Intelligence Agencies' Move to the Cloud: Challenges and Opportunities

Karin Säberg[1] and Gazmend Huskaj[1,2]
[1]Department of Computer and Systems Sciences, Kista, Sweden
[2]Geneva Centre for Security Policy, Geneva, Switzerland

karin.saberg@gmail.com
g.huskaj@gcsp.ch

Abstract: The purpose of this research is to discover more about the challenges and opportunities faced by intelligence agencies wishing to move their data to the cloud. Intelligence agencies collect and process enormous amounts of data and information and need the tools to do so. Two intelligence communities have moved to the cloud to face these issues but there is little scientific knowledge about moving an intelligence agency's data to the cloud. No research on the topic could be found and this study aims to fill part of that gap by using a case study research strategy and interviews with experts in the field. A literature review was completed to understand previously identified challenges when adopting cloud and was used to create two sets of interview questions. Five interviews were conducted, and a thematic analysis done resulting in fourteen themes. The themes revealed that there are many challenges with laws and regulations being the biggest one, while the opportunities brought by a cloud solution are the processing and analysis of data, and information sharing.

Keywords: Intelligence, Intelligence agency, Cloud, Cloud computing, Information security

1. Introduction

Intelligence agencies use multiple intelligence-collection methods: Human Intelligence, Signals Intelligence, Imagery Intelligence, Measurement and Signatures Intelligence, and Open-Source Intelligence (OSINT) (FBI, n.d.; MI5, n.d.; SÄPO, 2022). Of these, open-source intelligence is of growing 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). It concerns collecting data from "publicly available information, as well as other unclassified information that has limited public distribution or access" (NATO, 2013). SÄPO (2022) exemplifies OSINT using the internet, newspapers, radio and tv.

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). To accomplish their goals, intelligence agencies face two challenges: the "handling" (discovery, access, analysis, sharing) of the data and related security. To tackle these issues, the Central Intelligence Agency (CIA) employed cloud solutions for all 17 United States intelligence agencies (Konkel, 2014).

The deal was for Amazon Web Services (AWS) to provide this solution for ten years. The CIA reached a new agreement 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:

> *"[…] the cloud on its weakest day is more secure than a client service solution", and government organisations are desperately trying to upgrade legacy information technology (IT) systems (Corrigan, 2018).*

The scientific literature reveals scarce research on the topic, covering the US and UK's intelligence communities (Konkel, 2014; Konkel, 2020; Warrell & Fildes, 2021). None provide in-depth information about an intelligence agency's decision processes, challenges, (security) requirements and practical solutions. The most extensive study on the subject is a paper by Horlings (2022) discussing using computer science tools as part of the intelligence process. However, even she does not mention cloud solutions despite the verbatim mention of "scalable architecture for efficient storage, manipulation, and analysis" (Horlings, 2022, p. 13), a description that corresponds to cloud computing.

As such, there are issues with how to approach information security and the potential resistance to moving to the cloud. Facing these issues and understanding what intelligence agencies need to consider adopting cloud solutions requires additional research.

Specifically, this study considers the following research questions:

- What challenges do intelligence agencies face when adopting cloud solutions?

- What opportunities does a cloud solution bring to an intelligence agency?

This study aims to discover intelligence agencies' challenges in moving to the cloud. However, this research will also explore opportunities in using the cloud, which would also likely bring opportunities, such as tools and solutions benefitting their work.

2. Methods and Materials

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.

Using a case study research strategy with interviews as data collection method five experts in the field of intelligence agencies and the cloud were interviewed. Runeson and Höst (2009) proposes a five-step process when conducting a case study which was followed. The steps are as follows:

1. Case study design – plan the study and research.
2. Preparation for data collection – literature review leading to conceptualising and interviews based on these. Reviewed Denscombe (2014) and Yin (2018) for case study design.
3. Collecting evidence – semi-structed interviews circa 90 minutes long with experts in the field.
4. Analysis of collected data – thematic analysis according to Braun and Clarke (2022) and Denscombe (2014).
5. Reporting – writing the paper.

