MAPPING TECH COMPANIES’ CLOUD EXPANSION IN THE GULF AND ITS HUMAN RIGHTS IMPLICATIONS
KEY TERMS

**GCC:** Established in 1981, the GCC or the Gulf Cooperation Council is a regional political and economic institution comprising Saudi Arabia, the United Arab Emirates, Qatar, Bahrain, Kuwait and Oman.

**Data center:** A physical facility composed of servers, computers, storage systems, and computing infrastructure. May range in size, but most data centers tend to be very large, containing thousands of servers. Entities, like governments, security agencies, and companies use them to store, manage, and disseminate data.

**Cloud region:** A cloud region is typically made up of three or more data centers, communicating and exchanging data to provide resources on demand. While the concept of ‘the cloud’ is made up to seem like something virtual and abstract, physical data centers are what enable cloud computing to function; when we store data in ‘the cloud’ the data is stored and managed in data centers.

**Big Tech:** Refers to the biggest and most dominant information technology companies. The term often refers to the five biggest U.S. based tech companies (Google, Amazon, Microsoft, Meta, and Apple), but Chinese tech companies such as Alibaba and Tencent are sometimes also referred to as Big Tech.

**Colocation data center:** Data centers where many different companies/businesses share the data center facility. Each company controls their own hardware, but the day-to-day running of the data center (power, cooling, connectivity) is managed by the data center provider.

**Wholesale data center:** Similar to a colocation data center, but in wholesale data centers, the data center provider leases large blocks, or the whole facility, to one single customer. The line between what is considered a colocation/wholesale data center is not clear, but wholesale data centers have fewer clients, utilizing more capacity per client.

**Public data center:** Data centers that are owned and operated by third-party providers, accessible for different companies, businesses, and organizations to use. Wholesale and colocation data centers are public data centers.
Private data center: Data centers that are owned and operated by a single organization or business, used exclusively for its needs.

Carrier neutral: A carrier-neutral data center is one that operates independent of other network providers.

Digital authoritarianism: The use of digital technologies by authoritarian regimes to surveil, repress, control, and manipulate populations within their borders and beyond.

Spyware: Spyware is a type of malicious software that is installed on a computing device without the end user’s knowledge. It invades the device, monitors a user’s activities and steals their information, sends it to third parties without the user’s consent.

Alphabet Inc.: A company created by Google in 2015, functioning as a parent company and conglomerate. Owns multiple companies that were owned or created by Google, including Google itself.

Economy of scale: An economic sector or activity where the cost-efficiency increases as the scale of investment or production increases.
INTRODUCTION

This report maps the expansion of technology companies’ cloud and data center operations in countries of the Gulf Council Cooperation (GCC). Since 2018, an increasing number of companies, mainly from the U.S. and China, launched cloud regions and data centers in the Gulf, despite outcry from civil society groups over human rights violations and risks.

SMEX has covered aspects of this trend, raising, for instance, concerns about plans by tech giants Amazon and Google to construct data centers supporting cloud regions in Saudi Arabia¹ and the UAE². Other digital rights organizations and media outlets also wrote about the potential implications of these projects, citing the highly restrictive control of internet activities, pervasive government surveillance, and prosecution of online speech.³ The focal point of this existing coverage was the activities of two U.S. tech giants (Google and Amazon) in Saudi Arabia and UAE, the largest economies of the GCC and two regional powers in WANA. However, a range of other actors are involved and companies other than Amazon and Google are also investing to build data centers and cloud infrastructure in the Gulf. This report maps such investments in all six GCC countries by nine companies that are some of the world’s largest in data center and cloud computing infrastructure. These companies are either U.S. based (Amazon, Equinix, IBM, Google, Microsoft, and Oracle) or Chinese (Alibaba, Huawei, and Tencent).

The global market of cloud infrastructure is increasingly controlled by three companies: Amazon (34%), Microsoft (21%), and Google (11%), which together controlled 66% of the worldwide cloud provider market in 2022⁴. However, lesser known companies such as Oracle and Equinix are also prominent actors. They essentially specialize in providing digital infrastructure solutions for businesses and lease large amounts of data center space.⁵

---

First, the report explains how data centers work and their functions, and why it matters from a human rights and data privacy perspective where a data center is physically located. The second chapter maps investments made by the nine companies in the GCC, focusing on growing cloud investments since 2018 and the political and economic factors underlying this trend. This section emphasizes the rapid growth in global data center infrastructure and cloud computing markets, and the increased demand created by the governments of the GCC through their national vision frameworks and digital transformation programmes. Finally, the report outlines the human rights risks that come with increased data center and cloud infrastructure in the Gulf as a result of weak data protection laws, GCC states’ digital authoritarianism, and the opaqueness in the ventures of the tech companies. The report concludes by providing recommendations for tech companies, civil society, and the U.S. Congress.

Key findings

- U.S. companies Amazon, Equinix, IBM, Google, Microsoft, and Oracle, and Chinese companies Alibaba, Huawei, and Tencent have all either launched cloud centers or announced future plans to launch cloud operations in the GCC. Their operations and plans cover the entire region. Saudi Arabia and UAE are the countries in which most data center and cloud region projects have been announced or started.

- All of the top 5 biggest cloud providers worldwide (Alibaba, Amazon, IBM, Google, and Microsoft) are among the companies investing in data center infrastructure in the GCC countries. The global cloud provider market is becoming increasingly concentrated between these companies, and they hold a lot of power and influence on a global scale. These companies are committing to supporting the GCC governments’ ambitions of digital transformation, and are largely providing the physical infrastructure necessary for their achievement.
All the GCC countries are pursuing similar strategies when it comes to digitalization of society, economy and government. These strategies are outlined in national ‘vision’ frameworks and digital transformation programmes, where implementing eGovernments and becoming a hub for the digital economy are central objectives. Data centers are essential pieces of infrastructure to fulfill these ambitions of digital transformation, and are largely being provided by the outlined foreign companies.

