Blanquerna - Ramon Llull University
School of Communications and International Relations
Degree in International Relations

Final Degree Project:

"Big Tech's material contributions to digital authoritarianism in the GCC countries"

Author: Aksel Eck Kjærstad (07079828135)
Tutor: Blanca Camps Febrer

Research project
International Economy and Development

May, 2023

Abstract

Digital authoritarianism has been on the rise in the Gulf since the Arab Spring uprisings of 2011. Through practices such as surveillance, censorship, and social manipulation and disinformation, the Gulf governments have routinely deployed digital tools in order to repress dissidents, sway public discourse and control online content. Over the past decade, all six of the GCC countries' governments have adopted national vision frameworks, including objectives of sweeping digital transformations and (neo)liberalization programs which will see relationships between the governments and its citizens be transformed in various ways. In order to build the necessary infrastructure for said digital transformations the GCC governments have attracted investments from foreign Big Tech companies. This paper analyzes these investments and the foreign Big Tech companies support of the relevant governments' objectives for digitalization of society, economy and government. Through this analysis, it seeks to assess to what extent these investments will increase the governments' capacity to carry out digital authoritarian practices. Arguing that the Big Tech investments will give the governments legal control over larger quantities of personal data and that they will incorporate surveillance capitalist technologies into their state apparatus, the paper concludes that said investments will further increase the GCC governments' capacity for digital authoritarianism.

Table of contents

- **Abstract……..…..1**
- **Introduction…….……..…….…3**
- **Literature review……5**
  - Digitalization and digital governments…….,5
  - Digital authoritarianism…….5
  - Digital authoritarianism in the GCC countries…….…….7
  - Exporters of technologies for digital authoritarianism……..……8
  - Data centers and ‘data sovereignty’……..…….8
- **Theoretical and conceptual framework……...10**
- **Analysis……...13**
  - History of digital authoritarianism in the Gulf……..13
  - The GCC countries’ national vision frameworks - supported by foreign Big Tech…….14
    - Case study: Saudi Vision 2030……17
    - The vision frameworks as ‘neoliberal political projects’.....17
  - Leveraging foreign Big Tech to build the necessary infrastructure……..18
    - Increased processing capacity and ‘data sovereignty’……20
    - Transfer of ‘surveillance capitalist technologies’……21
  - ‘State apparatus’: Conceptualizing capabilities for digital authoritarianism……24
- **Results of analysis ……-……..……..26**
- **Conclusions..……..……..27**
- **Bibliography……...30**

Introduction

'Digital authoritarianism' is a term that has been increasingly deployed in literature over the past decade, to describe the ways in which authoritarian regimes exploit digital technologies in order to shape political dynamics in their regimes through manipulation of populations, surveillance and repression. Since the Arab Spring uprisings of 2011, in which digital technologies and social media were integral to mobilization against authoritarian governments, the West Asia and North Africa (WANA) region has seen an increase in retaliating crackdowns and augmented repression in the digital space.

The focus of this paper will be on the concept of 'digital authoritarianism', and to answer the question: "To what extent is the Gulf governments' capacity for digital authoritarianism strengthened through foreign investment by international Big Tech companies in digital infrastructure?". Its main objective is to identify the ways in which the investments made by these foreign Big Tech companies (Google, Amazon, Microsoft, IBM, Oracle, Equinix, Huawei, Alibaba and Tencent) are providing the governments of the Gulf with the material capabilities that further increases their capacity to carry out digital authoritarian practices. This research seeks to make evident the congruence between the technologies required for surveillance capitalism and digital authoritarian practices, and argue that through incorporating the technologies of the Big Tech companies into the state apparatuses of the Gulf governments, their capacity for digital authoritarianism will be further increased.

The present research maps out the national vision frameworks that each GCC country has outlined over the past decades, as well as corresponding programs for digitalization for many areas of society, economy and government, accompanied by (neo)liberal economic policies. Despite the history of human rights abuses and digital authoritarianism in the Gulf states, foreign Big Tech companies do not seem at all reluctant to support and invest in these regimes.

The research also quantitatively maps out a trend, identified as starting in 2018, of foreign Big Tech companies, from the US and China, investing in big-scale data center and cloud computing infrastructure in the Gulf region. As the dealings between these powerful companies and the authoritarian Gulf government are highly opaque, little information is publicly disclosed about their specific scope. However, a qualitative analysis of the companies' announcements of these projects and news articles written about them, shows that a striking number of the data

center investments are accompanied by transfers of advanced technologies such as artificial intelligence (AI).

Deploying an overarching political framework of International Political Economy the starting point of the analysis is the GCC countries' national vision frameworks, as they include crucial (digital) transformations of state structures and relationships between the governments and their populations, and are supported to such a large extent by the relevant foreign Big Tech companies. Looking at a case study of the Saudi Vision 2030 it will be argued, through Harvey's (2007) theory of 'the Neoliberal State', that these national vision frameworks are 'neoliberal political projects' intending to create a good business and investment climate for capitalist endeavors.

The case study of Saudi Vision 2030 evidences the extent of advanced technology transfers accompanying the data center investments, and some of the governance practices that the government intends to deploy them in. Through introducing Zuboff's (2019) concept of 'Surveillance Capitalism' and the ways in which the relevant Big Tech companies use personal data to create 'behavioral surplus' in order to predict human behavior, the paper will argue that the same technologies will be deployed in the digital governments blueprinted by the GCC states. Still acknowledging the difference between the concepts of 'surveillance capitalism' and 'digital authoritarianism' it argues that the material capabilities to carry out both are highly coinciding, and that when the relevant data centers and advanced technologies become part of the state apparatuses of the Gulf governments, their capacity to carry out digital authoritarianism will increase to a large extent.

Literature review

Digitalization and digital governments

The emergence of digital technologies have transformed economies, societies and systems of governments around the world. Digitalization can be defined as "the action or process of digitizing; the conversion of analogue data into digital form" (Parviainen, 2017). In a broader societal context, digitalization can be said to be "the way many domains of social life are restructured around digital communication and media infrastructures" (Srai and Lorentz, 2019). Existing literature largely focuses on the consequences that digital transformation has for the companies and the economy as a whole, in terms of business processes and the relations between companies and customers (Crittenden et al., 2019; Morley et al., 2018). Reviews of existing literature show an increasing focus on advanced technologies such as artificial intelligence (AI), machine learning (ML), and Big Data approaches (Morley et al., 2018).

There is also a considerable body of literature focusing on digital transformation in governments. Much of this literature emphasizes the ways in which implementation of digital technologies can increase transparency in government (Margetts, 2006; Matheus et al., 2021; Toro-Garcia et al., 2020). However, most of this literature acknowledges that there are barriers to digital transparency, such as 'political and legal barriers' including lack of privacy policies and mass surveillance causing lack of data protection. Related to the 'political and legal barriers' to transparency, this paper focuses on the ways in which the implementation of digital technologies may enhance authoritarianism rather than increasing transparency.

Digital authoritarianism

The term 'digital authoritarianism' is relatively new. The definition of digital authoritarianism, also referred to as 'digital autocracy' is well established in existing literature as the way in which authoritarian regimes exploit digital technologies in order to shape political dynamics in their regimes, through manipulation of populations, surveillance and repression (NORC, 2021) (Jones, 2022).

According to Kendall-Taylor, Frantz and Wright (2020) repression in the digital space differs from 'traditional' repression in the sense that it is a faster, more efficient, and more precise way for governments to restrict abilities to mobilize against the regime and to maintain control over populations. According to their historical analysis, dictatorships that deploy digital

authoritarian practices are more likely to avoid collapse than dictatorships that do not. Similarly, a game theory study conducted by Dragu and Lupu (2021), found that authoritarian regimes benefit from technological developments, as it makes it easier to carry out and cover up human rights abuses.

The body of literature that this paper mainly draws on puts emphasis on the different digital tools and tactics that authoritarian regimes deploy. The U.S. Agency for International Development's outlines a plethora of digital tactics and tools deployed by authoritarian regimes (NORC, 2021). "Social manipulation and disinformation", "monitor citizens and identify dissidents", and "increased legibility of society" are the three main tactics that the present research focuses on.

Social manipulation and disinformation involve a plethora of tactics. Data & Society (n.d.) outlines doxxing, hiring of fake activists (trolls), deploying bots on social media and targeting of journalists as the main ones. Furthermore, Fontaine and Fredrick (2019) highlight that innovative tactics such as microtargeting and deepfakes will be enabled by "a sophisticated new set of technological tools- some of them now maturing, others poised to emerge over the coming decade." Bradshaw and Howard (2018) carried out a study showing that the amount of countries using organized social media manipulation campaigns more than doubled between 2017 and 2019.

In the dimension of "monitor citizens and identify dissidents" lies surveillance. Feldstein (2021) emphasizes 'AI and big-data approaches' as one of the main forms of government surveillance. According to NORC (2021), "[t]he advancement of AI-powered surveillance is the most significant evolution in digital authoritarianism." AI technologies are developing at a rapid pace and the full extent of their impact on governance is yet to be seen. Thus, existing literature on the topic largely talks about the 'potentials' that new AI technologies have, as there is little empirical evidence on it (Salam et al., 2023; Valle-Cruz et al., 2019).