2.1 Data Collection

Purposive sampling and semi-structured interviews were used to collect data from experts in the field chosen based on their knowledge and experience in the intelligence community and their availability to participate. The experts have at least 10 years of experience, and varying degrees of experience with cloud solutions, either in research for intelligence purposes, procuring, or developing cloud solutions. Four of the interviews were performed in person and one using Zoom, and two of the interviews were recorded with consent. The interview questions cover two main themes: intelligence and technological aspects of moving an intelligence agency's data to the cloud. The two sets of interview questions were based on the concepts found in table 1 and 2, with some overlap between the two.

Experts 1, 2 and 5 were asked the intelligence questions, and experts 3 and 4 the technical questions. As the literature review revealed that technical challenges when moving an organisation's data and processes to the cloud are largely the same or similar independent on the user and purpose of the cloud, while challenges faced by intelligence agencies are nearly completely unaddressed. Thus, the need to understand the intelligence community's view on challenges on cloud solution adoption is in more dire need than addressing an already well-researched area. As such one more interview was performed to explore this specific aspect.

2.2 Data Analysis

A qualitative thematic data analysis was performed on the data, following a five-step process proposed by Denscombe (2014, pp. 247-248), and using Braun and Clarke (2022) for a deeper understanding.

The five-step process by Denscombe (2014) is described in Table 3.

Table 1: Overview of Data Analysis Process and its Application

Step	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	Present final iteration

Step	Step Five-stage data analysis	Application in this study
	with quotes, use visual means of presentation,	themes
5	Validation of the data – Data and method triangulation, alternative explanations comparison.	Compare to previous research etc.

Using Taguette, an open-source tagging tool, to complete the first iteration of coding, 151 codes were identified. The codes, with the relevant text, was printed and sorted into 24 categories, during this process one code was discarded as irrelevant. The 24 categories and 150 codes were next entered into FreeMind, a mind mapping tool, and sorted into themes. A total of 14 main themes were identified during this process.

3. Results

The results of the thematic analysis, depicted in Figure 1, show 14 main themes which will be explained here. While some are in line with previous research, others are not. The themes identified, in no specified order, are as follows:

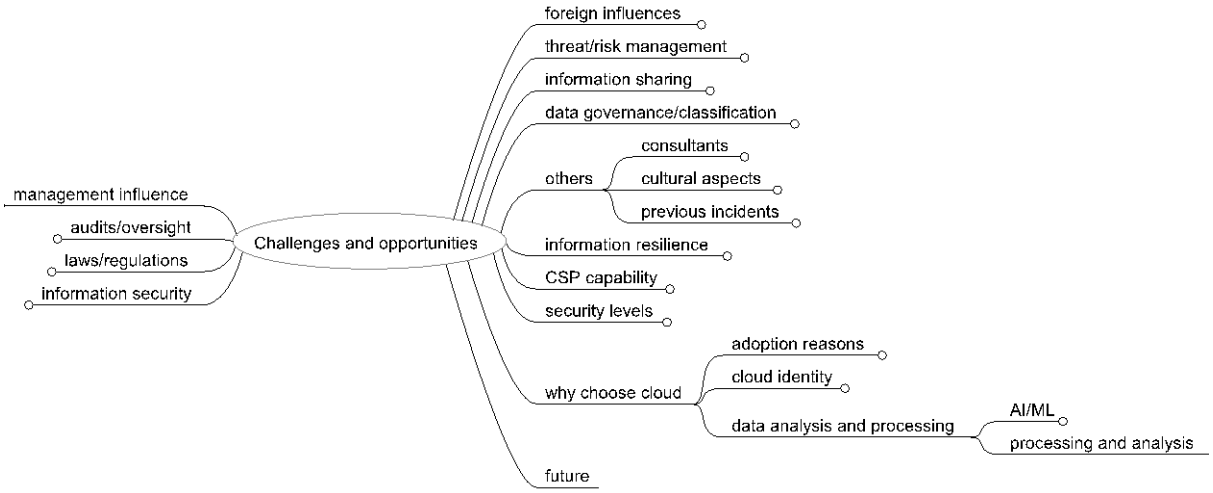

Figure 1: Thematic Analysis Results, with some sub-themes. Note: CSP = Cloud service provider, *Security levels* is renamed to *security clearance level* in the text