The geographical location of a data center matters because data is typically stored at the nearest data center, and because data is subject to the jurisdiction of its geographical hosting countries. Thus, as more data centers are located within the borders of the GCC countries, its governments will have legal control over an increasing amount of data. This will have consequences for how data is stored and managed across the WANA region.
METHODOLOGY

As there is no updated and publicly available research or documentation mapping out the data centers built in the WANA region since 2018, the first step of the research was to browse the web for information and announcements about data centers built in the relevant countries in order to quantitatively map them out. Data was collected over a period of eight months, between September 2022 and April 2023. We chose to look only at GCC countries because of the shared political and economic particularities of these countries, in addition to a business environment that attracts tech investments. The nine companies (Amazon, Alibaba, Equinix, Google, Huawei, IBM, Microsoft, Oracle, and Tencent) analyzed in the report were chosen based on three key criteria: 1) they are headquartered outside of the GCC region 2) they have previously announced or built data centers in the region, and 3) they are some of the largest tech companies in the world (we did not locate public evidence of another of the worldwide top 50 tech companies ⁶ investing in cloud and data centers in the GCC).

To locate this information, keyword searches of terms like “Google Saudi Arabia data center,” “Google Saudi Arabia cloud region,” “Amazon UAE data center,” “Amazon UAE cloud region” etc. were used. Search engine results generated included announcements on companies’ websites and governments’ official websites, in addition to news sources covering investments in data center projects.⁷ Other key information such as the scope of these investments and data processing capacity were not made available through official company and government sources.

The research then identified key political and economic factors driving this trend and its potential consequences for data privacy and human rights in the WANA region. In their announcements of cloud investments in the Gulf, most tech companies made commitments and gave explicit support to GCC governments’ national ‘visions’ and ambitions of digital transformation. Thus, the research also analyzed the close collaboration between foreign technology companies and GCC governments, and how this collaboration supports the ambitions and interests of both sets of actors. This was achieved by qualitatively evaluating information made available by different sources: SMEX experts⁸, market analyses of data center and cloud service markets, official government documents, and online articles by reliable think tanks and news sources.

---

⁷ Datacenterdynamics.com is a source frequently used in this research, and is useful to keep up with the analyzed trend, as it keeps up with most of the investments announced from tech companies and gathers much of the relevant information.
⁸ Experts from SMEX’s legal and technical units were interviewed for this report.
Data centers serve as fundamental infrastructure in the wider digital ecosystem as they are integral to the functioning of the internet as a whole and to digital economies.⁹ There are different types of data centers serving different purposes for different needs. This research focuses on data centers creating and supporting cloud regions since the majority of data centers built by foreign tech companies in the Gulf are geared towards providing cloud computing services. As the subsequent sections of the report will lay out, the decisions of where data centers are to be geographically located increasingly have political implications. Before further analyzing these aspects, this section will highlight some basic functions of data centers and explains what the cloud is and its implications for data privacy.

What is a data center?
A data center is a physical facility composed of servers, networked computers, storage systems, and computing infrastructure. While they range in size, data centers tend to be very large, containing thousands of servers. Entities, like governments, security agencies, and companies use them to store, manage, and disseminate data. The tech companies outlined in this report such as Alibaba, Amazon, and Google are often referred to as ‘hyperscale’ providers as they build data centers on a very large scale. These companies use data centers to run their own services and applications, to power artificial intelligence, as well as to lease capacity to governments and other businesses.¹⁰

The critical functions of data centers make them integral to the continuity of the daily operations of entities, and therefore their facilities generally include solid backup infrastructure to prevent potential down-time. The most prominent system of classifying and ranking the quality of data centers is that of the Uptime Institute.¹¹ They classify data centers into four tiers, based on redundancy of infrastructure and degree of resilience they can guarantee against potential down-time. Tier I is the least resilient and having the most potential downtime, and Tier IV is the most resilient, having just a few minutes of downtime per year and redundant infrastructure in essentially every component of the data centers.

---

¹¹ Uptime Institute, “Tier Classification System”, Uptime Institute, n.d., https://uptimeinstitute.com/tiers
The classification of data centers depends largely on their ownership and specific purposes. Small entities might choose to store their servers in-house and manage them on their own, ‘on-premise.’ However, as demands for data processing grows so does the need for space to run these operations, and companies commonly look for shared solutions. These data centers are termed ‘colocation’ or ‘wholesale’ facilities. In a ‘colocation’ data center, many companies place their IT systems in the same building, with the hardware being their own, but power, cooling, and connectivity to network service providers is usually ensured by the colocation provider, that is the company owning the data center. A ‘wholesale’ data center is similar, but entails that larger parts of the data center or the data center in its entirety is leased to a single customer.12

Data center infrastructure is constantly evolving, and companies are coming up with new solutions and technological innovations to meet increasingly advanced data processing requirements. The companies leading the way are mainly the tech companies included in this report, which are ‘hyperscale’ providers. As the data center market makes for an economy of scale13, companies are building data centers that are bigger and bigger, the biggest of which are referred to as ‘hyperscale’ data centers. These data centers have different purposes. Some data centers are used to manage technology systems for third parties, while others have the purpose of running a specific application or service provided by a company, for example, Google Search or Meta’s Facebook and Instagram platforms.14

Cloud regions, the geographic locations where cloud providers operate data centers, largely consist of ‘hyperscale’ data centers. Innovation in cloud computing technology is happening rapidly as demand is growing worldwide and GCC governments are implementing strategies to incorporate cloud technologies into public and private sectors. But, what is really ‘the cloud’?