Increased legibility of society is something that comes with having higher quantities and more accurate data about its citizens. Gunitsky (2016) argues that information and communications technologies, and social media, "can act as a continuous feedback loop between the rulers and the ruled, an informational mechanism through which elites can gain insights into hidden mass preferences and adjust policy accordingly". As this paper analyzes the vision

frameworks that the Gulf regimes have outlined, special emphasis is placed on how this change in governance will increase the legibility of the societies of the Gulf.

Digital authoritarianism in the GCC countries

The literature on digital authoritarianism in West Asia and North Africa (WANA) largely centers around the practices of the regimes of the Gulf, and especially Saudi Arabia and the UAE. Although this research holds that Saudi Arabia and the UAE are the most prominent perpetrators of digital authoritarianism in the region, it seeks to go beyond these two, and analyze the specific regional context of the GCC as a whole.

Most of the existing literature concerning digital authoritarianism in the WANA region takes the Arab Spring uprisings as a starting point. Being social movements where digital technologies and social media were integral to mobilization against authoritarian governments, they also saw an increase in retaliating crackdowns and augmented repression in the digital space (Jamil, 2022; Jones, 2022; Wessels, 2020). Wessels sees that the Arab Spring was "often framed within a revolutionary and even democratic notion linked to social media and mobile telephony". However, as Jones (2022) argues, social media has become one of the main mediums through which the Gulf regimes repress and manipulate their populations.

Jones' book "Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media" is the most comprehensive work tackling digital authoritarianism in the Gulf. Jones deals with multiple aspects of digital authoritarianism. Primarily it deals with how the Gulf regimes have used social media for deception and disinformation, through populism and manipulation of public discourse. The book also includes a chapter titled "Attacking Journalists and Silencing Dissidents", in which the case study of the killing of Washington Post journalist Jamal Khashoggi is seen as the epitome of how the Gulf regimes use digital tools to monitor citizens and target dissidents.

The narrative he weaves of how digital authoritarianism permeated the "Middle East" builds largely on case studies, and importantly, he highlights the potential hazards of "software created as far afield as Silicon Valley", combined with the malicious intentions of specific bad actors. This combination is the core of what the present research analyzes: how digital technologies imported from foreign actors may increase the capacities for digital authoritarianism in the Gulf. However, rather than focusing on software, this paper focuses on

how material infrastructure that has been increasingly constructed by foreign Big Tech companies will contribute to this.

Exporters of technologies for digital authoritarianism

The topic of the research, aside from the authoritarian governments of the Gulf, involves another set of actors: the foreign Big Tech companies (importantly from the US and China). The degree of collaboration between these two sets of actors has increased since 2018, as the Gulf governments are leveraging technologies from Big Tech companies to achieve the objectives of their national vision frameworks.

There is an existing body of literature dealing with international tech companies "exporting" technologies enabling digital authoritarianism. This literature has mainly focused on China and Russia, and how Chinese and Russian companies export technologies that allow foreign governments to emulate the digital authoritarian practices common in these two countries (Khalil, 2020; Morgues, 2019; Polyalkova, 2019). It centers around how Russia and China intend to 'sell' their models of digital authoritarianism to other countries.

While the existing literature on China's export of digital surveillance technologies is of high importance to the present research, this paper seeks to fill a gap in the existing literature by focusing on how the data center infrastructure investments and technology transfers made by US-based companies also increase the capacities for digital authoritarianism. Companies like Google, Amazon and Microsoft can be considered the main actors of 'surveillance capitalism', and are the companies most heavily investing in the Gulf region.

Pertinent to filling the existing gap in relevant literature are the ideas put forth in Zuboff's (2019) work "The Age of Surveillance Capitalism". Writing from a multidisciplinary perspective centered in political economy and cybersecurity, Zuboff builds on case studies evidencing how Big Tech companies enable surveillance and other breaches of privacy. It provides useful notions to theorize how Big Tech technologies in the hands of the authoritarian governments of the Gulf will increase digital authoritarianism in the region.

Data centers and 'data sovereignty'

Data centers are integral to the storage, processing and distribution of data. Their physical and virtual infrastructure enable the functioning of digital services and power new, advanced

technologies such as AI (Zhang, 2023b). A considerable part of existing literature focuses on the evolution of data centers and their significance for the increasingly digitized economy (Borgman, 2015; Jurayevich & Bulturbayevich, 2020). There is also relevant literature on the geopolitical significance of data center infrastructure, especially relating to cloud computing, which is increasingly the main strategy of optimizing data center capacities (Herr, 2020).

'Data sovereignty' is a concept that has been increasingly used in literature over the past decade, and is the principle that data is subject to the jurisdiction of its geographical hosting country. There is currently a wide range of technical and legal literature available on their emerging importance (Brannon, 2018; Taylor, 2020; Zheng, 2020). The existing literature largely covers the implications that data sovereignty has for business environments, and to some extent for geopolitical dynamics. While these are important factors playing into the strategies of the Gulf governments to localize citizens' data and achieve data sovereignty, this research intends to add to the existing literature by asserting the ways in which the increased control over citizens' data will increase the governments' capacities for digital authoritarian practices. In order to do this, this paper draws on policy analysis conducted by legal experts at SMEX, analyzing the personal data protection laws in Saudi Arabia and the UAE (Rahme, 2022)(Constantine, 2022).

Theoretical and conceptual framework

The present analysis of how the investments of foreign Big Tech companies in digital infrastructure located in the Gulf states may strengthen the governments' capacities to carry out digital authoritarian practices includes a nexus of powerful actors and complex, opaque processes. The Big Tech companies collaborating with the Gulf governments in order to build data centers and cloud regions are not only the biggest technological companies in the world - they are the world's biggest companies, period (Microsoft #2, Google #4, Amazon #5)[1] (Companies Market Cap, 2023). The Gulf governments are among the most powerful of the WANA region - especially so in the governance of the region's digital space where populations and individuals are subject to a wide range of tools of digital authoritarianism.

In order to make sense of this complex nexus of actors, this research uses an International Political Economy (IPE) framework, largely drawing on Cammett, Diwan, Richards & Waterbury (2015), as the foundation for its analysis. In their work "A Political Economy of the Middle East" they present a theoretical framework which fundament is: "Outcomes in the political economy of development can best be conceptualized as the political interactions between three domains: (1) the state, state policies, and state structures; (2) the economic agents operating, and how the economy behaves over time; and (3) social actors, whether groups or individuals." The framework also holds that "material interests" is one of the major variables vital to understanding political economy - in line with this, this research keeps a fundamental focus on material digital infrastructure, mainly data centers.

The framework is highly pertinent and applicable to the topic of the present research, as it intends to investigate and analyze connections between: (1) state actors (GCC states), their policies (national visions and digital transformation plans) and state structures (eGovernments, economy and digital infrastructure); (2) the economic agents operating (foreign Big Tech companies and state-owned companies) and the economy's behavior (digitalization and neoliberalization); (3) and social actors (the population of the Gulf region, social classes and civil society groups).

Against a backdrop of historical examples of the GCC states' track record of digital authoritarian practices, the paper initiates its analysis by quantitatively mapping out the national

[1] Notably, Saudi Aramco, building a cloud region in collaboration with Google, clocks in at #3 on this ranking.

vision frameworks of each GCC state and identifies each states' outlined objective for digitalization, digital government strategies and economic policies/aspirations. Through qualitatively analyzing the case study of Saudi Vision 2030, the political projects that the Gulf states are undertaking through their national vision frameworks are identified as neoliberal projects, following David Harvey's (2007) theory of the "The Neoliberal State". According to his critique of neoliberal theory, the neoliberal state is one that imposes, by force, the 'necessary' market conditions to "create a 'good business or investment climate' for capitalistic endeavors" (Harvey 2007, p. 70). This framework is used to argue the notion that these political projects are largely designed to attract foreign direct investments, especially in material digital infrastructure from Big Tech companies.

The relevant Big Tech companies can be deemed as the main actors of 'surveillance capitalism', and surveillance capitalist technologies are useful in providing capacities for digital authoritarianism. 'Surveillance capitalism', according to Zuboff (2019), is a "new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales". This paper quantitatively maps out the data centers and cloud regions built by foreign Big Tech companies in the Gulf and argues that the material capabilities granted by these data centers, and the accompanying technology transfers, will allow for further surveillance, manipulation and repression of individuals, civil society, and the general population of the Gulf.

Backing up this notion of increased material capabilities, this paper is also informed by Althusser's theory of the State Apparatus. Through exposing the close collaborations between the foreign Big Tech companies and Gulf governments in building the data center infrastructure, it argues that these technologies will become part of the state apparatus of the Gulf regimes. The theory of the State Apparatus "defines the State as a force of repressive execution and intervention in the interests of the ruling classes". Althusser distinguishes between the Repressive State Apparatus (RSA) and the Ideological State Apparatuses (ISA), although they function in a intertwined manner: the RSA, through institutions like police and army, functions dominantly by repression (including physical repression), and secondarily by ideology; and the ISAs, through institutions of media, education and culture, function predominantly by ideology, and secondarily by repression. It will show that the digital technologies provided by the foreign Big Tech companies, from China and the US, will become part of the Gulf states' RSA and ISAs.