3.1 Management Influence

This theme explores management's role and influence on cloud adoption and usage. It covers Service Level Agreements (SLAs) procurement, requirements, budgeting, and resource allocation. The experts we interviewed were divided on SLAs. While one expert believed in existing expertise, two others noted for improved "contractual capacity." These experts felt that those managing SLAs and contracts often lack the legal or technical competence.

Management should consider internal and external requirements and understand how to measure the usage requirements for cloud solutions. Initial resource allocation and budget for cloud transition was a highlighted concern.

A significant issue is the management's lack of knowledge about cloud solutions, their internal workings, and what using one means for an intelligence agency. Management must close their knowledge gap before real cloud solution adoption can start. This is currently a hurdle, and the experts noted that change comes from the top.

3.2 Audits/Oversight

The necessity for audits remains unchanged from existing solutions. However, a cloud solution could likely make oversight easier. Because both audits and oversight trace actions in the system, it also relates to the contractual and SLA-aspects discussed under the management influence theme. SLAs and contracts should support audits and logging tools to a sufficient degree.

3.3 Laws/Regulations

Laws and regulations often lag behind the technological and digital evolution, and both national laws and regulations, as well as EU law like GDPR must be adhered to. The experts noted that Swedish government agencies are often very autonomous and may have different regulations regarding cloud usage, further complicating the issue. Also, regulations and laws regarding secret and top secret classified information are unclear, and does not support cloud usage at all, meaning that the full potential of a cloud cannot be utilised if not all necessary information can be put in a cloud solution. According to the experts, even though changes to legislation is being made, it is slow and is not keeping up with the needs.

3.4 Information Security

This theme covers many aspects of information security, like best practices, processes, information security principles, and risks with new technologies. The experts agree following best practice recommendations and staying up to date with current technologies. Encryption was mentioned as a possible solution to manage information security risks, which also requires relevant processes to manage encryption.

Information security principles include zero trust environments, two-men rules, and least-privilege access. This were reoccurring practices mentioned by the experts as ways to ensure security.

Risks include new technologies and methodologies: they should not be used until tried and tested. Additional risks include the cloud-specific data segregation issue. Although a benefit of the cloud is the use of shared resources, this is not always good for an intelligence agency: it needs to be strictly managed through data segregation to ensure the security and secrecy of information. This also limits cloud usage possibilities.

3.5 Foreign Influences

Concerns were raised adopting and using cloud solutions: foreign actors can leverage these solutions to increase their influence. Mostly US government and US companies were in focus that the US government can demand access to US company data, and by extension, their customers. One expert expressed a concern of government's right to access data versus their actual ability to do so.

There are further issues with more entities adoption cloud solutions putting pressure on those who have not to be able to keep up in the international intelligence community. Four of the experts also expressed concerns about being denied access to data if a foreign cloud service provider were to be used. However, the main concern in this theme is the legal issues present in using a US cloud service provider and the security issues this brings.

3.6 Threat/Risk Management

Intelligence agencies need to take risks and balance threats and opportunities, a reoccurring topic. The experts argued that it's impossible to have a zero-risk approach using a cloud solution and vulnerabilities do exist. Therefore, to utilise these Internet-based tools, threats and opportunities must be well-balanced.

3.7 Information Sharing

Information sharing within a country's intelligence community, and between different countries' intelligence communities, is of importance. The experts indicated that information sharing would be easier using cloud solutions and may likely become a necessity in the future. Furthermore, intelligence reports are being shared today, but in the future, by using the cloud, data rather than reports may be shared. Providing access to data requires appropriate security controls to ensure that the right people have access to the right data at the right time. Cloud solutions can provide the tools to control information sharing and who has access to what, and reduce the risk of missing critical points and data spreading.

