INFO FLASH
Finabel
European Army Interoperability Centre

FINABEL - THE EUROPEAN ARMY INTEROPERABILITY CENTRE

JANUARY 2023

OUTSOURCING THE CLOUD: CROSS-BORDER PUBLIC-PRIVATE PARTNERSHIP AND EUROPEAN INTEROPERABILITY FOR CLOUD INFRASTRUCTURES

WRITTEN BY
TOM MANTELET

EDDITED BY
JAMES EDWARD COLOMBO

Introduction

In the past decade, the cyber domain, or cyberspace, has become the most challenging and pressing issue of recent times in the area of international security. In an ultra-connected world, where information travels at an uncontrollable rate and data is becoming the new resource to be mined; it ultimately affects every aspect of modern life. From the economy to civil liberties, it has become the new focus of national security strategies and legal frameworks.

Governments have adopted national cyber-security strategies to protect the physical layer of the cyber environment. The protection of physical cyber-infrastructure and the cyber-physical effect was the primary focus of an attempt to limit the impact a cyberattack would have in the real world. This cyber-physical effect refers to the impact of the cyber environment on human life.

However, nowadays, the Internet of Things (IoT) and the quest for digitalization makes this layer even harder to establish. Whereas cybersecurity is mainly perceived as the preservation of critical infrastructure from cyber threats, the interconnectivity of modern technologies in daily life enters into the domain of personal online privacy or personal data (Carr, 2016).

Modern countries have adopted this digitalization and are running many of their national institutions through the internet. It has completely revolutionized modern societies and bureaucratic state systems. For example, it is now possible in some countries to vote online, check your medical records, ask for bank statements or subscribe to insurance.

When looking at the Covid-19 pandemic, digital tools were extremely important for modern society. Both public and private institutions have greatly increased their digital activity to keep functioning properly and adapt to the crisis. Most of these transformations exist because of Cloud technology, which allows to stock and host of data from institutions, citizens, and private companies.

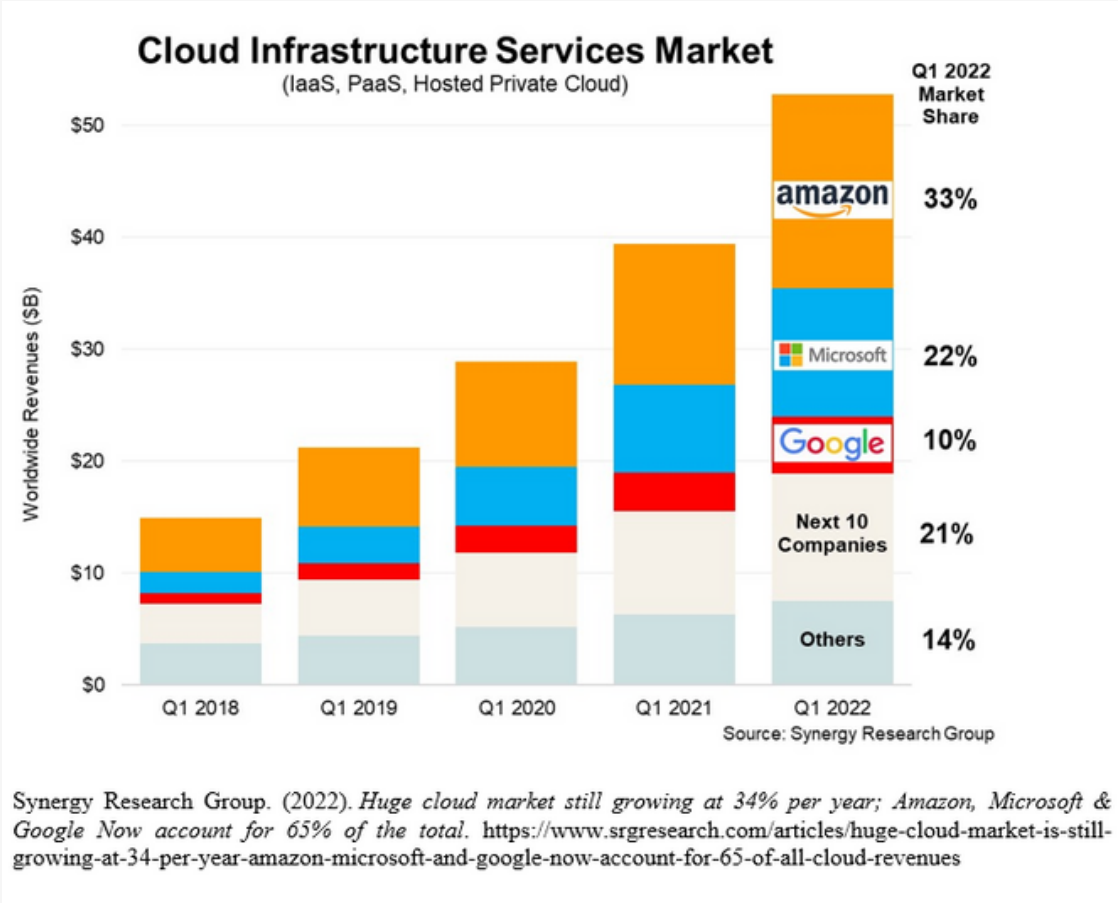
In this sense, the national Cloud is greatly attached to national economies, public health and even security making it a key critical infrastructure (virtual or physical) that, if destroyed, would have a tremendous impact on a nation's ability to function correctly (Carr, 2016). A national Cloud is a Cloud used at the national level by the government, answering to a specific label designed by a national security doctrine, to digitally run institutions.