Thus, within the overarching IPE theoretical framework deployed, this paper will conceptualize the national vision frameworks of the Gulf states (1) as state policy intending to digitally transform state structures: the frameworks, imposed by the historically authoritarian states also include provisions of liberalization and privatization, and are thus conceptualized as 'neoliberal political projects'. The direct support towards these political projects, and digital infrastructure investments and technology transfers made by the foreign Big Tech companies (2) in collaboration with the governments of the GCC, are highlighted as the main interplay between the first two sets of actors. This dynamic is identified as implicating the transfer of 'surveillance capitalist capacities' into the 'state apparatuses' of the Gulf states, which fortifies the capacities to carry out digital authoritarian practices. By strengthening their ideological and repressive state apparatuses, the Gulf states will acquire further means to further surveil, manipulate and repress a larger set of social actors (3), such as civil society groups, political dissidents and specific individuals such as journalists. In this way, theory is deployed to argue the extent to which the capacity for digital authoritarianism in the Gulf is strengthened through foreign Big Tech companies' investments.

Analysis

History of digital authoritarianism in the Gulf

As a backdrop to the analysis, an initial overview of the history that the GCC states have of digital authoritarianism is pertinent to start off with. As the present analysis seeks to show how foreign Big Tech companies' investments in material digital infrastructure in the Gulf states will increase digital authoritarianism, this backdrop provides an initial idea of how the GCC governments might exploit the newly acquired technologies in order to exert further power in the region's digital space.

Similar to most of the other countries in the WANA region, the Gulf states have seen an increase in retaliating crackdowns and augmented repression in the digital space since the Arab Spring uprisings. The GCC countries, most prominently Saudi Arabia and the UAE, have increasingly exploited digital technologies into their repressive state apparatuses and routinely violated Articles 12 and 19 of the Universal Declaration of Human Rights - articles which are respectively supposed to protect individuals against "arbitrary interference with his privacy, family, home or correspondence" and ensure "the right to freedom of opinion and expression" (United Nations, 1948).

The Gulf governments' digital authoritarian practices have been especially pervasive through the tool of 'monitoring citizens and identifying dissidents'. In 2017, it was revealed that Saudi Arabia, the UAE, Qatar and Oman had acquired the surveillance system 'Evident' from UK defense company BAE. This system allowed to "conduct mass surveillance of users' online activities, decrypt encrypted communications and determine the location of users based on data emitted by their mobile devices" (Abrougui & Najem, n.d.). The governments of Saudi Arabia, the UAE, Bahrain and Oman have also acquired the Pegasus from the Israeli NSO group. The spyware was deployed to target thousands of individuals through exploiting vulnerabilities in their smartphones - including 36 journalists from Aljazeera. Pegasus was also used to target Washington Post columnist Jamal Khashoggi before he was murdered in the Saudi consulate of Istanbul, believed to have been ordered by Saudi Crown Prince Mohammed bin Salman (MBS) (Al Jazeera, 2020).

The Saudi government reportedly has a secret program to monitor, detain, kidnap and torture dissidents, launched by MBS in 2017. There have been several reports over individuals

tortured and killed because of their online activism (Freedom House, 2021). Amnesty International asserted in 2022 that the GCC states at least 75 individuals, journalists and human rights activists, were at the time imprisoned for exercising their freedom of expression. However, due to the lack of transparency in these regimes, "this tally is not reflective as such of the full scale of such arrests and prosecutions" (Amnesty, 2022).

According to NORC (2021), AI-powered surveillance is the most significant evolution in digital authoritarianism. The subsequent sections of this paper outline some of the ways in which GCC governments plan to integrate AI technologies transferred by foreign Big Tech companies into their state apparatuses. This will increase their abilities to monitor citizens and identify dissidents.

The history of digital authoritarianism in the GCC countries also include pervasive uses of the tactics of 'censorship' and 'social manipulation and disinformation'. The GCC countries included in Freedom House's 'Internet Freedom' ranking (Saudi Arabia, UAE and Bahrain) score poorly, ranking as "not free" in the dimension of 'limits to content' ('censorship') (Freedom House, 2022). Furthermore, the Gulf governments have routinely used social media to manipulate public discourse, disrupting conversations through so-called 'electronic armies' of bots. The tactic has been used on Twitter in cases of manipulation of discourse around Khashoggi's murder and to prop up attention around Emirati leader Mohammed bin Zayed (O'Toole, 2022). While 'censorship' and 'social manipulation and disinformation' are not thoroughly analyzed in the following sections, these aspects are important to contextualize the wide range of practices of digital authoritarianism that the Gulf governments deploy.

The subsequent sections do, however, analyze how the digital infrastructure invested in by foreign Big Tech companies will increase the governments' capabilities for digital authoritarianism through 'increasing legibility of society', giving the governments increased abilities to identify discontent and potential dissidents even before they make their voices heard on social media.

The GCC countries' national vision frameworks - supported by foreign Big Tech

Within the nexus of actors and complex, opaque processes, an adequate starting point for the analysis is the national vision frameworks outlined by each of the GCC governments. This, because: they are comprehensive frameworks outlining state policies that are transforming state

structures, largely through programmes of digitalization; they are set to transform various relationships between the governments and the populations of their countries; and they are explicitly supported and committed to by the various foreign Big Tech companies investing in digital infrastructure in the GCC states. The frameworks include strategies for digital governments and the integration of AI, which this paper argues will increase their capabilities to 'monitor citizens and identify citizens' and 'increase legibility of society'.

Table 1 outlines the national vision frameworks of each GCC country, shows that they all include integral aspects of digital transformation, and specific plans to digitize their government infrastructure, as well as neoliberal economic policy reforms. The GCC countries have adopted these frameworks in order to concretize a push for a diversification away from the region's oil dependent economy, and to create digitized economic and societal structures that allow them to compete in an increasingly digitized global economy.[2] Data centers are an *integral* piece of infrastructure for this economic diversification towards digitalization, to the extent that El-Masry (2021) have deemed the data center industry as "the GCC's new oil fields".

Table 1: GCC countries' national vision frameworks, digital transformation programmes, digital government strategies and economic policies/aspirations

	Saudi Arabia	**UAE**	**Bahrain**	**Qatar**	**Oman**	**Kuwait**
Vision framework	Saudi Vision 2030	We The UAE 2031	Bahrain Vision 2030	Qatar Vision 2030	Oman Vision 2040	Kuwait Vision 2035
Digitalization	Digital Transformation Programme	Fourth Industrial Revolution Strategy	"Cloud-first" nation objective	Smart Qatar Vision	Transformation Programme for Digital Economy	Digital transformation as a main pillar
Government strategy	Smart Government Strategy	Digital Government Strategy 2025	Digital-first principle	Digital Government Strategy	Government Digital Transformation Programme	Prioritization of digitization
Economic policies/	Privatization Program	Abu Dhabi Economic	Bahrain Economic	"Advanced Business	"Empowered Private	"Private sector leads the

[2] The World Bank (2023) estimates that 60% of global GDP relies on digital communications technologies.

aspirations	Special Economic Zones	Vision 2030 Special Economic Zones	Vision 2030[3] Special Economic Zones	Environment"[4] Special Economic Zones	Sector"[5] Special Economic Zones	economy"[6] Special Economic Zones

Sources: (Amazon, 2019; Data Center Dynamics, 2018, 2019, 2021a, 2021d, 2021e; IBM, 2022; Microsoft 2019, 2022b; Moro Hub, 2021; Oracle, 2020, 2021, 2022; SMEX, 2022a; Swinehoe, 2023a, 2023b, 2023c; Yahoo, 2022)

The fact that they are all pursuing similar strategies mirrors some of the most basic objectives of the Gulf Cooperation Council; that is to "effect coordination, integration and interconnection between member states in all fields" (Gulf Cooperation Council, n.d.). Also, the GCC's objective to "establish joint ventures and encourage cooperation by the private sector" is an aspect that is mirrored in the trend analyzed in this paper, as the digital infrastructure necessary to reach the objectives outlined in the vision frameworks are built in cooperation with foreign Big Tech companies. In order to encourage this cooperation and to leverage the technology of Big Tech, the GCC countries are implementing neoliberal economic policies, such as privatization, tax breaks and economic free zones.

As each of the vision frameworks are highly comprehensive and encompass fundamental transformations of large swaths of society, the extension of this paper does not allow for a thorough analysis of each framework. Thus, the following subsection includes a case study of the Saudi Vision 2030, which makes a more in depth analysis of the ways in which the government say they will deploy the AI technologies transferred through the Big Tech companies' data center investments. It also conceptualizes the vision framework as a 'neoliberal political project', through introducing Harvey's theory of "The Neoliberal State". Keeping in mind the objective of coordination, integration and interconnection between the member states of the GCC and the congruence between the six states' national vision outlined in Table 1, it may be argued that all of the national visions can be characterized as 'neoliberal political projects'.

