Informed Consent Form
4. Your answers will be anonymised through synthesis with the answer of the other participants. No references will be made to your name or other identifying information. Where citations are needed pseudonymization will be done, example: E1 (Expert 1).
5. The scenario concerns either the use of, or adoption of, cloud solutions to be used in the intelligence process, especially moving intelligence data to the cloud.
6. Before we start:
    a. You can choose to not answer any questions at your discretion.
    b. Do ask if you need a question clarified, or term.
    c. Any questions regarding the interview process?

Appendix C Interview Questions

General Questions

1. How many years have you worked, or been active, in the intelligence community?
2. Have you, or are you, currently working with a cloud computing solution? (Motive: understand their current experience with it)
3. Does this affect your view of intelligence agencies and the use of the cloud? (Motive: if their current experience affects their view, positively/negatively)

Technical Questions

Note: all of these are within the scenario of cloud computing use or adoption for intelligence agency use.

4. How does data security concerns affect a potential cloud computing adoption?
5. How do you view the risk of data loss and a cloud solution?
6. How do you view regulations and legal demands on cloud computing for intelligence use?
7. Consider the potential loss of control of data, how would you approach this?
8. What is your view on employee expertise regarding use of the cloud, both from normal users and the technical staff? And the need to manage and understand Service Level Agreements?
9. How would you consider the threat of compromised accounts and insider threats in the cloud compared to more traditional solutions? How do you view the threat of cloud service provider insiders?
10. How would you approach business continuity and service availability when using the cloud?
11. What is your view on data migration and potential lack of interoperability?
12. Consider the need for secure communications between the cloud solution and the user, how would you approach this?
13. How would you approach the cloud forensic need? (note: event logs category)
14. Do you consider the demands on user access control different on a cloud solution compared to a more traditional implementation? Why/why not?
15. Would you consider insecure APIs and interfaces for cloud solutions more prevalent than for non-cloud solutions?
16. How do you view the lack of knowledge about data location? How would you solve this?
17. Would you consider the potential lack of data segregation a security threat?
18. How would you approach necessary audits on a cloud solution?
19. Any final thoughts or additions?

Intelligence Questions

4. How does data security concerns affect a potential cloud computing adoption?
5. How do you view the lack of knowledge about data location? How would you solve this?
6. How do you view the risk of data loss and a cloud solution?
7. Consider the potential loss of control of data, how would you approach this?
8. How do you view regulations and legal demands on cloud computing for intelligence use?
9. What is your view on privacy regarding cloud solutions and intelligence use?
10. What is your view on employee expertise regarding use of the cloud, both from normal users and the technical staff? And the need to manage and understand Service Level Agreements?
11. What is your view on using cloud solutions for the intelligence process?
12. Would financial factors affect adopting a cloud solution? In what way?
13. How does your management reason about using cloud solutions? Or moving to the cloud?
14. What is your view on moving from data management to data governance?
15. How do you view the need for intelligence sharing and the cloud's impact on this?
16. What is your view on the potential information overload in the intelligence process?
17. What is your view on the potential processing gap in the intelligence process?
18. What is your view on using Big Data and AI in the intelligence process?
19. Do you think that intelligence agencies would move to cloud computing? Why, why not?
20. Are you aware of the CIA and GCHQ deal regarding use of cloud computing?
    a. If yes: What are your thoughts about these deals.
    b. And the implications?
21. Are you aware of any other intelligence agency use of the cloud? If possible, would you explain this use?
22. Any final thoughts or additions?

Appendix D Concepts Description and Concerns

Concept name and description based on research in Chapter 2. Used during interviews for consistency when defining concepts and terms.