3.8 Data Governance/Classification

Governance, and a unified and same classification system is needed if multiple agencies were to use the same cloud solution. The interviews revealed that intelligence agencies and communities use different security and data classification schemes: different classifications may be of the same kind, or the same data may be classified differently. Not only that, but the same information may have different data security levels. This poses challenges to information sharing as well as using the same cloud.

3.9 Information Resilience

Information resilience was noted by one of the experts as an important factor for intelligence agency's use of the cloud, especially the military. Information resilience is about having the capability to continue working during crisis and war. The cloud can be an important tool for this. Unbound by physical laces that can be destroyed, military capability is ensured no matter where people are and their situation. This also includes sovereignty, a nation's ability to control its digital tools and data (Couture & Toupin, 2019; Floridi, 2020).

3.10 Cloud Service Provider Capability

Cloud service provider capability is important. In particular, the ability to deliver on data and information security, and redundancy. A lot of resources, especially staff, are needed to manage self-hosting solutions. The experts noted that if the US, with far more resources than most governments, opted for a cloud solution rather than self-hosting, then this indicates that the needs and requirements are far too cumbersome for smaller countries. Here, cloud service providers have resources to handle any potential issues. However, cloud service providers have different services and locking oneself to cloud-specific solutions can turn into issues further down the road, which is why the capabilities and services of cloud providers should be considered carefully.

3.11 Security Clearance Levels

Organisations handling data, information and intelligence related to national security value security clearance levels. Therefore, when choosing and planning for a cloud solution, those responsible should implement, plan, and consider how to manage security clearance levels for data and information. This becomes even more important if multiple intelligence agencies and government bodies share intelligence. The aim is to classify data and information correctly and to address some of the personnel security clearance. However, security clearance is (presumably) already well practiced and is not an issue specific to cloud-solutions.

3.12 Why Choose the Cloud?

Here, the reasons, benefits and challenges are presented. The findings show that intelligence agencies currently use old and slow tools. The reasons to adopt a cloud solution include, automation, speeding up work by utilising more efficient tools, sharing systems, resources, scalability, data format, different deployment models (community, hybrid, private, and public clouds), and similar benefits. Choosing a cloud solution provides important technical advantages, the most important being data processing and analysis. The experts noted that information overload has always been an issue for intelligence agency. Utilising a cloud to automate and speed up data processing and analysis can mitigate information overload.

The experts raised their concerns on using machine learning (ML) and artificial intelligence (AI) to make decisions without proper human oversight. Although ML and AI speed up data processing and analysis, human oversight and checks in place are needed to reduce these concerns.

3.13 Future

This theme is unique compared to the rest. While the other themes touch upon more specific challenges and opportunities, the findings suggest that the cloud is the future for Intelligence communities, partly because of the themes already covered above, but more so the opportunities the cloud brings organisations, especially one that handles massive amounts of data like an intelligence agency. The need to process and analyse vast amounts of data requires the appropriate tools, and cloud computing is such as tool. And this is nothing new.

One expert noted that Google, for example, is already using the cloud for intelligence purposes. They process and analyse their data through cloud computing to predict our needs to direct advertisements. What is this, if not intelligence? And it is correct. Google uses the cloud to produce intelligence about their customers to direct advertisements to them: the cloud is part of an intelligence process. Therefore, this is already happening every minute and day and is a possibility with the cloud, an argument to consider well before dismissing it.

3.14 Others

This theme combines three topics: consultants, cultural aspects, and previous incidents. The experts mentioned consultants as sources of risk and opportunities. Third-party and independent actors can bring valuable services such as audits. Cultural aspects in an organisation were possible challenges towards cloud adoption, but some groups support the cloud and would like to see it used.

A potential challenge to cloud adoption was previous incidents; there have been some cases where Swedish government agencies have attempted to adopt cloud solutions which have failed. 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.