[3] "By 2030, the private sector should be able to drive economic growth in Bahrain independently" (Bahraini government, 2008)
[4] "[...] giving special privileges to non-Qatari foreign investors allowing them to provide up to 100% of capital for any project, and exempting them from income tax for up to 10 years." (Qatar Government Communications Office, 2021)
[5] The business environment will be developed, the private sector will play a leading role and will be empowered to achieve balanced economic development (Omani government, 2021)
[6] Restore the regional leadership role of Kuwait as a financial and commercial hub, and reviving the pivotal role of the Kuwaiti private sector in the leadership of development (Kuwaiti government, 2017)

Case study: Saudi Vision 2030

Saudi Vision 2030 includes a multitude of strategic objectives, specified targets and key performance indicators for the transformation of different sectors of economy, society and government. One of the specific objectives outlined in Saudi Vision 2030 is the one of 'a developed digital infrastructure'. This section acknowledges that "[a] sophisticated digital infrastructure is integral to today's advanced industrial activities" (Kingdom of Saudi Arabia, 2016).

Highly pertinent is the integrated National Strategy for Data & AI, which includes implementation of Big Data and AI in the priority sectors of education, government and health care (National Strategy for Data & AI, n.d.). As parts of these state structures will become digitized and driven by AI technologies, it can be identified how relationships between the government and its populations will transform.

Through deploying these technologies the government will rely on, and have access to, a much wider range of the personal data of its citizens. Many processes in the relationship between government and population will be automated, which is a fundamental change in the relationship itself. Furthermore, a change in the relationship which highly pertains to the main thesis of this paper, is that the privacy of the citizens will be jeopardized and the government will have access to a much wider range of personal data of its citizens. This will significantly increase the government's capacities of monitoring citizens and identifying dissidents. It may also increase the governments' 'legibility of society', in the sense that an increased access to personal data of citizens may enable the government to collect information about citizens' preferences and thus, be able to identify and root out "sources of discontent before they spiral into something more threatening" (NORC, 2021).

The vision frameworks as 'neoliberal political projects'

The widespread digital transformation of government, society and economy are accompanied by economic policies that are neoliberal in their nature. Saudi Vision 2030 includes its own "Privatization program" for, includes the provision of "corporatization" of the health care sector, explicitly states that the government seeks to "remove all obstacles preventing the private sectors from playing a larger role in development" (Kingdom of Saudi Arabia, 2016a). The

country is also establishing special economic zones, applying "special commercial regulations to boost investment possibilities".

Harvey (2007) theorizes that a 'Neoliberal State' imposes, by force, the necessary market conditions to "create a 'good business or investment climate' for capitalistic endeavors". Saudi Arabia, an authoritarian state in nature, is by force imposing these transformative policies of digitization and neoliberalization of the economy. Thus, the national vision framework may be conceptualized as a 'neoliberal political project', as it is intended to increase the role of the private sector and create an environment for capitalist investments to flourish.

In symbiosis with the neoliberal economic policies, the comprehensive objectives for digital transformation create the climate, and demand, for investments from private technology companies. The Saudi Vision 2030 document explicitly outlines that "[w]e will partner with the private sector to develop the telecommunications and information technology infrastructure" (Kingdom of Saudi Arabia, 2016a). That is just what they have done. As Table 2 in the next section shows, foreign Big Tech companies have recognized this demand and the profit prospects of investing in data center and cloud infrastructure in Saudi Arabia.

This paper maintains the argument that the congruence between Saudi Vision 2030 and the national vision frameworks of the other GCC countries allows for a generalization of all these frameworks as 'neoliberal political projects'. Thus, the data center and cloud infrastructure investments by foreign Big Tech companies in all the GCC countries outlined in Table 2 can be said to be part of a trend following the same economic logic.

Leveraging foreign Big Tech to build the necessary infrastructure

The extensive ambitions for digitalization that the GCC states outline in their vision frameworks require vast ecosystems of digital infrastructure providing internet connectivity. According to Ball (2019), fiber-optic internet cables and data centers are the most integral pieces of material infrastructure that enable internet connectivity. While the GCC countries have seen an increase in fiber-optic cables being constructed over the past years (Cochrane, 2023), the present analysis focuses on data centers. Table 2 quantifies the data center and cloud region[7] investments made by foreign Big Tech companies in the Gulf since 2018.

[7] Cloud computing is increasingly becoming the main method of data storage (Herr, 2020). A cloud region is typically created, and supported by, two or more data centers.

This section focuses on how these investments and the technologies transferred by foreign Big Tech companies may increase capacities for digital authoritarianism in the Gulf. It first argues that due to the principle of data sovereignty, the increase in quantity of data that will be subject to the jurisdiction of the Gulf countries will increase the governments' capacities to surveil and monitor its citizens. Second, the advanced technology transfers that accompany the outlined data center investments are of high magnitude, as the Gulf governments will likely take advantage of this technology in order to achieve their objectives of digitizing their governments.

Table 2: Data center and cloud infrastructure investments made by foreign Big Tech companies in the Gulf since 2018

	Saudi Arabia	**UAE**	**Bahrain**	**Qatar**	**Oman**	**Kuwait**
Google	1 cloud region	x	x	1 cloud region	x	1 cloud region
Amazon	x	1 cloud region	1 cloud region	x	x	x
Microsoft	1 cloud region	2 cloud regions	x	1 cloud region	x	x
Oracle	3 cloud regions	2 cloud regions	x	x	1 cloud region	x
Equinix	3 data centers	x	x	x	2 data centers	x
IBM	x	2 data centers	x	x	x	x
Huawei	1 cloud region	2 data centers	1 data center	x	x	x
Alibaba	1 cloud region	x	x	x	x	x
Tencent	x	x	1 data center	x	x	x

The data center and cloud region investments mapped out in Table 2 show that the ventures in the GCC countries are undertaken by Big Tech companies based in China and the US. The link between Chinese companies' digital infrastructure and capacities for digital authoritarianism is quite clear, as China is seen as the pioneer of digital authoritarianism and there is a considerable body of literature discussing how China exports their capabilities for digital authoritarianism around the world (Khalil, 2020; Morgues, 2019). This section puts more

emphasis on the ways in which Big Tech companies from the US, which is not commonly classified as a digital authoritarian country, also contribute to increasing capabilities for digital authoritarianism. This section argues that the technologies transferred largely grant the governments with the material capabilities of 'surveillance capitalism' - which largely coincide with the material capabilities of 'digital authoritarianism' due to the coinciding aims of predicting and controlling human behavior.

Increased processing capacity and 'data sovereignty'

Before 2018, the data center market of the WANA region was considered immature due to a lack of carrier-neutral companies, and few international actors present in the regional market. The market was dominated by local telecommunications companies which do not have data centers as their main focus, and the heavy investment needed to build high quality data centers was not present (Al Naqbi, 2018). There had only been two data center investments made by foreign Big Tech companies in the GCC countries, with Equinix and Alibaba building one data center each in the UAE (Alibaba, 2016; Schwarzmann, 2012). Thus, the rapid increase in investments by foreign Big Tech is striking. The WANA data center market, which was valued at $2.7 billion in 2022, is further projected to grow by a compound annual growth rate (CAGR) of more than 20%, and will reach $10.4 billion by 2028 (Zawya, 2022c). Parallelly with this trend, data consumption in the region is expected to increase by 400% by 2028 (Zawya, 2022c), meaning that much more user data will be available, and subject to the jurisdiction of the Gulf governments.

Data sovereignty is the principle that data is subject to the jurisdiction of its geographical hosting country (Tech Target, n.d.). One way in which the data center investments by foreign Big Tech companies in the Gulf may increase capacities for digital authoritarianism is the mere *quantity* of data that the governments will have legal control over. This aspect pertains to the investments from both Chinese and US companies, as it is linked to the *quantified* data processing capacities that the data centers and cloud regions outlined in Table 2. The principle of data localization is also an important aspect to include in this analysis, as data is typically processed and stored at the *nearest* data center - reinforcing the assertion that the personal data of the populations residing in the Gulf countries will in fact be processed and stored at the outlined data centers, which are subject to the legal control of the Gulf governments (Eck, 2022).

Analyses of Saudi Arabia's and the UAE's personal data protection laws (PDPLs) further reinforce the argument that the outlined investments will increase capacities for digital authoritarianism in these countries. While the laws look "good on paper", intended to mirror the EU's General Data Protection Regulation (GDPR)[8], they contain important loopholes and exceptions for the law from applying in instances relating to cases such as "security", "the Kingdom's reputation" and "personal data held with security and judicial authorities" (Constantine, 2022)(Rahme, 2022). Legal analyses conducted by cited legal experts at SMEX assert that these loopholes and exceptions will essentially allow for the governments to act as they want with their data.

Thus, the first way in which the Big Tech investments in digital infrastructure will increase capacities for digital authoritarianism in the Gulf pertains to the quantity of personal data that the governments will have access to. As the material infrastructure processing an increasing amount of individuals' personal data are located within the jurisdiction of these governments, they are able to assert the sovereignty of this data. Through applying laws that give them agency to extract this personal data, their ability to monitor citizens will be augmented to a large extent.

Transfer of 'surveillance capitalist technologies'

Accompanying the data center investments outlined in Table 2, the foreign Big Tech companies have transferred significant amounts of advanced technologies to the Gulf countries. As discussed in the previous section, the basic functions of data centers include the capabilities of processing and storing big quantities of data. In addition to this, data centers are essential in supporting the working of advanced technologies such as AI. The Big Tech companies outlined in this paper, particularly the ones headquartered in the US, are currently the pioneers of new AI technologies. AI technologies are increasingly fuelling 'surveillance capitalism', and as described in previous sections, the GCC governments intend to include such technologies in their form of government.