This search for digitalization requires certain capabilities, transformations and knowledge that could take time to implement. Nonetheless, in the Cloud domain, this problem can be answered through public-private partnerships. Even though this approach could be seen as controversial due to the distinct objectives of the public and private sectors, this model could also be highly functional and provide a sustainable answer to the development of a national Cloud.

When it comes to national security, a public-private partnership in this domain is always a sensitive subject, especially regarding questions of responsibilities and accountability (Carr, 2016). Regarding Cloud technology and data protection, most countries have specific laws to safeguard their citizens' data privacy which needs to be coupled with the private sector modus operandi.

As Cloud technology is expected to increasingly become part of everyday life in most areas of modern society, it is believed that public-private partnerships will flourish in this domain, as both sectors will adapt to this exponentially growing demand and marketplace.

If we look at the current biggest Cloud providers, the US remains first, with Amazon Web Services, Microsoft and Google representing 65% of 2022 Cloud infrastructure service world market shares (Synergy Research Group, 2022). The rest is also divided among other US-based companies such as Oracle or IBM, but also the Chinese company Alibaba.



Synergy Research Group. (2022). *Huge cloud market still growing at 34% per year; Amazon, Microsoft & Google Now account for 65% of the total.* https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues

This hegemony in Cloud infrastructures gives the US significant power in shaping the marketplace and creates a new dimension to the public-private partnership by exporting national cyber laws. For example, if a country wants to build Cloud infrastructure, it could partner with a US Cloud provider such as Amazon Web Services; however, the US has specific legal framework regarding data protection or access that can differ from other countries, for example, the 2018 CLOUD Act. According to the special circumstances outlined by the Act, the US government would have access to another country's data. On the other hand, some countries have regional and national safeguards to protect their citizens against such intrusions, such as the European Data Protection Board (EDPB). Therefore, how can multinational public-private partnerships be successfully implemented in the European Union, in respect of national laws and data privacy regulations, to build national Cloud infrastructures? To what extent these partnerships are possible?

This research will use the cross-border public-private partnership between France and Google/Thales to build the future Cloud de Confiance for French institutions and companies. The scope of this research will be based on the European Union and French data protection regulations against the United States 2018 CLOUD Act. This paper will be constructed around three main points. Firstly, a presentation of what Cloud networks imply about public-private partnerships according to the US 2018 CLOUD Act and the EU General Data Protection Regulation (GDPR). Secondly, this paper will examine the Google/Thales partnership designed to construct a French Cloud network and its resonance with the EU GDPR, to accommodate French National Strategy (Gouvernement, 2021) for the Cloud. Thirdly, by using the example of the Google/Thales French Cloud, this paper analyses how such a complex partnership can function and build trust between the private and public sectors. In conclusion, this study intends to draft policy recommendations for the Cloud, building public-private partnerships in the European Union, exploring sovereignty, European interoperability, domestic regulations and risk awareness.