‘The Cloud’

Cloud regions are supported by two or more data centers, and data in the cloud is stored and managed in the different data centers. While we may be inclined to think of the cloud as merely a virtual concept, it is not something abstract

12 Dawn-Hiscox, “What is a data center?”
13 An economic sector/activity where the cost-efficiency increases as the scale of investment/production increases (Will Kenton, “Economies of Scale: What Are They and How Are They Used?”, Investopedia, June 11th 2022, https://www.investopedia.com/terms/e/economiesofscale.asp)
14 Dawn-Hiscox, “What is a data center?”
floating around. As Trey Herr, writing for the Atlantic Council, puts it, “[t]here is no such thing as the cloud, there are just other people’s computers.” ¹⁵

The cloud is essentially a collaboration of different computers, servers, and data centers that communicate and exchange information to provide resources on demand. Due to how ‘the cloud’ works, redundant copies of data are made in multiple data centers in different locations. Thus, data locality in the cloud is extremely unclear and the data flows constantly across borders, which make privacy laws difficult to enforce.

Most cloud companies are notoriously opaque in their ventures with key information about storage of data and the data centers used for storage are not publicly available. In fact, many companies share and lease data center capacity from each other, adding more complexity to data locality in the cloud. For example, Microsoft and Oracle collaborate in providing certain cloud services,¹⁶ and so do Equinix and Google.¹⁷ In 2018, documents were leaked showing Amazon’s use of data centers in their ventures around the world, highlighting a highly complex and opaque network of data centers. In the Gulf, foreign companies, such as Huawei in Saudi Arabia, are partnering with local telecommunications companies and utilizing their existing data centers to host cloud regions.¹⁹ This complex and opaque network is part of what makes data locality in the cloud so ambiguous.

In principle, the user owns their data in the cloud. However, since cloud providers own and control the infrastructure hosting the cloud, they, in fact, have the ultimate control over the user data. Thus, the security and privacy of data in the cloud is becoming an increasingly important point of discussion. But why does it matter where the physical container of our virtual data is located?

Data localization and data sovereignty: Why it matters where data centers are located

The geographical location of a data center is important for two main reasons. First, **data is subject to the jurisdiction of its geographical hosting country.** Second, **data is typically disseminated and stored at the nearest data center.**

There is no existing global framework that controls the flows of data. Over the past decade, the terms ‘data localization’ and ‘data sovereignty’ have become increasingly used in public discourse. Data localization is the practice of keeping data within the region/country it originated from, and for this, having data centers located within a specific region or country is essential.

Data sovereignty subjects data to the laws and governance structure of its hosting country. Thus, where data centers are constructed is highly important due to the legal control it gives to authorities over the data stored in these data centers. As demands from users and businesses of low latency and high speed services are increasing, companies are seeking to bring computing capacity closer to where it is needed. As a principle, data is first saved in the nearest data center. Data center capacity in the wider WANA region is not very developed, but it is being increasingly concentrated in the Gulf. Thus, tech companies’ data centers within the jurisdiction of Gulf states will have implications for how the data of individuals and businesses, not only the Gulf, but the wider WANA region, will be stored and processed. Control over the infrastructure providing connectivity and computing capacity to WANA will give Gulf governments increased access to large chunks of user and derived data and control and power over it. Considering the history of digital authoritarian practices of GCC governments, there are concerns about the negative impact that this may have for privacy and freedoms in the region.

---

21 The ability of a computing system or network to provide responses with minimal delay.
MAPPING OF DATA CENTERS AND CLOUD REGIONS IN THE GCC

While an ecosystem of data centers existed in the GCC before 2018, the market was considered immature due to a lack of carrier-neutral\textsuperscript{22} companies and a few international actors present in the regional market. The market was dominated by local telecommunications companies that do not have data centers as their main focus, and the investment needed to build high quality data centers was lacking.\textsuperscript{23}

From 2018, however, the biggest tech companies in the world have been venturing into the data center and cloud markets of the Gulf. These companies are constructing data center infrastructure on a very large scale. These data centers are mostly geared towards providing data processing solutions and cloud services for companies, creating an environment conducive to business and bolstering the digital economy. The increasing number of data centers is expanding the capacity for processing, computing, and storing data in the Gulf region. According to market projections, the data center and cloud service markets in the broader WANA region are expected to continue to grow rapidly as international technology companies seek profitability and as GCC countries aim to localize data and become a hub for digital economy.

The data center ecosystem in the Gulf before and after 2018

There is no complete and up-to-date list of data centers and cloud regions in WANA available to the public. Datacentermap.com, a “web service acting as the link between providers and clients in the data center industry,” has the most comprehensive data, providing a comprehensive overview of the ecosystem of data centers and cloud regions across the world until around 2018. While the source is not complete, it still provides a solid overview of the ecosystem of public data centers\textsuperscript{24} and amount of data processing capacity of each country prior to 2018.

The following table provides an overview of the number of data centers and cloud regions publicly available for enterprises in the GCC countries prior to 2018, as compiled by Datacentermap.com.

\textsuperscript{22} A carrier-neutral data center is one that operates independent of other network providers (Michael Isberto, “What Is Carrier Neutral Colocation?”, Colocation America, February 24th 2021, https://www.colocationamerica.com/blog/importance-of-carrier-neutral-colocation)

The source does not provide a complete overview of the infrastructure existing in these countries as it does not include data centers used by governments and companies for their own data storage needs (known as private data centers). The source’s overview of GCC countries seemingly stopped being updated around 2018. It should also be noted that each cloud region constructed typically consists of two or three separate data centers collaborating to create and uphold the supply of cloud services.

24 Public data centers are managed by companies providing availability for businesses to utilize for their storage capacity, unlike private data centers, which are not available for others to use.

In 2018, all six GCC countries had existing colocation data centers and all countries with the exception of Kuwait had existing cloud regions available for enterprises to use for their data storage needs. Saudi Arabia and the UAE had the highest number of data centers and cloud regions.