The Big Tech companies outlined in this paper, particularly the ones headquartered in the US, can be deemed among the main actors and perpetrators of 'surveillance capitalism'. Here, they will be referred to as 'surveillance capitalist companies'. In "The Age of Surveillance

[8] Regarded as the 'gold standard' for personal data protection laws

Capitalism", Zuboff (2019) writes extensively about the practices of Microsoft, Amazon, and particularly Google, and the ways in which the companies commodify human behavioral data through collection, tracking, storage and processing. Oracle, world's largest database management company should also be highlighted, as the company claimed already in 2017 to have data from 3 billion user profiles, with thousands of data points that can be used to predict future behavior of individuals (Wolfie, 2017).

The 'surveillance capitalist companies' are notoriously opaque in their ventures, and key information about storage of data, and the data centers used for this, is not publicly available. In fact, many of the companies share and lease data center capacity from each other, adding more complexity and opaqueness to the processes of 'surveillance capitalism'. For example, Microsoft and Oracle collaborate in providing certain cloud services (Microsoft, 2022c), and so do Equinix and Google (Equinix, n.d.). 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 (Moss, 2018).

Within this opaque network of data storage infrastructure the personal data of billions of individuals are stored. The 'surveillance capitalist companies' use this human experience as raw material for "hidden commercial practices of extraction, prediction and sales" and create 'behavioral surpluses' in order to be able to predict and manipulate the behavior of large groups of individuals (Zuboff, 2019). As the technologies of 'surveillance capitalism' have become more advanced, Zuboff argues that the companies not only try to predict users' behavior, but also intend to modify it - as to "make the future for the sake of predicting it" offers more guaranteed outcomes". (Zuboff, 2019, p.203) The idea of the surveillance capitalists seems to be that the best way to predict behavior is to control it, which can also be identified as a logic of digital authoritarianism.

AI developments are increasingly fuelling 'surveillance capitalism' (Stahl et al., 2022), and similarly, the advancement of AI-powered surveillance is also the most significant evolution in digital authoritarianism (NORC, 2021). In the announcements of their data center and cloud region investments in Saudi Arabia and the UAE, Google, Oracle, Amazon and Oracle have outlined the types of advanced technologies that will accompany their infrastructure projects (Amazon, 2022; Microsoft, 2019; Swinhoe, 2023b; Zawya, 2022a). Google has accompanied their Google Cloud investment in Saudi Arabia with a "Cloud Academy" giving mentorship to

companies in “artificial intelligence (AI), Data & Analytics, machine learning (ML) and marketing” (Zawya, 2022a). Oracle’s vice president of Oracle EMEA (Europe Middle East and Africa) commented on the announcement of their investment in Saudi Arabia that “Oracle Cloud delivers pioneering innovation in technologies like AI, Machine Learning, and IoT, and it will help fuel the economic growth and digital transformation that is an integral part of the Saudi Vision 2030” (Swinhoe, 2023b).

These examples show the direct ways in which the Big Tech companies transfer ‘surveillance capitalist capabilities’ to the GCC governments. How the governments intend to use this may be best captured by the Saudi Government’s outlined plan of how to use ‘Big Data’ in their Smart Government Strategy: “The increased use of Big Data and analytics is identified as one of the Technology drivers by the Smart Government Strategy (2020-2024). It recognizes the potential of Big Data, Machine Learning, & Predictive Analytics for decision-making and to predict potential non-compliance in any focused area” (Kingdom of Saudi Arabia, 2020).

Here, a congruence between the strategy of ‘surveillance capitalism’ and the strategy pursued by the Saudi government can be identified. The use of ‘Big Data’ analytics to predict potential non-compliance among citizens relates to the surveillance capitalist notion of ‘behavioral surplus’, and has the potential to be a powerful tool for digital authoritarianism.

This section has outlined two interconnected ways in which the digital infrastructure investments made by foreign Big Tech companies will increase capacities for digital authoritarianism in the GCC countries: first, through the construction of data centers that provide a sharp quantitative increase in the data storage and processing capacity in GCC countries; and second, through the accompanying transfers advanced technologies, such as AI, that allow for more pervasive monitoring of citizens and increases legibility of society. The workings of ‘surveillance capitalism’ rely upon the same infrastructure, as the advanced technologies allowing for the accumulation of ‘behavioral surplus’ needs access to vast amounts of data, stored in data centers. This can be directly illustrated by the fact that the ‘surveillance capitalist companies’ outlined in this research are also the biggest data center companies in the world (Zhang, 2023a). Thus, just as there is a congruence between the strategies pursued in ‘surveillance capitalism’ and digital authoritarianism, there is a congruence between the *material* infrastructures underlying the capabilities for both. The next section seeks to discuss how the

integration of this infrastructure into the state apparatuses of the GCC states will increase their capabilities to carry out digital authoritarian practices.

‘State apparatus’: conceptualizing capabilities for digital authoritarianism

Althusser’s (1971) theory of the ‘state apparatus’ provides a pertinent approach to analyze how the digital infrastructure investments of foreign Big Tech companies will increase digital authoritarianism in the GCC countries. In defining the state as a “force of repressive execution and intervention in the interests of the ruling classes”, Althusser’s theory is pertinent to the logic of digital authoritarianism. This section seeks to make clear how the newly acquired digital infrastructure will be integrated into the repressive state apparatuses (RSAs) and ideological state apparatuses (ISAs) of the GCC state. The digital infrastructure built by Big Tech will be a shift in the means of communication between the governments and its citizens, and advanced technologies will transform sectors such as education and health -thus, it can be said to become part of the states’ ISAs. Furthermore, through the governments’ part ownership of data centers and the integration of this infrastructure into the states’ physical structure, it can be conceptualized that it becomes part of the states’ RSAs

The ISA functions predominantly through institutions, by enforcing ideology in communication, media, culture and education. As the present analysis has discussed, the GCC governments have outlined ambitions to digitally transform many sectors of society. Through these transformations the ways the government can access citizens’ data are changing, and the deployment of AI in the education and health sectors see a shift in the capabilities in the ISAs of the GCC states. Through deploying the acquired ‘surveillance capitalist technologies’ in their ISAs, the governments will have strengthened means to monitor and predict citizens’ behavior.

A look at Saudi Vision 2030’s section outlining its ambitions for the ‘non-profit sector’ gives an idea of how this will affect civil society in Saudi Arabia. The section outlines ambitions for a stronger non-profit sector, and for strengthening “the organization of our social and compassionate work”. While this seems like a good environment for civil society to flourish, the vision also emphasizes that the sector needs to “adhere to relevant laws, executive regulations, and effective practices of governance” (Kingdom of Saudi Arabia, 2021, p. 66). The Saudi government wants the non-profit sector aligned with their ideology, and through an ISA fortified

by foreign Big Tech's technologies their capabilities to mold civil society to repress dissent can be said to be strengthened.

The concept of RSA is closely linked to the notion of *material* infrastructure, as it includes the government structure and its administration, police and prisons. It relates to the physical repression that the state has the power to exert. A majority of the data center infrastructure projects outlined in Table 2 of the last section were undertaken by the foreign Big Tech in close collaboration with government institutions. For example, Google Cloud's data centers in Saudi Arabia are built in collaboration with Saudi state-owned company 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 (Aramco, 2020). Also in Saudi Arabia, Oracle will build their most recently announced cloud region in partnership with the Saudi Ministry of Communications and Information (Swinhoe, 2023a). In the UAE, Huawei will build one of their data centers in collaboration with the Abu Dhabi municipality (Huawei, 2020).

In other cases, we can identify an even more direct integration of the Big Tech companies' technologies into the state structures. In Bahrain, the government expects to "gradually migrate government entities to AWS [Amazon] and eventually have most government data centers shut down" (Data Center Dynamics, 2019). In Oman, the government 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" (Oracle, 2022). In these cases the physical infrastructure constructed by the foreign Big Tech companies become part of the governments' infrastructure itself, and directly become a part of the states' RSA.

Results of analysis

This analysis, first of all, brings to the table that the GCC states indeed have a history of carrying out digital authoritarian practices - mainly the practices of "monitoring citizens and identifying dissidents" and "social manipulation and disinformation". Especially relevant is the fact that the governments have shown that they are not reluctant to exploit technologies by foreign companies in order to carry out these practices.

The quantitative mapping of Table 1 shows that all six of the GCC states have implemented national vision frameworks with corresponding objectives of digitalization, digital government strategies and economic policies enhancing privatization and increased financial investment. The corresponding case study of Saudi Vision 2030 exposes how the framework includes the provisions of deployment of AI and Big Data technologies in key government services, and that foreign Big Tech companies are committing to providing the governments with the needed technologies.