Theoretical Background

What is the Cloud?

The Cloud is not a physical entity but rather a global network of servers which are operating as a single ecosystem. There are currently four types of Cloud computing systems: Private Cloud, Public Cloud, Hybrid Cloud and Multi-Cloud (Microsoft Azure, 2022). For this research, the Hybrid Cloud definition will be used. Hybrid Cloud refers to "a type of cloud computing that combines on-premises infrastructure—or a private cloud—with a public cloud" (Microsoft Azure, 2022). Hybrid clouds allow data and apps to move between the two environments, in other words, "organizations gain the flexibility and innovation the public cloud provides by running certain workloads in the cloud while keeping highly sensitive data in their own datacentre to meet client needs or regulatory requirements" (Microsoft Azure, 2022).

The most important feature the Cloud technology provides is data and systems redundancy, or the act of duplicating copies of your data, systems, and equipment to have an infinite number of safe backups in case user data is threatened. In this sense, Cloud technology provides both the flexibility and the security necessary for public or private organizations to operate their services freely.

Public-private partnerships in cyberspace

Governments are currently evaluating cyberspace as a matter of national security. It is also clear that the rapid evolution and demand for Cloud infrastructure cannot be answered by the public sector alone. Public-private partnerships need to be monitored through laws and regulations to serve national security interests and protect the users. On the other hand, the question of whether national security is too important to be given to cost/benefits-driven organizations as Cloud network providers remains a significant issue to resolve.

It seems that in the case of Cloud computing services, the interests of the public and private sectors can be aligned as a more secure network would bring trust and, therefore, customers. Of course, a 100% alignment of interests is almost impossible, therefore they are usually governed by regulations (Carr, 2016). In the case of Cloud providers, they mostly abide by US regulations whilst nevertheless operating worldwide. It is of vital interest for any public-private partnerships made with these Cloud giants to ensure they abide by the rules and regulations where all gaps must be filled to comply with domestic norms.

Cross-border public-private partnership can be defined as a partnership between two private organizations from two separate countries with one public actor. One issue it presents concerns the nature of the cooperation between the two sectors, as well as to whom the private sector is answering, especially in a cross-border public-private partnership. In the following case study, such a partnership is presented that includes Google, a US-based company, and Thales, a French-based company, building a hybrid Cloud (S3NS) for France (Thales, 2021), under its national Cloud strategy. This unique relationship is challenging the national security policies of both the United States and France and shows how a state is equipped or ready to answer such a challenge (Carr, 2016).

The 2018 CLOUD Act

The CLOUD Act was enacted in 2018 in response to a Supreme Court pending case regarding US-based provider-stored emails in Ireland (Evans et al., 2019).. The provider refused to give access to the stored emails because they claimed that the US request stopped at the US border (Evans et al. 2019). Therefore, the CLOUD Act was meant to solve this issue by extending access to all emails, or data, regardless of their location in the world if subject to a criminal warrant. Moreover, the United States found the process of data gathering, in the case of criminal prosecution, too slow through the Mutual Legal Assistance Treaty (MLAT) signed with other countries (Evans et al. 2019). To sum up, if a US court were to issue a criminal warrant to access data stored abroad by a US-based Cloud provider, following executive agreements between the United States and the other country, the United States justice department can access this data.

From this point of view, the CLOUD Act sounds more like judicial cooperation between states. However, as previously mentioned, the biggest and most developed Cloud providers are US-based companies. In the case of a public-private partnership with these companies, the country contracting a US-based Cloud provider must comply with the CLOUD Act.

The CLOUD Act underlines some important issues in which Cloud technology is becoming a matter of national security. Furthermore, the warrant is issued by a United States court order, and as such it is a possibility that Cloud service providers “face a conflict between complying with US laws and personal data protection” required by a specific region or country in which it operates (Evans et al. 2019). This conflict can be observed in the EUGDPR.