Before 2018, two of the biggest international players in cloud infrastructure had invested in the region. Equinix opened, in 2012, a data center in UAE, while in 2016, Chinese giant Alibaba opened a data center in the UAE.

Since 2018, more companies have started investing in data center and cloud infrastructure in the GCC. The following table provides an overview of the announced investments in data center and cloud infrastructure made by foreign tech companies from 2018 to April 2023.

Twenty-eight investments were identified, a sharp increase from only the two data centers built by foreign tech companies (Alibaba and Equinix) in the region before 2018. Six U.S. based companies (Amazon, Equinix, Google, IBM, and Microsoft) account for 22 of these investments, and three Chinese companies (Alibaba, Huawei, and Tencent) account for six. The table below shows that investments have been made in all six GCC countries. The UAE and Saudi Arabia are seeing the highest increase in the number of data centers and cloud regions launched by U.S. and Chinese companies within their jurisdictions. The UAE accounts for 12 investments and Saudi Arabia accounts for seven.

The numbers making up this table have been taken from a wide range of sources, such as news articles, government websites, and company websites. Given the limited details about the size and scope of investments disclosed by companies and governments, the table provides a mere quantitative overview of investments in cloud infrastructure by tech companies in the GCC. There could also be other investments by other companies that were not announced to the public. It should be noted that each cloud region typically consists of two or more collaborating data centers, meaning that the number of individual data centers exceeds 28.
SAUDI ARABIA
- Google: 1 Cloud Region
- Microsoft: 1 Cloud Region
- Oracle: 3 Cloud Regions
- Huawei: 1 Cloud Region
- Alibaba: 1 Cloud Region

OMAN
- Oracle: 1 Cloud Region
- Equinix: 2 Data Centers

BAHRAIN
- Amazon: 1 Cloud Region
- Microsoft: 2 Cloud Regions
- Oracle: 2 Cloud Regions
- Equinix: 3 Data Centers
- IBM: 2 Data Centers
- Huawei: 2 Data Centers

KUWAIT
- Google: 1 Cloud Region
- Huawei: 1 Data Center
- Tencent: 1 Data Center

QATAR
- Google: 1 Cloud Region
- Microsoft: 1 Cloud Region

UAE
- Amazon: 1 Cloud Region
- Huawei: 1 Data Center
- Tencent: 1 Data Center

QATAR
- Oracle: 1 Cloud Region
- Equinix: 2 Data Centers
Political and economic factors underlying growing cloud investments in the GCC

There are several intertwined economic and political factors, on both regional and global levels, that can arguably explain the sharp increase in data center and cloud computing infrastructure being built in the GCC since 2018.

The market of data center infrastructure and cloud services is rapidly growing and the increased data center capacity and the rapid implementation of new cloud computing technology are changing the way in which economic activity is being carried out. According to RationalStat’s analysis, the MENA data center market grew at a compound annual growth rate (CAGR) of more than 80% between 2019 and 2021. In 2022, the MENA data center market was valued at $2.7 billion. Compared to the total value of $200 billion of the global data center market, this is a relatively small share. Until 2028, the MENA data center market is expected to grow at a CAGR of more than 20%, and reach $10.4 billion. Parallelly with this trend, data consumption in the region is expected to increase by 400% by 2028. As profit prospects remain high, investments in data center infrastructure in the region are likely to continue growing.

<table>
<thead>
<tr>
<th>Year</th>
<th>Worldwide end-user spending on public cloud services</th>
<th>MENA end-user spending on public cloud services</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020</td>
<td>$270 billion</td>
<td>$3.9 billion</td>
</tr>
<tr>
<td>2021</td>
<td>$413 billion</td>
<td>$4.8 billion</td>
</tr>
<tr>
<td>2022</td>
<td>$490 billion</td>
<td>$5.7 billion</td>
</tr>
<tr>
<td>2023</td>
<td>$270 billion(projection)</td>
<td>Not available</td>
</tr>
</tbody>
</table>

Source: Gartner (April 2023) Gartner (October 2021)

26 nions/considerations-moving-data-middle-east/
27 Middle East and North Africa (MENA) is the term used by RationalStat, SMEX uses West Asia and North Africa (WANA).
These statistics show that the regional market only makes up a small percentage of the worldwide market, but that the growth rate of the regional MENA markets is keeping up pace with the global market. As all the major cloud service providers are currently investing in cloud infrastructure in the Gulf,\textsuperscript{31} as data consumption in the region is expected to increase by the cited 400\% by 2028, and as the Gulf governments are implementing ‘cloud strategies,’ the regional market can reasonably be expected to continuously grow.

GCC political economy: From oil dependency to digital powerhouse

GCC states have traditionally relied on oil and gas production for big parts of contribution to national gross domestic product (GDP) and government revenues, and still do so to a significant extent. GCC governments realized the volatility that comes with having an economy heavily relying on revenues from the oil and gas sector, and have been seeking to diversify their economies. In recent years, one of the main strategies for diversification of the economy away from oil has been that of digital transformation. In this day and age, economic diversification cannot be achieved without some sort of digital transformation. In fact, the World Bank estimates that around 60% of global GDP relies on digital communications technologies.32

However, GCC countries are not merely building the digital infrastructure necessary to keep pace with the global digital transformation. Led by Saudi Arabia and the UAE, they are aiming to lead in the global digital economy, and have as an overarching objective of becoming a global hub connecting Asia, Europe, and Africa. For this, they emphasize the importance of having a sophisticated digital infrastructure, of which data centers are an integral part. Being such integral pieces of infrastructure in the push towards digital transformation of the economy, diversifying it away from oil, researcher Ahmed El-Masry, writing for the Middle East Institute, has termed the data center industry “the GCC’s new oil fields”.33