Data security	Ensure that data is safe from breaches and unauthorised entities.
Data loss	Data is lost in some capacity by being unlinked from its context or otherwise inaccessible. Also includes the cloud service provider not being able to deliver services.
Regulation and legal compliance	How to comply with regulations and legal requirements when utilising the cloud. Includes issues such as not knowing the location of data leading to data protection concerns.
Loss of control	The cloud service provider manages and is in control of the data bringing up issues with data unavailability, confidentiality, and privacy.
Employee expertise	The employees need expertise to manage the cloud and Service Level Agreements (SLAs).
Compromised accounts and insider threats	Compromised accounts present a threat and risk. The accounts can have been compromised for any reason. Insiders within the organisation and cloud service provider also pose a threat.
Business continuity and service availability	The data should always be available to ensure the business can continue providing its services.
Lack of interoperability and portability	Potential vendor lock-in due to lack of interoperability and inability to easily migrate or connect alternative solutions.
Secure communications between cloud service provider and customer	Being able to access the cloud and the services provided securely.
Event logs	The cloud service provider needs event logs and investigative support to ensure that security incidents can be investigated.
User access control	Implementing appropriate user access controls and management, using principles such as least privilege and only using administrative accounts when needed.
Insecure APIs and interfaces	APIs and interfaces give access to cloud infrastructure and if poorly implemented can pose security risks.
Data location	Lack of knowledge where data is located presents data protection issues.
Data segregation	Improper data segregation between customers is a security concern. This concerns both cloud service provider customers and the organisation the service is being provided to.
Audits	The need to perform audits on systems, especially in the public sector makes it a security concern.
Big data and AI	The use and implementation of big data analytics and AI in the information process.
Privacy and legalisation	How privacy and legalisation impact both the intelligence process but also potential IT/cloud solutions.
Information sharing	Sharing information in the intelligence community, both within an agency and to others.
Data governance	How to manage the collected data, data management is the implementation of data governance.
Information overload	When the quantity of information overwhelms the analysts' ability to deliver results.
Processing gap	The gap between the information gathered and ability to analyse it.
Organisational readiness	How ready an organisation is to implement cloud solution, includes human knowledge and IT infrastructure, resources available and allocated.
Financial factors	Cost of migration compared to cost of operation, the potential cost savings.
Management commitment	Support from the top by resources allocation and process engagement

Appendix E Discussion on Related Research

Governments and the Cloud

Numerous studies on the topic of government adoption of cloud solutions exist and this section will consider a small fraction of these to further help create an understanding of the challenges and reasons faced by these agencies.

The challenges faced by governments looking to adopt cloud solutions, or evaluating the current state, are mainly in line with the security challenges found in 2.2.1 (El-Gazzar, 2014; Jones, 2015; Tweneboah-Koduah et al., 2014; Zwattendorfer et al., 2013). However, financial factors are noted as both pros and cons regarding public sector cloud computing adoption (Tweneboah-Koduah et al., 2014; Zwattendorfer et al., 2013).

In one case many of the security concerns in 2.2.1 had been mitigated, however security and privacy were still a key risk due to devices being lost or stolen and not immediately reported as such (Jones, 2015). In the same study management and staff commitment, and the development of new business processes was part of the successful cloud implementation.

Another study by Busch et al. (2014) examined the views of senior government IT managers in Australia on cloud adoption. Their findings show a willingness to adopt cloud solutions, but the survey results indicate that the question is rather *how* it should be done. It is worth noting that no questions were asked about challenges regarding the cloud only if the surveyors understood more about the usage of the cloud, and if they are more or less likely to adopt cloud solutions.

A similar study on the challenges of cloud computing adoption in Norway was carried out by El-Gazzar (2014) where the findings show similar results to the study by Tweneboah-Koduah et al. (2014) and discusses similar issues found in 2.2.1 regarding cloud security. El-Gazzar notes that Norway, despite not being part of the EU, is likely to be influenced by decisions made by it as a consequence of being part of the European Economic Area (EEA). She also discusses legal and privacy issues at length, bringing up the (at the time, yet finalised) GDPR (General Data Protection Regulation), and *safe harbour* agreements with the US, agreements that have since been nulled (Federal Trade Commission, 2016; International Trade Administration, 2020). One unique point El-Gazzar brings up is the use of cloud consultants to help the cloud adoption process to support the government agencies. The result of the study focuses on legislative and regulatory challenges with little to no insight regarding other challenges.

Liang et al.'s study (2017) identified five main categories, cloud trust, technology driving, cloud provider support, organisation readiness and environmental stimulus, as the main determinants towards cloud adoption in Chinese government agencies. They note the potential lack of generalisability due to different culture environments and government structure, however their findings appear to be in line with other research considered in this study. Included in the five main categories are sixteen subcategories, many which overlap with other studies' findings, especially the subcategories found in the environmental stimulus category, but also organisation readiness and technology driving. Environmental stimulus includes subcategories such as policy and regulations, industry standards, and financial funds, agreeing with the previous findings of Zwattendorfer et al.