European Data Protection and General Data Protection Regulation

The European Union is heavily focused on regulating data protection and data privacy. Therefore, the European Data Protection Supervisor (EDPS) and European Data Protection Board (EDPB) regard CLOUD Act's privacy protection as too lenient for European citizens (Evans et al. 2019). According to Article 48 of the European Union GDPR (2016):

"Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State"

However, the CLOUD Act has been enacted to shortcut the MLAT regarding the transfer of personal data. In this aspect, it is conflicting with EU data privacy regulations and EU laws. Therefore, according to Article 6 of the GDPR, a transfer of data could be done through MLAT but not on the basis of the CLOUD Act (GDPR, 2016). Furthermore, other derogations presented in Article 49 of the GDPR would allow data transfer for matters of public interest or vital interest but also if the data owner agrees to the transfer (GDPR, 2016).
Overall, the GDPR aims to protect EU citizens from potential violations of their data and safeguards their rights against non-MLAT requests such as stated in the CLOUD Act.

When attached to a private-public partnership, it is important to well understand the implications of data privacy regulations in each country involved in the partnership. This specific relationship will be explored in the cross-border public-private partnership case study of Google-Thales-France in building the next national Cloud de Confiance.

Case Study: S3NS Google-Thales Partnership and the French National Strategy for the Cloud

The French National Strategy for the Cloud has been drafted by the French government in May 2021 to answer to the rapid growth and demand for Cloud technologies in France. For France, the Cloud strategy is built around three major points of integration: the transformation of French public administrations and companies, digital sovereignty and economic competitiveness (Gouvernement, 2021). Through this approach to the Cloud, France aims at protecting the data of its companies, administrations and citizens while affirming its sovereignty in the domain.

In its strategy, France has issued a new label named "Cloud de Confiance" or SecNumCloud (Gouvernement, 2021). This new label aims at directly targeting data privacy and security for its users. This type of securitization operates both at the technical level , with safe and secured technology, and judicial levels. From the perspective of a public-private partnership with an extra-territorial and non-European company, the judicial measures are intended to protect the Cloud from risks regarding the application of extra-territorial laws that fail to conform with European values (Gouvernement, 2021).

Therefore, the label Cloud de Confiance would merge foreign Cloud technology with European or French legal control to answer the three following conditions (Gouvernement, 2021):

- To answer the security requirements and norms.
- To locate and operate Cloud infrastructures in France or Europe.
- To ensure operational and commercial management and delivery by a European entity, owned by European actors.

In November 2021, US-based company Google and the French company Thales announced the creation of a strategic partnership to codevelop and implement hybrid Cloud technology and infrastructures in France, respecting the SecNumCloud label (Thales, 2021). This project will be used by French public institutions and French companies that could benefit from its flexibility, power, security, and sovereignty, answering to all the requirements fixed by the French National Agency for the Security of Information Systems (ANSSI) and the European Union GDPR (Thales, 2021).

In this partnership, Google Cloud will bring the Cloud architecture, innovations, technologies, and power. On the other hand, Thales will guarantee French sovereignty by managing the encryption and access in close cooperation with the French Operational Centre for Cybersecurity (Thales, 2021). Therefore, Thales will ensure the necessary trust, security, and data privacy of the Cloud users (Thales, 2021).

Following the conditions expressed by the France's National Strategy for the Cloud, French public institutions and private companies could benefit from the S3NS because this one will operate under a new society answering to French regulations and laws that will be majority-owned by Thales. Furthermore, all the services offered by the S3NS in France will be hosted in the country in an infrastructure separated from Google Cloud's network and servers.

Regarding the continuous updates from the system, Thales also guarantees the evaluation and validation of these updates under a security protocol piloted by Thales itself (Thales, 2021).

A Quest for Autonomy and Sovereignty?

On paper, the Google/Thales-France partnership appears to be bulletproof regarding data privacy and national data protection. As published in its National Strategy for the Cloud, France emphasizes the key role its Cloud de Confiance will have on the economy, autonomy, and sovereignty. Every aspect of this partnership, legal and technical, have been built to counter the 2018 CLOUD Act and delivers adequate data privacy to the users. Of course, as stated in the EU GDPR, it is still possible to obtain derogations to access specific data in cases of criminal investigations, but in such instances will be subject to a well-examined request through a Mutual Legal Assistance Treaty and not as part of the CLOUD Act.