While the oil industry in the Gulf is dominated by the public sector, part of the strategy of diversification of the economy away from oil has been the inclusion, and prioritization, of the private sector. An environment favorable to business and conducive to foreign investment is thus a prerequisite. Tax cuts and cheap land increase the profit prospects of companies seeking to venture into the Gulf’s data center market. The creation of Economic Free Zones is also a policy adopted by GCC countries in order to attract investment.34 For example, Qatar has through its National Vision 2030 implemented Qatar Free Zones Authority (QFZA) in order to enhance digital transformation, and the QFZA entered a close collaboration.

with Google Cloud. The Qatar Free Zones provide incentives such as 100% foreign ownership and renewable 20-year tax holidays, including zero corporate tax, zero customs duty, and no personal income tax.\textsuperscript{35}

The mentioned national visions and digital transformation programmes that each of the GCC countries have adopted over the past years make up the frameworks that concretize the push for a diversification away from the oil dependent economy. It should be noted that these national vision frameworks go beyond merely economic transformation as they encompass government and many sectors of society. For example, Saudi Vision 2030 includes eleven ‘Vision Realization Programs’ that encompass the financial sector, health sector, housing, industry, religion, quality of life and more.\textsuperscript{36} A common theme for all, however, is digital transformation. Relevant to the construction of data centers, aside from the digital economy transformation, are the stated ambitions to transform ways of governance and push towards eGovernments, AI and data-driven decision making.

<table>
<thead>
<tr>
<th>Vision framework</th>
<th>Digitalization</th>
<th>Government strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saudi Arabia</td>
<td>Digital Transformation Programme</td>
<td>Smart Government Strategy</td>
</tr>
<tr>
<td>UAE</td>
<td>Fourth Industrial Revolution Strategy</td>
<td>Digital Government Strategy 2025</td>
</tr>
<tr>
<td>Bahrain</td>
<td>“Cloud-first” nation objective</td>
<td>Digital-first principle</td>
</tr>
<tr>
<td>Qatar</td>
<td>Smart Qatar Vision</td>
<td>Digital Government Strategy</td>
</tr>
<tr>
<td>Oman</td>
<td>Transformation Programme for Digital Economy</td>
<td>Government Digital Transformation Programme</td>
</tr>
<tr>
<td>Kuwait</td>
<td>Digital transformation as a main pillar</td>
<td>Prioritization of digitization</td>
</tr>
</tbody>
</table>

GCC government’s national vision frameworks and digital transformation strategies


The implementation of eGovernments is especially relevant because it is logical that the data stored and processed through data centers, including those owned by tech companies, will be utilized to power the necessary AI and drive the governments’ data-driven decision making. In some cases, the data centers constructed by these companies will directly become a part of state apparatuses. For example, Bahrain expects to “gradually migrate government entities to AWS and eventually have most government data centers shut down,”42 and Oman expects its government to “run its entire IT estate on Oracle Cloud Infrastructure [...] All of the government’s existing data centers will be served with Oracle’s cloud services.”43

So, while the trend of U.S. and Chinese tech companies constructing data centers in the Gulf follows the pattern of increased contribution of the private sector to the economy, government involvement in the ventures is evidence of continued government control in key sectors. Through the construction of the data centers within the geographical region, much more data is localized within the region. Through partial government control over the relevant data centers, as well as the introduction of data protection laws within these countries, steps are taken towards ensuring data sovereignty. Knowing the principle that data is typically first saved in the nearest data center, it is evident that the exponential increase in computing power and storage capacity in the Gulf will have consequences for the way in which data is stored and managed in the wider WANA region. These aspects, combined with the track record of digital authoritarian practices of the GCC countries, a history of surveillance, censorship, disinformation campaigns and online persecution, raises concerns for digital and human rights in the broader WANA region.

HUMAN RIGHTS IMPLICATIONS

The digital space in the GCC is highly controlled. Over the past years, especially since the Arab Spring uprisings of 2011, governments in the region have increasingly deployed digital technologies as tools to control and oppress voices of journalists, activists, and other civil society actors. Keeping in mind the weak personal data protection laws in the region, there is reason to believe that the same governments will not hesitate to exploit the increased data storage and processing capacity provided by the new data centers built by international companies in order to further manipulate digital spaces and advance their own interests. This raises serious concerns for digital rights, privacy, and freedoms in the WANA region.

Digital authoritarianism in the GCC

GCC governments routinely violate Articles 12 and 19 of the Universal Declaration of Human Rights, articles which respectively enshrine the right to privacy and the right to freedom of opinion and expression.

In particular, Saudi Arabia and the UAE frequently take advantage of technology provided by international companies such as surveillance systems, spyware, and social media platforms to exert power over domestic and foreign populations. The most notorious of these technologies is the Pegasus surveillance spyware, which governments of Bahrain, Oman, Saudi Arabia, and the UAE acquired from the Israeli NSO group. The spyware was deployed by the governments of these countries, in order to potentially target thousands of individuals by exploiting vulnerabilities on their smartphones - this included 36 journalists from Aljazeera. The Pegasus spyware is also believed to have been integral to the killing of Saudi Washington Post columnist Jamal Khashoggi on October 2, 2018. This last example may be the epitome of digital authoritarianism in the Gulf: severely infringing upon the privacy of individuals in order to brutally silence voices dissenting from a regime’s line and ideology.

Another prominent practice of digital authoritarianism deployed by Gulf regimes is the use of social media bot armies in order to manipulate public discourse. The tactic was previously used on Twitter to manipulate discourse around Khashoggi’s murder\(^{46}\) and to prop up attention around Emirati leader Mohammed bin Zayed.\(^{47}\) Outside the GCC’s borders, experts believe that the UAE and Saudi governments were previously behind social media propaganda campaigns supporting the Sudanese military after they committed a massacre of pro-democracy protesters in 2019, supporting Khalifa Haftar’s attempt to overthrow a UN-recognized government in Libya\(^{48}\), and to distract from criticism over violations from Saudi-aligned forces in the war in Yemen.\(^{49}\)

More data, yet weak personal data protection laws and a high degree of government control.