(2013), Tweneboah-Koduah et al. (2014), and El-Gazzar (2014), raising the argument that their findings, it not in whole, at least in part can be applied on governments cloud adoption determinants outside of China.

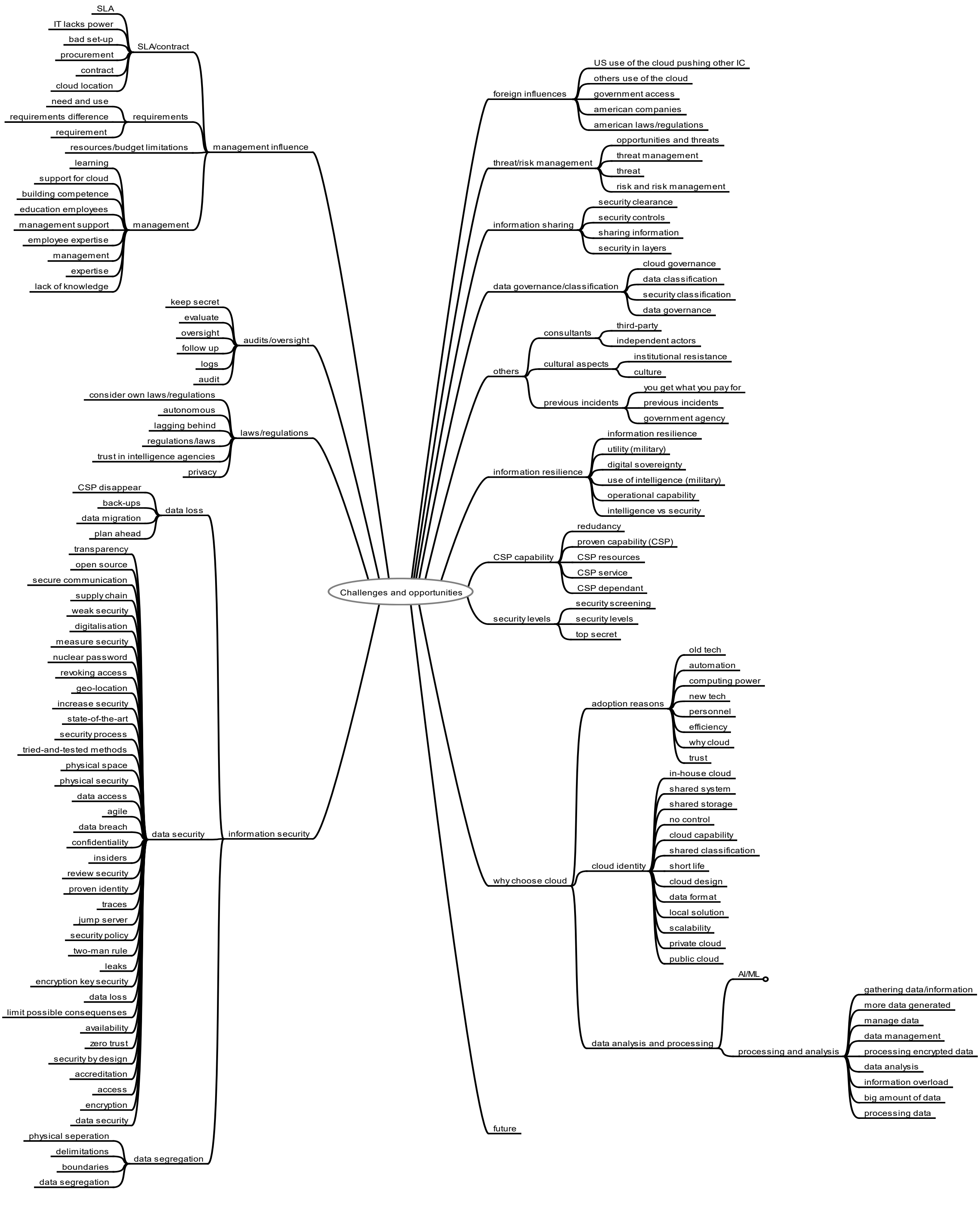
Military Cloud Computing

While research about public sector adoption of cloud computing solutions and its benefits and challenges are plentiful the research on the topic and military applications are less abundant. Most of the found literature on the topic concerned practical and specific security solutions or application of AI, something outside the scope of this study, with little about the general challenges and requirements regarding military use of the cloud, this can likely be attributed to, similarly to intelligence agencies, the need for secrecy and the closed nature of military organisations.