The quantitative mapping of Table 2 makes evident a sharp increase in foreign Big Tech companies investing in data center and cloud computing infrastructure in the Gulf states since 2018. It maps out nine companies: from the US, Google, Amazon, Microsoft, IBM, Oracle and Equinix; and from China, Alibaba, Huawei and Tencent. Through exposing the principles of data localization and data sovereignty, this analysis asserts that this trend will have the consequence that much more user data will be processed in, and subject to, the jurisdiction of the Gulf governments. The lack of transparency of these investments, however, makes it impossible to quantify exactly the increased computing power that will be located in the Gulf. From the quantified amount of data centers built, however, it can be identified as Saudi Arabia and the UAE are the countries increasing their capacities the most through this trend.

The analysis further shows that through these investments, as most of the data centers are built in partnership with government entities of the Gulf, the governments will have a high degree of control over the infrastructure and the data that is stored and processed through it. In some cases, such as in Bahrain and Oman, the infrastructure will even directly become part of the structure of the governments. In all cases, the governments will have legal control over the data stored and processed through the data centers located within their geographical jurisdiction.

Conclusions

This paper concludes that the Gulf governments' capacity to carry out digital authoritarianism will increase through the investments made by foreign Big Tech companies. As their state apparatuses integrate the digital infrastructure provided by the 'surveillance capitalist companies', the governments will have increased their capacities to reach the objectives outlined in their national vision frameworks. The GCC states' history of digital authoritarianism evidences that their political leaders have in different ways repressed the digital space of the WANA region, routinely violated the privacy and right to freedom of expression of its citizens and been willing to use brutal methods to silence dissidents.

They have not been reluctant to exploit technologies from foreign companies to do so. Foreign Big Tech companies invest in vast data center capacities in the region, attracted by the economic incentives enforced through the GCC states' 'neoliberal political projects'. In their ventures, they are showing blatant disregard for the history these states have of violating the human rights of privacy and right to freedom of expression.

Thus, this paper has discussed three main ways in which the capacities of the GCC governments to carry out digital authoritarianism will increase as a consequence of these investments:

1. Data centers built within the geographical borders of the states localize the data of its population. The data center capacity of the GCC countries before 2018 was not very developed, but over the past five years foreign Big Tech companies are providing the necessary infrastructure to localize the data of the population. As the implementation of PDPLs assert data sovereignty of this data, the GCC governments will have the legal control over this data. The PDPLs contain vague language exempting the law from applying in certain cases, which means that the governments will have agency to do as they want with this data.
2. In combination with increased data storage capacities, the transfers of surveillance capitalist technologies from the Big Tech companies provides the GCC governments with the means to more closely monitor and surveil its citizens. The governments have in their national vision frameworks outlined strategies to digitalize many sectors of society, including the deployment of AI strategies in

education and health and the implementation of Big Data in government. This paper has conceptualized that these technologies become a part of, and fortify, the governments' ISAs. The technologies become part of the states' own structure, and fundamentally change the means of communication between the governments and the citizens in a way that increases the legibility of society, allowing the governments to more effectively identify discontent and potential dissidents before they express themselves publicly.

3. Adding to this, the shared ownership that the GCC governments will have of many of the data centers implies a direct integration of the infrastructure into the structures of these states. In some cases, government entities will run their operations through these data centers, meaning that the infrastructure will become part of the RSAs of the states. This fortifies the material capacities that the GCC governments have at their disposal to repress dissidence.

The research has kept a fundamental focus on material capabilities and infrastructure, and provided insight into the congruence between the digital infrastructure and technological capabilities exploited in both digital authoritarianism and 'surveillance capitalism'. Capacity to store large quantities of data is essential, and AI represents the most significant advances within the capacities of both systems. The transfer of AI, Machine Learning and Big Data technologies from the Big Tech companies to the GCC governments is a significant development involving powerful actors and powerful technologies. This paper has intended to analyze this development through sustaining an IPE approach, emphasizing the relationships and connections between state actors (GCC governments) and economic agents (foreign Big Tech). Both sets of actors are relatively opaque in their dealings, and precise numbers about scope and scales of investments are not publicly available.

More work needs to be done to improve transparency, and further research should be conducted about the increasingly close relationship between the biggest companies in the world and the authoritarian regimes of the Gulf. Furthermore, as this paper has highlighted the principle of data localization, it is likely that the personal data of individuals in the wider WANA region will also have their data stored and processed through data centers within the GCC countries' jurisdiction. Thus, further research should also be done inquiring the implications that the

increasing data center capacity in the GCC have for the ecosystem of personal data in the wider WANA region.

Bibliography

Abrougui, Afef & Mohamad Najem (n.d.). "Follow the Money for Better Digital Rights in the Arab Region". *Middle East Political Science.* https://pomeps.org/follow-the-money-for-better-digital-rights-in-the-arab-region

Alibaba (2016, November 21) "Alibaba Cloud has Launched Data Center in Dubai". Alibaba Cloud. https://www.alibabacloud.com/startup/events/dubai-launch

Al Jazeera (2020, December 21). "Al Jazeera journalists hacked using Israeli firm's spyware". *Al Jazeera.* https://www.aljazeera.com/news/2020/12/21/al-jazeera-journalists-hacked-by-spyware-sold-by-israeli-firm

Al Naqbi, Hassan (2018). "Companies looking to host their data in the Middle East should look at the United Arab Emirates". Data Center Dynamics. https://www.datacenterdynamics.com/en/opinions/considerations-moving-data-middle-east/

Althusser, Louis (1971), *Ideology and Ideological State Apparatuses (Notes towards and Investigation).* Marxist.org. https://www.marxists.org/reference/archive/althusser/1970/ideology.htm

Amazon (2019) "Now Open: AWS Middle East (UAE) Region". AWS. https://docs.google.com/document/d/1A19JgYtADaCdJ2QpN8o87nDII-lFB3R6GjIlELWmgd8/edit

Amazon (2020, May 18) "Announcing availability of AWS Outposts in United Arab Emirates and Kingdom of Saudi Arabia". AWS. https://aws.amazon.com/about-aws/whats-new/2020/05/announcing-availability-of-aws-outposts-united-arab-emirates-kingdom-of-saudi-arabia/

Amazon (2022, August 29) "Now Open - AWS region in the United Arab Emirates (UAE). AWS. https://aws.amazon.com/blogs/aws/now-open-aws-region-in-the-united-arab-emirates-uae/

Amnesty (2022)."Silence is king: the persecution of activists in the GCC". *Amnesty International.* https://www.amnesty.org/en/latest/campaigns/2022/10/silence-is-king-the-persecution-of-activists-in-the-gulf/

Arab News (2022). “Tech giant Google Cloud opens new center to train Saudis on digital technologies”. Arab news. https://www.arabnews.com/node/2200246/business-economy

Aramco (2020). “Aramco to bring Google Cloud Services to Saudi Arabia”. Aramco. https://www.aramco.com/en/news-media/news/2020/aramco-to-bring-google-cloud-services-to-saudi-arabia

Azam, Muzaffer (2022). “Alibaba Cloud Services in Saudi Arabia”. Alibaba Cloud. https://www.alibabacloud.com/blog/alibaba-cloud-services-in-saudi-arabia_599248

Bahraini government (2008), “Bahrain Economic Vision 2030”. *Bahrain.* https://www.bahrain.bh/wps/portal/!ut/p/a1/lZJfT8IwFMW_ijzscf

Borger, Julian (2022). “Ex-Twitter employee found guilty of spying on Saudi dissidents”. The Guardian. https://www.theguardian.com/us-news/2022/aug/09/twitter-saudi-arabia-dissident-spying

Borgman, Christine (2017). *Big Data, Little Data, No Data.* Cambridge (MA): The MIT Press.

Bradshaw, Samantha, & Philip Howard (2018). “The Global Organization of Social Media Disinformation Campaigns”. *Journal of International Affairs,* Vol 81 (1.5), pp. 23-32. https://www.jstor.org/stable/26508115

Brannon, Ike, & Hart Schwartz (2018). “The New Perils of Data Localization Rules”. *Regulation,* Vol 41(2), pp. 12-13. https://csuc-url.primo.exlibrisgroup.com/permalink/34CSUC_URL/4pe823/cdi_proquest_miscellaneous_2063806137

Cammett, Melani, Ishac Diwan, Alan Richards, & John Waterbury (2015). *A Political Economy of the Middle East.* Oxfordshire: Routledge.