Gulf states are among those with the highest internet penetration rates in the world. Along with the increasing capacity for storing and processing data in local data centers, the data consumption in the region is expected to grow by 400% between 2022 and 2028.\(^{50}\) Thus, due to the increasing data localization and the push for data sovereignty, more and more data will be subject to the jurisdiction of these states. This is an integral point of concern for privacy and human rights in the region.

Saudi Arabia and the UAE introduced personal data protection laws (PDPLs) aimed at localizing data within their jurisdictions. Sufficient data center infrastructure is essential to achieve this and to ensure data sovereignty. Saudi Arabia also introduced a separate Cloud Computing Regulatory Framework (CCRF)\(^{51}\) that contains stipulations about the retention and storage of personal data in its jurisdiction. The CCRF stipulates that government entities may only host their data with cloud service providers that have the appropriate licenses issued by the Communications and Information Technology Commission, and that no data of Saudi Arabia’s public sector may be transferred outside of the country for any purpose.\(^{52}\)

---

46 Abrougui & Najem, “Follow the Money for Better Digital Rights in the Arab Region”
48 Ibid
49 Abrougui & Najem, “Follow the Money for Better Digital Rights in the Arab Region”
50 O’Toole, “Digital authoritarianism: The rise of electronic armies in the Middle East”
51 RationalStat, “Middle East and North Africa Data Center Market Analysis and Forecast 2019-2028”
The PDPLs in Saudi Arabia and the UAE contain vague language and concerning loopholes: Saudi Arabia’s PDPL contain exceptions for the law to not apply in cases related to “security, the Kingdom’s reputation, the Kingdom’s diplomatic relations, confidential sources of information, exceptions related to the public authorities,”53 and UAE’s PDPL stipulates that the law “shall not apply” to “government data” or “personal data held with security and judicial authorities” among other exceptions.54 These loopholes essentially give the governments room to handle the data as they wish, putting individuals’ privacy and human rights in the Gulf and the broader WANA region at further risk.

Further indicating the notion that the authoritarian governments of the region will have close access to the increasing amount of data that will flow through their territory, is the fact that most of the relevant data centers are being built in close collaboration with government entities. In many cases, such as Huawei’s data center in Bahrain55 and Google’s cloud region in Saudi Arabia,56 government-related entities (respectively Batelco57 and Aramco) will control infrastructure and provide services.

Aramco, the world’s largest oil producer and the third largest company in the world, is primarily owned by the Saudi state. In Saudi Arabia’s push to achieve the objectives outlined in the Saudi Vision 2030, Aramco is a strategically important player. As the country is looking to diversify its economy away from oil dependency, Aramco is in the process of being transformed into a “global industrial conglomerate.”58 Google Cloud’s data centers in Saudi Arabia are built in collaboration with Aramco. While Google will deploy and operate the cloud region, a subsidiary of Aramco will be offering the cloud services to customers in Saudi Arabia.59

58 Batelco is a telecommunications company in which the Bahraini government is the majority stakeholder. It is the main telecommunications company in Bahrain and also has a presence in a multitude of other countries around the WANA region.
Previous cases illustrate how authoritarian governments in the region will not hesitate to abuse their access to data to exercise control and crack down on dissent. In a 2022 federal court ruling in the US, a former Twitter employee was “found guilty of spying on Saudi dissidents using the social media platform and passing their personal information to a close aide of Crown Prince Mohammed bin Salman.”

This example shows the length to which the Saudi regime is willing to go to reach their objectives and consolidate power, and that they are not necessarily afraid of the repercussions that might come with exploiting tech companies’ platforms.

The close collaboration between international cloud providers and government-owned companies and entities will only increase the risk of unauthorized access to data by GCC governments.

Human rights due diligence

Technology companies do not hide their commitments to supporting the digital ambitions of GCC governments. Many make explicit commitments to supporting data localization requirements in the region by providing data center infrastructure.

When announcing their launch of a cloud region in Qatar, Microsoft highlighted that their investments will “empower customers to meet local compliance and policy requirements” and “provide a foundation for the country to achieve Qatar National Vision 2030.”

In Saudi Arabia, Oracle’s vice president of technology for EMEA (Europe, Middle East, and Africa) said upon the announcement of the company’s second cloud region in the country that his company is “fully committed to support Saudi Arabia’s digital economy objectives in line with Saudi Vision 2030.”

As explained above, given the GCC’s poor human rights record and weak data protection laws in the region, the joint ventures between GCC governments and the world’s most powerful technologies companies is bad news for digital rights. The most dominant technology companies, often known as Big Tech, collect and keep a wide range of user data through their data processing and cloud services. US company Oracle alone claims to have data from 3 billion user profiles, with thousands of data points that can be used to predict future behavior of individuals.
Yet, what are these companies doing to protect human rights in their new ventures? Not enough as demonstrated by publicly available evidence.

During the 2022 Annual General Meeting of Alphabet, a majority of shareholders rejected a proposal led by global advocacy group SumOfUs to “commission a human rights assessment of the company’s plans to locate cloud centers in countries with poor human rights records,” including Saudi Arabia, and publish it online. A majority of independent shareholders (57.6%) voted in favor of the proposal. However, due to Alphabet’s voting system, which gives more votes to a certain class of shareholders—the 17.06% consisting of company executives, officers, and its former CEO—managed to secure a majority of votes in favor of building the data center in Saudi Arabia.

The company did promise to conduct a human rights impact assessment in Saudi Arabia, and claim to have done so. However, they have not made such an assessment public, nor have they shared it with the shareholders or the 39 human rights organizations that called upon Google to make the assessment. Alphabet’s Human Rights Policy claims that: “In everything we do, including launching new products and expanding our operations around the globe, we are guided by internationally recognized human rights standards.” However, Google has “not provided information on what organization undertook that “independent human rights assessment” and it has not provided information on the ‘matters identified’ or ‘steps [taken].” In other words, the human rights diligence claimed by such a prominent US company like Google is not very reassuring, and is yet another source of concern.