4. Discussion

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 (Alouffi et al., 2021; Balani & Varol, 2020; Bhajantri & Mujawar, 2019; Butt et al., 2022; Wulf et al., 2019) 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 such as the lack of interoperability and portability was found in previous research (Alouffi et al., 2021; El-Gazzar, 2014; Jones, 2015; Verma & Adhikari, 2020; Zwattendorfer et al., 2013), 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/regulation theme. Previous research (El-Gazzar, 2014; Horlings, 2022) 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. Conclusions

This study aimed to answer the following research question: What challenges do intelligence agencies face when adopting cloud solutions? And the following sub-question: What opportunities does a cloud solution bring to an intelligence agency?

The main finding of this study is that laws and regulations are the biggest challenge for intelligence agencies moving to the cloud. This challenge is beyond the direct control of the intelligence community, as it depends on the legal frameworks of different countries and jurisdictions. Local laws may restrict the use of cloud services, while foreign laws, especially those of the US, may pose a threat to the security and privacy of the data stored in the cloud.

The main benefit of a cloud solution for intelligence agencies is the enhanced analytical and processing capabilities, as well as the potential for information sharing and collaboration. These advantages may outweigh the risks of cloud adoption, if the risks are properly managed and mitigated. However, this requires a high level of technical expertise and organisational readiness from the intelligence agencies and their partners.

This study contributes to the literature on intelligence agencies that wish to move to the cloud by exploring the specific challenges and opportunities faced by intelligence agencies in this domain. It also highlights the gap between the technological and legal requirements of cloud adoption, which is often caused by the lack of appropriate technical knowledge among the lawmakers and regulators.

A possible direction for future research is to investigate how this gap can be bridged, and how the legal frameworks can be updated and harmonised to facilitate the use of cloud services by intelligence agencies, while ensuring the protection of their data and interests.

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. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1–4). https://doi.org/10.1109/ISDFS49300.2020.9116266.

Bhajantri, L. B., & Mujawar, T. (2019). A survey of cloud computing security challenges, issues and their countermeasures. In Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019) (pp. 376–380). https://doi.org/10.1109/I-SMAC47947.2019.9032545.

Braun, V., & Clarke, V. (2022). Thematic analysis. SAGE.

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.

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 (5th ed.). Open University Press.

El-Gazzar, R. (2014). An overview of cloud computing adoption challenges in the Norwegian context. In Proceedings - 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014 (pp. 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.

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 January 30, 2023, from https://usnwc.libguides.com/c.php?g=494120&p=3381426.

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.

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

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.

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.

Koç, B., Şener, U., & Eren, E. P. (2022). Determinative factors of cloud computing adoption in government organizations. In 2022 3rd International Informatics and Software Engineering Conference (IISEC). https://doi.org/10.1109/IISEC56263.2022.9998286.

Konkel, F. (2014). 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). 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/.

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. Parachute. https://parachute.cloud/cloud-computing-statistics/.

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

NATO. (2013). NATOTerm. https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en.

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.

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.

Porrawatpreyakorn, N., Tangprasert, S., Nuchitprasitchai, S., Chaipunyathat, A., & Viriyapant, K. (2019). Understanding key enablers of cloud computing adoption and acceptance over time. In 2019 Research, Invention, and Innovation Congress (RI2C).

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. Retrieved from https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf.

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.

Warrell, H., & Fildes, N. (2021, October 26). Amazon strikes deal with UK spy agencies to host top secret data. Financial Times. 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. In Proceedings - 21st IEEE Conference on Business Informatics, CBI 2019 (Vol. 1, pp. 258–267). https://doi.org/10.1109/CBI.2019.00036.

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE.

Zwattendorfer, B., Stranacher, K., Tauber, A., & Reichstädter, P. (2013). Cloud computing in E-government across Europe: a comparison. In Technology-Enabled Innovation for Democracy, Government and Governance: Second Joint International Conference on Electronic Government and the Information Systems Perspective, and Electronic Democracy, EGOVIS/EDEM 2013, Prague, Czech Republic, August 26-28, 2013, Proceedings 2 (pp. 181-195). Springer Berlin Heidelberg.