Christl, Wolfie (2017). “Corporate Surveillance in Everyday Life”. *Cracked Labs.* https://crackedlabs.org/en/corporate-surveillance

Cochrane, Paul (2023, April 5). “How Saudi Arabia is redrawing the map of the future with fiber-optic cables”. *Middle East Eye.* https://www.middleeasteye.net/news/saudi-arabia-fibre-optic-cables-internet-future-map-redrawing

Companies Market Cap (2023, May 2) “Largest Companies by Market Cap”. https://companiesmarketcap.com/

Constantine, Nay (2022). “UAE’s Data Protection Law: Between Exceptions and Exemptions”. *SMEX*. https://smex.org/uaes-data-protection-law-between-exceptions-and-exemptions/

Crittenden, W., & I. Biel (2019). “Embracing digitalization: student learning and new technologies”. *J. Mark. Educ.* 41(1), 5–14 (2019). https://www.sciencedirect.com/science/article/pii/S2214629618301051

Data & Society (n.d.). “Efforts to exploit technical, social, economic, and institutional configurations of media can catalyze social change, sow dissent, and challenge the stability of social institutions.” *Data & Society.* https://datasociety.net/research/media-manipulation/

Data Center Dynamics (2017, January 4) “Ooredoo opens new data center floor in Qatar”. https://www.datacenterdynamics.com/en/news/ooredoo-opens-new-data-center-floor-in-qatar/

Data Center Dynamics (2018, October 26) “Huawei to build Tier III data center for Bahrain’s Batelco”. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/huawei-to-build-tier-iii-data-center-for-bahrains-batelco/

Data Center Dynamics (2019, July 30) “AWS opens first Middle Eastern Region in Bahrain”. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/aws-opens-first-middle-eastern-region-bahrain/

Data Center Dynamics (2021a, December 3) “Google Cloud’s Saudi Arabian data center will be built in Dammam”. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/google-clouds-saudi-arabian-data-center-will-be-built-in-dammam/

Data Center Dynamics (2021c, April 20) “Microsoft’s Israel data center reportedly delayed to 2022”. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/microsofts-israel-data-center-reportedly-delayed-to-2022/#:~:text=Microsoft%20has%20delayed%20the%20planned,between%20Tel%2DAviv%20and%20Jerusalem

Data Center Dynamics (2021d, October 28) “Oracle to launch cloud region in Saudi Arabia’s Neom city”. Data Center Dynamics.

https://www.datacenterdynamics.com/en/news/oracle-to-launch-cloud-region-in-saudia-arabias-neom-city/#:~:text=Oracle%20opened%20its%20first%20Saudi,including%20a%20second%20Saudi%20region

Data Center Dynamics (2022, August 3) “Ooredoo breaks ground on three data centers in Oman”. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/ooredoo-breaks-ground-on-three-data-centers-in-oman/

Data Center Map (n.d.). https://www.datacentermap.com/. Data Center Map.

Eck, Aksel (2022). “Implications of Big Tech data center infrastructure in the Gulf”. *SMEX*. YouTube video, 27:55. https://www.youtube.com/watch?v=ZdQtOXGmGGE&t=9s

El-Masry, Ahmed (2021, March 31). “The data centers industry: The GCC’s new oil fields”. *Middle East Institute.* https://www.mei.edu/publications/data-centers-industry-gccs-new-oil-fields

Equinix (n.d.). “Build your hybrid multicloud environment and increase customer satisfaction through secure connections to Google Cloud”. *Equinix.* https://www.equinix.se/partners/google-cloud

Equinix (2021) “Dubai Data Centers”. Equinix. https://www.equinix.se/data-centers/europe-colocation/united-arab-emirates-colocation/dubai-data-centers

Equinix (2022a) “Why Choose our Muscat Data Center?” Equinix. https://www.equinix.om/data-centers

Equinix (2022b) “Equinix to build first data center in Salalah, Oman”. Equinix. https://www.equinix.ae/newsroom/press-releases/2022/03/equinix-to-build-first-data-center-in-salalah-oman

Feldstein, Steven (2021). *The Rise of Digital Repression*. Oxford: Oxford University Press. DOI: 10.1093/oso/9780190057497.003.0002

Fontaine, Richard, & Kara Frederick (2019, March 15). “The Autocrat’s New Tool Kit”. *The Wall Street Journal.* https://www.wsj.com/articles/the-autocrats-new-tool-kit-11552662637

Frantz, Erica, Andrea Kendall-Taylor, & Joseph Wright (2020). “Digital Repression in Autocracies”. V-Dem Institute, March, pp. 1-22.

Freedom House (2022). “Freedom on the Net report: Countries”. *Freedom House.* https://freedomhouse.org/countries/freedom-net/scores

Freedom House (2021). “Freedom on the Net: Saudi Arabia”. *Freedom House.* https://freedomhouse.org/country/saudi-arabia/freedom-net/2021

Gartner (2021). “Gartner Forecasts End User Spending on Public Cloud Services in MENA to Grow 19% in 2022”. Gartner. https://www.gartner.com/en/newsroom/press-releases/2021-10-27-mena-public-cloud-spending-forecast-2022

Gartner (2022). “Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 billion in 2023”. Gartner. https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023

Google (2021a). “Expanding our infrastructure with cloud regions around the world”. Google. https://cloud.google.com/blog/products/infrastructure/google-cloud-platform-region-updates

Google (2021b) “Google Cloud selected to provide cloud services to digitally transform the State of Israel”. Google Cloud. https://cloud.google.com/blog/topics/inside-google-cloud/google-cloud-selected-to-provide-cloud

Google Books Ngram Viewer (2019). “‘Data localization’, ‘Data sovereignty’, (1980-2019)”. *Google Books*. https://books.google.com/ngrams/graph?content=digital+authoritarianism&year_start=1980&year_end=2019&corpus=en-2019&smoothing=3

Google Books Ngram Viewer (2019). “Digital Authoritarianism (1980-2019)”. *Google Books*. https://books.google.com/ngrams/graph?content=digital+authoritarianism&year_start=1980&year_end=2019&corpus=en-2019&smoothing=3 -services-to-the-state-of-israel

Gulf Cooperation Council (n.d.), “About GCC”. *GCC.* https://www.gcc-sg.org/en-us/AboutGCC/Pages/StartingPointsAndGoals.aspx

Gulf News (2022, August 7) “Huawei signs off on Saudi data centre investment, set to finalise location”. Gulf News.

https://gulfnews.com/business/huawei-signs-off-on-saudi-data-centre-investment-set-to-finalise-location-1.89774910

Gunitsky, Seva (2016). "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability". *Perspectives on Politics,* Vol 13 (1), pp. 42-54. https://www.cambridge.org/core/journals/perspectives-on-politics/article/corrupting-the-cybercommons-social-media-as-a-tool-of-autocratic-stability/CD2CCFAB91935ED3E533B2CBB3F8A4F

Harvey, David (2007). *A Brief History of Neoliberalism.* Oxford: Oxford Academic

Herr, Trey (2020, August 31). "Four myths about the cloud: The geopolitics of cloud computing". *Atlantic Council.* https://www.atlanticcouncil.org/in-depth-research-reports/report/four-myths-about-the-cloud-the-geopolitics-of-cloud-computing/

Huawei (n.d.). "Building a Digital Oasis for Saudi Arabia". Huawei. https://e.huawei.com/en/case-studies/industries/government/2020/a-digital-oasis-for-saudi-arabia

Huawei (2020) "Building a Municipal Data Center for the 'Pearl' in the South Coast of the Arabian Gulf". Huawei. https://e.huawei.com/en/case-studies/industries/government/2020/abu-dhabi-municipality-smart-modular-dc

IBM (2022, January 7) "IBM Services Introduces Two Data Centers in the UAE to Help Accelerate Customer Journeys to Hybrid Cloud". IBM Newsroom. https://mea.newsroom.ibm.com/2020-01-07-IBM-Services-Introduces-Two-Data-Centers-in-the-UAE-to-Help-Accelerate-Customer-Journeys-to-Hybrid-Cloud

Jamil, Sadia (2022). "Postulating the Post-Arab Spring Dynamics of Digital Journalism in the Middle East". *Digital Journalism,* Vol 10 (7), pp. 1257-1261. https://www.tandfonline.com/doi/abs/10.1080/21670811.2022.2040040?role=button&needAccess=true&journalCode=rdij20

Jones, Marc Owens (2022). *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media.* London: Hurst Publishers.

Jurayevich, Mahmudov Baxriddin & Mullabayev Baxtiyarjon Bulturbayevich (2022). "The Impact of the Digital Economy on Economic Growth". *International Journal of Business, Law, and Education,* vol 1(1), pp. 4-7.

http://download.garuda.kemdikbud.go.id/article.php?article=1965582&val=20970&title=THE%20IMPACT%20OF%20THE%20DIGITAL%20ECONOMY%20ON%20ECONOMIC%20GROWTH

Khalil, Lydia (2020). *Digital Authoritarianism, China and COVID*. Lowy Institute Analysis. https://www.jstor.org/stable/pdf/resrep27665.pdf?acceptTC=true&coverpage=false&addFooter=false

Kingdom of Saudi Arabia (2016a) "Saudi Vision 2030". *Saudi Vision 2030.* https://www.vision2030.gov.sa/media/rc0b5oy1/saudi_vision203.pdf

Kingdom of Saudi Arabia (2016b). "Vision Realization Programs". *Saudi Vision 2030*. https://www.vision2030.gov.sa/

Kingdom of Saudi Arabia (2020). "Smart Government Strategy". *United National Platform*. https://www.my.gov.sa/wps/portal/snp/aboutksa/smartstrategy

Kingdom of Saudi Arabia (2021). "National Transformation Program: Delivery Plan 2021-2025". *National Transformation Program*. https://www.vision2030.gov.sa/media/nhyo0lix/ntp_eng_opt.pdf

Kuwaiti government (2017), "Kuwait vision 2035: New Kuwait". *Kuwait.* https://www.mofa.gov.kw/en/kuwait-state/kuwait-vision-2035/

Margetts (2006). "Transparency and Digital Government". In Christopher Hood, and David Heald (eds), *Transparency: The Key to Better Governance?*. British Academy, London. https://doi.org/10.5871/bacad/9780197263839.003.0012