One of the most prominent examples of military use of the cloud is the US Department of Defense's (DOD) Joint Enterprise Defense Infrastructure (JEDI) program (Peters, 2019). The JEDI cloud solution is meant to unify and streamline currently used cloud services that are decentralised and hinders sharing of shared resources and data across the DOD. However, this program was cancelled in 2021, following this a new cloud solution was proposed, Joint Warfighting Cloud Capability (JWCC) (Jasper & Konkel, 2021), and was in December 2022, rewarded to AWS, Google, Microsoft, and Oracle (Konkel, 2022). Both these attempts show that the DOD is more than willing, and see a need, for the cloud capabilities to support their military operations. With the JWCC being, at the time of writing, recently announced there is little news, reports or otherwise reliable sources about it.

Another country using cloud solutions as part of their military operations is the Republic of South Korea, where the choice to move to the cloud is a response to "the nationwide distribution of numerous applications, wastage of budget and personnel resources and exposure to various disasters and security threats owing to insufficient infrastructure" (Cho et al., 2021, p. 1). While the solution is currently IaaS based the study argues that it needs to be expanded to SaaS and proposes a framework to migrate and manage military applications.

Appendix F Thematic Analysis Full Results



Appendix G Reflection Document

I believe that the goals have been reached well, the background was a challenge as there are none too few scientific sources on the topic and the word limit limited the possible discussion on related topics. However, I consider that with the resources available to me I overcame this.

The ethical aspects and potential consequences are, admittedly, hard to judge. Intelligence as a field is closed and shrouded in secrecy, it stands to reason that society may be untrusting of such an organisation and the information it may hold. And putting such information in the cloud, where, if managed poorly, anyone could access it is a risk. On the flip side, however, intelligence agencies are just as likely to not want any possible leaks or breaches and can be argued to be less likely to end up being a risk to citizens.

I have, during most of my studies admittedly, struggled with research strategy and method choice, especially why and which to choose. Case study is one I had a hard time grasping and arguing for it was something I found hard.

The planning went well; however, one interviewee could not be interviewed until late which caused delays. The data analysis also took longer than expected. Thankfully, my supervisor advised to schedule the thesis as if it is one less month than the actual time, which meant that even with these delays I have managed to finish near the planned date. Without more practice in research, it is hard to say what could have been done better, perhaps clearer requirements regarding my own deadlines towards the interviewees, though they provided me with a favour, and I feel this would not be a good solution.

One thing I have missed during this process compared to when I wrote my bachelor’s thesis is a partner to discuss with. While my supervisor has done his best and taken the time to provide feedback it cannot be compared to discussing with a peer writing the same thesis. I do believe that I may have missed out on valuable knowledge and reflections due to this and that I would, if I were to be in a position where I do something similar again, seek out feedback or discussions where possible.

A fair amount of my courses relates to this thesis, any of the ones that have brought up information security has been of use. The SIFU course provided basic understanding of the intelligence process which was helpful, the method and scientific writing courses of course provided valuable knowledge. The other courses have compounded over the years, and it is hard to name specific courses that contributed to this study.

I believe this thesis has helped, and will help, me in the future when working. It has allowed me a unique insight into intelligence agencies and their thought processes. While I do not think it directly affected it, I do think it piqued the interest of where I will be working after graduating.

Overall, I am really pleased with my thesis, it changed direction a bit towards the end and perhaps did not discover what I had first expected. But what I have learnt and having to consider the implications of some of my results have been a great experience. The final product is something I feel I can be proud in. Many of those I interviewed or otherwise discussed the topic of my thesis with expressed an interest in seeing the final results which to me shows a certain interest in the topic of the thesis, further highlighting that it may be unique and provide something of value in the scientific and intelligence field.