According to Ranking Digital Rights (RDR), a research initiative that evaluates the policies and practices of the world’s most powerful tech and telecom companies and studies their effects on people’s fundamental human rights, Google falls short in its disclosures about assessments on “freedom of expression and information risks associated with new activity,” despite having a relatively strong disclosure about its policy of conducting human rights impact assessments.

---

RDR’s Big Tech Scorecard ranks 14 digital platforms (including Alibaba, Amazon, Google, Microsoft, and Tencent) on their policies and practices affecting people’s rights to freedom of expression and privacy. The latest ranking, launched in 2022, found that Alibaba and Amazon had no disclosure on whether or not they conduct assessments. Most companies lacked disclosure of how they handle requests from governments to restrict content and hand over user information.

The involvement of Chinese companies
Another source of concern is the investments of prominent Chinese tech companies in the region. In Saudi Arabia, Alibaba is constructing cloud computing infrastructure, and closely collaborating with government entities to establish a joint venture called the Saudi Cloud Computing Company.70 This is an integral part of Saudi Arabia’s cloud strategy. Huawei invested in data centers in Bahrain,71 Saudi Arabia,72 and the UAE.73

The Chinese state has frequently been criticized for exporting surveillance technologies through Chinese companies and for augmenting digital authoritarianism in the Global South.74 75 Concerns have been raised about the surveillance capacities ingrained in Chinese technologies in terms of the capacities it gives other governments deploying them. Some have even raised the concern of “the risk that the Chinese vendor companies - and thereafter possibly Chinese state security - could gain access to sensitive data.”76 Thus, the implementation of Chinese companies’ data centers and cloud regions in the Gulf might further compromise the privacy and freedoms of individuals across the WANA region.

CONCLUSION

This report has initially explained the basic functioning of data centers, their important role in the functioning of the internet, and how separate data centers collaborate to create ‘the cloud.’ The report highlighted that the geographical location of a data center is important since data is typically disseminated and stored at the nearest data center, and is subject to the jurisdiction of its geographical hosting country. Considering the GCC governments’ push for digitalization, data localization and data sovereignty, and in light of their digital authoritarian practices, increasing data center capacity in these countries raises concerns about the negative impacts that this may have for privacy and human rights in the region.

Subsequently, the report has quantitatively mapped out 28 separate investments made in data center and cloud infrastructure by nine major foreign tech companies, from the U.S. and China, in the Gulf since 2018. This is a sharp increase, as only two such investments had been made prior to 2018. Saudi Arabia and the UAE, the countries with the most developed ecosystem of cloud infrastructure prior to 2018 have also seen the highest influx of foreign investments in data centers and cloud regions.

The report’s analysis of economic factors underlying this trend demonstrate that the rapidly growing global data center and cloud service markets, and an increasingly digitized global economy are integral to spurring these investments. The markets of the WANA region make up a relatively small share of the global markets, but are growing at a rapid pace. And, as all the major cloud service providers are currently investing in cloud infrastructure in the Gulf,78 as data consumption in the region is expected to drastically increase, and as the Gulf governments are implementing digitalization programmes and ‘cloud strategies,’ the regional market can reasonably be expected to continuously grow. As a result, more attention from researchers and civil society in the region needs to be paid to foreign technology companies’ investments in cloud infrastructure.

78 For example, Qatar is giving “special privileges to non-Qatari foreign investors allowing the to provide up to 100% of capital for any projects, and exempting them from income tax for up to 10 years” https://www.gco.gov.qa/en/focus/economic-policy/
Ultimately, the report raises serious concerns about the implications that the relevant investments may have for human rights, privacy, and freedoms not just in the Gulf but also the entire WANA region. GCC digital authoritarianism and willingness to exploit technology provided by foreign companies in order to reach their objectives is a source of concern for how they may exploit newly acquired data center capacity to further manipulate digital spaces. The weak personal data protection laws and high degree of government control over the data centers reinforce concerns about the degree of access and control that the governments will have over personal data of individuals around the WANA region.

Adding to these concerns is the fact that the relevant technology companies also have a track record of being opaque in their ventures. Many of the companies commit to helping the GCC governments in reaching their objectives of digital transformation and data localization, and at the same time most of the companies lack disclosure of how they handle requests from governments when it comes to both censorship of content and user information. Thus, the strengthened relationships between the highlighted companies and the GCC companies is a dangerous development for digital rights in the region, and the implications of the infrastructure investments highlighted in this report should be paid close attention to.
List of recommendations

Tech companies:

- Conduct thorough Human Rights Impact Assessments (HRIA) before deciding to launch data centers in new markets. Make the results of these assessments public so that customers can trust that their interests and privacy are being protected. Such assessments should follow robust standards, such as those set by Ranking Digital Rights,79 and include assessments of how local laws affect privacy and freedom of expression and information in relevant GCC jurisdictions. The assessments should also be assured by external and impartial third parties, and when they identify concerns, additional evaluations should be carried out and relevant mitigation actions should be taken.80

- When establishing data centers in regions with lax privacy regulations, delineate legal liability, specifying whether the user or the company will be held accountable when local authorities enforce these regulations. The specification of such liability should consider the moral responsibility and therefore the legal support the company should provide if any user is prosecuted due to political reasons resulting from a privacy breach during the use of the company’s services.

- Be transparent about the process for handling government demands to hand over user information. Companies should be transparent about how they respond to government demands for user information in all jurisdictions where they operate, including the Gulf. They should exercise due diligence on these demands and push back on inappropriate demands that do not follow the prescribed legal and company processes and demands that infringe on human rights. Companies should also notify users to the extent legally possible when governments demand access to their data.