However, the fact of contracting a foreign company to build a hybrid Cloud that will be used at the core of your national institutions, citizens' engagement in the society and economic competitiveness could bring an additional concern on whether autonomy and sovereignty have been reached. In the short term, this partnership appears as the perfect solution to answer the rapid demand for digitalization. Nevertheless, in the long run, such partnership remains full of uncertainties.

The first concern would be the transfer of technology. In every partnership, especially when involving complex technologies, the transfer of technologies and capabilities is a matter of discussion. To operate the Cloud while respecting every regulation imposed by France and the European Union in terms of data control and data privacy, Google Cloud needs Thales. On the other hand, to distribute a powerful, constantly updating and high-performance Cloud technology, Thales needs Google Cloud. For the time being, it seems that both private companies' interest leans in the same direction. However, if the goal mentioned under the French National Strategy for the Cloud is to reach autonomy and sovereignty in this matter (Gouvernement, 2021, 4) this partnership does not disclose any transfer of technology that would allow France to operate its "Cloud de Confiance" alone. Thus, it suggests this partnership will continue in the future. So far it does not present a real issue except that it does not grant France all the technological autonomy and sovereignty it requested. On the other hand, it is unsure if France would possess the resources to build a national Cloud on its own without outsourcing a part of it to a foreign private actor.

The second issue refers to the high stakes of such a partnership. Both Thales and France revealed the purpose of the national Cloud and to what extent it will be used. Contrary to the usual public-private partnerships that can be observed in the context of national security, the Cloud would be considered part of the extremely critical infrastructure when it will be implemented in all sectors of French industry and institutions. In the matter of cybersecurity, it is believed the guidelines established by Thales and the French National Strategy for the S3NS are strong and would effectively protect its users (Gouvernement, 2021). However, Google Cloud is a US company and therefore subject to United States laws and pressures. This partnership is not only an example of cooperation between the private and public sectors, but it also shows a level of trust between France towards the United States.

In the worst-case scenario involving a significant political crisis between France and the United States, there would be no real safeguards to avoid the United States' Supreme Court from enacting a new law that could potentially jeopardize the Google Cloud-Thales partnership. Such an act would shut down the French Cloud and paralyze the French economy and the function of vital state institutions. This case is not likely to happen, but such outcomes must be evaluated in order to adequately formulate long-term national policy. On the other hand, it has been mentioned that the Cloud will be separated from Google's network and servers. Therefore, in theory, the Cloud should have more autonomy and independence for Thales and France to operate the Cloud despite relying on Google's technology.

Conclusion

From the Google Cloud-Thales partnership with France to build a secured and trustful Hybrid Cloud example, it became clear that it has strong advantages and downsides. In the long term, such a partnership could be an issue if France does not invest in creating its own Cloud infrastructure separate from Google Cloud.Building such infrastructure requires time and resources that France does possess, but the solution offered by this current partnership is advantageous to the short-term political and security ambitions of the French government. From this perspective, it is believed that the main result of the public-private partnership is time and resource-saving.

On the other hand, partially outsourcing critical infrastructure such as a nation-state's Cloud to a foreign private entity puts your national security at risk. As highlighted before, the US have a different approach to data protection and privacy compared to European Countries. Furthermore, as previously discussed, 65% of 2022 Cloud infrastructure service world market shares were owned by Google, Microsoft and Amazon, all of which are US-based companies (Synergy Research Group, 2022). It can be assumed that most EU Countries will be more likely to outsource one of these three US companies to create their national Cloud infrastructure in the future.

Policy Recommendations

To tackle these potential issues, this research proposes four policy recommendations regarding the creation of national Clouds in the European Union. Based on the S3NS case study, the recommendations aim to provide reliable propositions to safeguard long-term a sovereign European hybrid Cloud and reduce risks of conflict of interest between the private and public sectors. Furthermore, they seek to promote European legal and cyber interoperability to enhance the robustness of Europe's Cloud industry and legal framework. The recommendations are the following:

1.**Bolster European investment in Cloud technology**. To promote investment and development of European Cloud providers that are based in Europe and answer to the European Union's GDPR to build and preserve Cloud technology knowledge in accordance with European values and cyber-security objectives. To do so, a European fund should be allocated to help in the emergence of European Cloud providers that could, in the long run, compete with the United States' hegemony on the world market. This funding has already been proposed under the Single Electronic Data Interchange Area (SEDIA) but the process is too long and lacks credible engagement (European Commission, 2021). It needs a better and stronger long-term partnership between the European Union and the European private sector to develop Cloud infrastructures that could be then used by European states without having to look further afield.

2**.Increased Cooperation**. Cooperation in regulations between European countries is, therefore, necessary to enhance a secured Cloud integration on the continent. Full cooperation at the European level would challenge intrusive foreign legal frameworks and bolster European competitiveness in this increasingly expanding market. Furthermore, it is a matter of national and European security to work with local private companies. It could be the first layout to the creation of a common European Cloud which would be extremely valuable when looking at more interoperability in European defence.

3.**Long-term learning-based Cloud solutions**. In the short term, to partner with United States-based Cloud providers is an effective solution. Nonetheless, European states should embody technology and knowledge transfer in their partnership to gain autonomy in the future. The Google/Thales example partially introduced this notion by jointly creating a new structure that will run the French Cloud and be majority-owned by Thales. Therefore, the new structure is hosted on French soil and is separated from Google's network and servers. It would be advised to adopt the same strategy for future partnerships as it indirectly participates in the transfer of knowledge and technology in Cloud services. Because the infrastructure is hosted on French soil, it falls under the control of France which could learn and re-create such infrastructures.

Furthermore, it also directly falls under French and European regulations which bypass the CLOUD Act. Consequently, it is a good transition from a short-run to a long-run learning-based solution.

4.**Local implementation and monitoring**. Cross-border private-public partnerships are complex and underline policy gaps that could be filled by carefully highlighting their potential risks. The creation of a National Strategy to apply through a domestic and trusted public-private partnership would bring additional control and safeguards to the National Cloud. As such, it is recommended to host the infrastructure locally and to monitor the encryption and access jointly with the national cyber security agency. Checks and balances are truly important in these critical partnerships as trust must be conserved to effectively function.

Reference List

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62. https://doi.org/10.1111/1468-2346.12504.

GDPR. (2016). Derogations for specific situations. Article 49 General Data Protection Regulation. Accessed on 2022, November 23. Retrieved from https://gdprinfo.eu/en-article-49.

GDPR. (2016). Transfers or disclosures not authorised by Union Law. Article 48 General Data Protection Regulation. Accessed 2022, November 23. Retrieved from: https://gdprinfo.eu/en-article-48.

Gouvernement. (2021). Direction interministérielle du numérique. Accessed on 2022, November 23. Retrieved from: https://www.numerique.gouv.fr/uploads/Strategie-nationale-pour-le-cloud.pdf.

European Commission. (n.d.). Funding & tenders. Single Electronic Data Interchange Area (SEDIA). Accessed on 2022, November 23. Retrieved from: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2021-cloud-ai-01-industrial-data

Evans, M., Kessler, D., Lennon, J., & Ross, S. (2019, September 6). US Cloud Act and international privacy. Data Protection Report. Accessed on 2022, November 23. Retrieved from: https://www.dataprotectionreport.com/2019/08/u-s-cloud-act-and-international-privacy/

Microsoft Azure. (2022). Public cloud vs private cloud vs hybrid cloud: Microsoft azure. Public Cloud vs Private Cloud vs Hybrid Cloud | Microsoft Azure. Accessed on 2022, November 23. Retrieved from: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds/#benefits

Synergy Research Group. (2022). Huge cloud market still growing at 34% per year; Amazon, Microsoft & Google Now account for 65% of the total: Synergy Research Group. Synergy Research Group. Accessed on 2022, November 23. Retrieved from: https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues

Thales. (2021, June 10). Thales et Google Cloud Annoncent UN Partenariat Stratégique pour développer conjointement un " Cloud de confiance " en France. Thales Group. Accessed on 2022, November 23. Retrieved from: https://www.thalesgroup.com/fr/group/investisseurs/press_release/thales-et-google-cloud-annoncent-partenariat-strategique

Thales. (2022). Thales Présente s3ns en partenariat avec google cloud et dévoile son offre de transition vers le cloud de Confiance. Thales Group. https://www.thalesgroup.com/fr/group/press_release/thales-presente-s3ns-partenariat-google-cloud-et-devoile-son-offre-transition