- Publish data on the number and types of demands submitted by governments to hand over user information. The data should include the number of demands received from each jurisdiction, including the Gulf countries in which cloud providers operate, compliance rates, and number of users affected. If, due to political or legal reasons, the company may face serious consequences if they publish this data (for example, legal or safety risks for staff), those reports should be shared with designated civil society groups in confidentiality to preserve some level of transparency and accountability.
List of recommendations

Tech companies:

☐ Conduct thorough Human Rights Impact Assessments (HRIA) before deciding to launch data centers in new markets. Make the results of these assessments public so that customers can trust that their interests and privacy are being protected. Such assessments should follow robust standards, such as those set by Ranking Digital Rights,79 and include assessments of how local laws affect privacy and freedom of expression and information in relevant GCC jurisdictions. The assessments should also be assured by external and impartial third parties, and when they identify concerns, additional evaluations should be carried out and relevant mitigation actions should be taken.80

☐ When establishing data centers in regions with lax privacy regulations, delineate legal liability, specifying whether the user or the company will be held accountable when local authorities enforce these regulations. The specification of such liability should consider the moral responsibility and therefore the legal support the company should provide if any user is prosecuted due to political reasons resulting from a privacy breach during the use of the company’s services.

☐ Be transparent about the process for handling government demands to hand over user information. Companies should be transparent about how they respond to government demands for user information in all jurisdictions where they operate, including the Gulf. They should exercise due diligence on these demands and push back on inappropriate demands that do not follow the prescribed legal and company processes and demands that infringe on human rights. Companies should also notify users to the extent legally possible when governments demand access to their data.81

☐ Publish data on the number and types of demands submitted by governments to hand over user information. The data should include the number of demands received from each jurisdiction, including the Gulf countries in which cloud providers operate, compliance rates, and number of users affected. If, due to political or legal reasons, the company may face serious consequences if they publish this data (for example, legal or safety risks for staff), those reports should be shared with designated civil society groups in confidentiality to preserve some level of transparency and accountability.

79 Synergy Research Group, “Quarterly Cloud Market Once Again Grows by $10 Billion from 2022; Meanwhile, Little Change at the Top”
81 Ibid
Civil society:

- Research, document, and publicize human rights impacts associated with cloud providers’ operations in the Gulf. Work closely with civil society in the Gulf states, monitoring and documenting human rights violations potentially associated with, or facilitated by, the newly built data centers (surveillance, censorship).
- Understand how cloud operations in the Gulf may facilitate targeting of people due to their online activities and provide technical support to those targeted.
  - Conduct more research into the possible implications of the types of technologies that will be transferred to the GCC countries through the construction of these data centers (AI, Big Data technologies, Machine Learning).
  - Conduct more research into how the construction of these data centers will affect the data flows around the wider WANA region. To what extent will data from individuals in countries around the region be disseminated and stored through these data centers?

- Step up pressure on tech companies doing business in the Gulf. Stakeholders across the world should intensify pressure on tech companies to be more transparent about collaboration with the GCC governments. Public pressure should include demands that the tech companies prioritize and take steps to ensure the respect for human rights when they invest in countries that have a track record of human rights violations – demanding that they do not blindly prioritize profits. Public pressure campaigns of this nature, such as the proposal led by SumOfUs82 in 2022, have been carried out in the past intending to raise awareness about the human rights risks included in constructing data centers in authoritarian countries. The information gathered in this report can be utilized in order to carry out public pressure campaigns with a wider scope, intending to pressure the wide range of tech companies investing in data centers in the region to take measures to safeguard human rights in their ventures.

---

U.S. policy makers:

- Introduce a law (similar to France’s Corporate Duty of Vigilance law) that requires companies headquartered in the US to effectively manage the human rights risks related to their activities. The law should require companies to establish, implement and publish its own Human Rights Impact Assessment corresponding with the UN’s human rights due diligence procedures outlined in the Principles on Business and Human Rights, ensuring that the companies are taking the measures needed to identify and prevent human rights violations in their supply chains.

- The law should include the company’s own activities, as well as the activities of subsidiaries, suppliers, and subcontractors directly and indirectly linked to the company.

- A Human Rights Impact Assessment should include:
  - Risk mapping: identification, analysis, and ranking of potential risks;
  - Steps implemented to address, mitigate, and prevent risks and violations;
  - Outline of procedures implemented for periodically assessing the company’s subsidiaries, subcontractors, and supplier’s compliance;
  - A method for identifying existing or potential risks in cooperation with relevant trade unions;
  - A monitoring scheme to follow up on the measures implemented and assess their efficiency.
  - Threats: what can threaten the companies’ efforts to protect human rights.

- Human rights impact assessment requests made to SEC should not require a motivation such as high risk business activities, but should instead be based on the size and the number of users the company has.

- Finalize the National Action Plan on Responsible Business Conduct which the principal’s are influenced by both OECD guidelines for Multinational Enterprises and UN Guiding principles on Business and Human Rights.

---

83 https://actions.eko.org/en/a/no-google-cloud-region-saudi
85 Worldfavor, “All you need to know about France’s Corporate Duty of Vigilance Law”, accessed 06.03.2024 https://blog.worldfavor.com/all-you-need-to-know-about-frances-corporate-duty-of-vigilance-law
The bottom line is that technology companies, whether U.S. or China based, are seeking profits in new markets, and their profit prospects are prioritized above their human rights diligence. With an emerging lucrative data center and cloud service markets in the GCC along with financial incentives, technology companies are turning a blind eye to their lackluster human rights track records. Importantly, the biggest tech companies, including those that claim to care about human rights, are failing to adequately protect these rights in their (cloud) business operations in the Gulf and the broader WANA region.

77 James Kynge et al., “Exporting Chinese surveillance: the security risks of ‘smart cities’”