Matheus, Ricardo, Marji Janssen & Tomasz Janowski (2021). "Design principles for creating digital transparency in government". *Government Information Quarterly,* vol. 38 (1). https://www.sciencedirect.com/science/article/pii/S0740624X20303294#s0030

Microsoft (2018, May 8) "Microsoft introduces Azure Stack in Saudi Arabia with Sahara Net and Lenovo". Microsoft News. https://news.microsoft.com/en-xm/2018/05/08/microsoft-introduces-azure-stack-in-saudi-arabia-with-sahara-net-and-lenovo/

Microsoft (2019, June 19) “Microsoft Cloud datacenter regions now available iin the UAE to help fuel the Middle East’s future economic ambitions”: Microsoft News. https://news.microsoft.com/en-xm/2019/06/19/microsoft-cloud-datacenter-regions-now-available-in-the-uae-to-help-fuel-the-middle-easts-future-economic-ambitions/

Microsoft (2022a, May 17) “Microsoft Azure UAE Regions launched four new key services to accelerate digital transformation programmes”. Microsoft News. https://news.microsoft.com/en-xm/2022/05/17/microsoft-azure-uae-regions-launches-four-new-key-services-to-accelerate-digital-transformation-programmes/

Microsoft (2022b, August 31) “Microsoft opens first global datacenter region in Qatar, bringing new opportunities for a cloud-first economy”. Microsoft News. https://news.microsoft.com/en-xm/2022/08/31/microsoft-opens-first-global-datacenter-region-in-qatar-bringing-new-opportunities-for-a-cloud-first-economy/

Microsoft (2022c). “Oracle and Microsoft announce availability of Oracle Database Service for Microsoft Azure”. *Microsoft.* https://news.microsoft.com/2022/07/20/oracle-and-microsoft-announce-availability-of-oracle-database-service-for-microsoft-azure/

Moro Hub (2021) “Moro Hub signs an agreement with Huawei to build the first phase of the largest solar powered data centre in the Middle East and Africa”. Moro Hub. https://www.morohub.com/en/blog/moro-hub-signs-an-agreement-with-huawei-to-build-the-first-phase-of-the-largest-solar-powered-data-centre-in-the-middle-east-and-africa/

Morgues, Robert (2019). *Artificial Intelligence, China, Russia, and the Global Order.* Alabama: Air University Press. https://www.jstor.org/stable/pdf/resrep19585.17.pdf

Morley, J., Widdicks, & I. Hazas: “Digitalisation, energy and data demand: the impact of internet traffic on overall and peak electricity consumption”. *Energy Res.* Soc. Sci. 38(1), 128–137. https://www.sciencedirect.com/science/article/pii/S2214629618301051

Moss, Sebastian (2018). “WikiLeaks publishes list of AWS data center locations, colo providers”. *Data Center Dynamics.* https://www.datacenterdynamics.com/en/news/wikileaks-publishes-list-aws-data-center-locations-colo-providers/

National Strategy for Data & AI (n.d.). “National Strategy for Data & AI”. *Kingdom of Saudi Arabia.* https://ai.sa/

NORC (2021). *Digitized Autocracy Literature Review*. Chicago: U.S. Agency for International Development. https://pdf.usaid.gov/pdf_docs/PA00XV9R.pdf

Omani government (2021), "Vision Document". *Oman.* https://www.mof.gov.om/pdf/Vision_Documents_En.pdf

Oracle (n.d.). "About Oracle". Oracle. https://www.oracle.com/in/corporate/

Oracle (2022, June 22) "Sultanate of Oman Achieves Major Digital Milestone on Journey to National Vision 2040 Supported by Oracle." Oracle. https://www.oracle.com/kw/news/announcement/sultanate-oman-achieves-major-digital-milestone-with-oracle-2022-06-22/

O'Toole, Megan (2022). "Digital authoritarianism: The rise of electronic armies in the Middle East". Middle East Eye. https://www.middleeasteye.net/opinion/middle-east-digital-authoritarianism-electronic-armies-rise

Parviainen, P., & M Kääriäinen (2017). "Tackling the digitalization challenge: how to benefit from digitalization in practice." *IJISPM* 5(1), 63–77. https://www.researchgate.net/publication/315830926_Tackling_the_digitalization_challenge_How_to_benefit_from_digitalization_in_practice

Polyakova, Alina, & Chris Meserole (2019). "Exporting Digital Authoritarianism: The Russian and Chinese models". *Brookings.* https://www.brookings.edu/research/exporting-digital-authoritarianism/

Qatar Government (2008), "Qatar National Vision 2030". *Qatar.* *https://www.gco.gov.qa/en/about-qatar/national-vision2030/*

Qatar Government Communications Office (2021), "Economic Policy". *Qatar.* https://www.gco.gov.qa/en/focus/economic-policy/

Qu, Tracy (2022). "Alibaba's cloud services business launches two new data centres in Saudi Arabia to step up its overseas expansion": South China Morning Post. https://www.scmp.com/tech/big-tech/article/3180915/alibabas-cloud-services-business-launches-two-new-data-centres-saudi

Rahme, Marianne (2022). “Data Protection In Saudi Arabia: Comparative Analysis”. *SMEX.* https://smex.org/data-protection-in-saudi-arabia-comparative-analysis/

Roberts, Margaret (2018). *Censored: Distraction and Diversion Inside China’s Great Firewall.* New Jersey: Princeton University Press.

Salam, Rahmat, Marja Sinurat, Izzatussolekha, Akhmad Yasin, Rian Sacipto (2023). “Implementation of Artificial Intelligence in Governance: Potential and Challenges”. *Influence: International Journal of Science Review,* vol 5(1), pp. 243-255. https://influence-journal.com/index.php/influence/article/view/122

Saudi Press Agency (2022). “Saudi Cloud Computing Company Launches services in the region”. Zawya. https://www.zawya.com/en/business/technology-and-telecom/saudi-coud-computing-company-launches-services-in-the-region-k3g8dug2

Srai, J., & H. Lorentz (2019). “Developing design principles for the digitalisation of purchasing and supply management.” *J. Purch. Supply Manag*. 25(1), 78–98. https://www.repository.cam.ac.uk/items/bca241a1-7420-4e11-970c-ef997c12896f

Stahl, Bernd Carsten, Doris Schroeder & Rowena Rodrigues (2022). “Surveillance Capitalism”. *Ethics of Artificial Intelligence,* pp. 39-52. https://link.springer.com/chapter/10.1007/978-3-031-17040-9_4

Swinhoe, Dan (2023a). “Oracle announces plans for third Saudi Arabia cloud region”. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/oracle-announces-plans-for-third-saudi-arabia-cloud-region/

Swinhoe, Dan (2023b). “Huawei hosts Saudi cloud region in Center3 data center”. Data center Dynamics. https://www.datacenterdynamics.com/en/news/huawei-to-host-saudi-cloud-region-in-center3-data-center/

Swinhoe, Dan (2023c). “Microsoft plans new data center and cloud region in Saudi Arabia”. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/microsoft-planning-new-data-center-and-cloud-region-in-saudi-arabia/

Taylor, Richard (2020). “”Data localization”: The internet in the balance”. *Telecommunications policy*, Vol 44(8). https://csuc-url.primo.exlibrisgroup.com/permalink/34CSUC_URL/4pe823/cdi_proquest_journals_2449985338

Terman, Rochelle (n.d.). “Internet Censorship (Part 1): The Technology of the Working Web”. *Townsend Center, University of California, Berkeley.* https://townsendcenter.berkeley.edu/blog/internet-censorship-part-1-technology-working-web

Toro-Garcia, Andrès Felipe, Cristian Camilo Gutierrez-Vargas & Luis Carlos Correa-Ortiz (2021 “Digital Government Strategy for the Construction of More Transparent and Proactive Governments”. *Trilogìa ciencia Tecnologìa Sociedad,* vol. 12 (22), pp. 60-91. http://www.scielo.org.co/scielo.php?pid=S2145-77782020000100060&script=sci_abstract

UAE government (2021). “‘We the UAE 2031’ vision”. *UAE.* https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/innovation-and-future-shaping/we-the-uae-2031-vision

United Nations (1948). “Universal Declaration of Human Rights”. United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012,against%20such%20interference%20or%20attacks.

Valle-Cruz, David, Edgar Alejandro Ruvalcaba-Gomez, Rodrigo Sandoval-Alamazan, Ignacio Criado (2019). “A Review of Artificial Intelligence in Government and its Potential from a Public Policy Perspective”. *20th Annual International Conference on Digital Government Research,* pp. 91-99. https://doi.org/10.1145/3325112.3325242

Wessels, Josepha (2020). “Authoritarianism, Digital Dissidence and Grassroots Media in the Middle East and North Africa region”. *CyberOrient*, Vol 13 (1), pp. 4-27. https://anthrosource.onlinelibrary.wiley.com/doi/abs/10.1002/j.cyo2.20191301.0001

World Bank (2023, March 31). “Digital Development”. *World Bank.* https://www.worldbank.org/en/topic/digitaldevelopment/overview

Yahoo (2022, June 9) “Alibaba’s cloud services business launches two new data centres in Saudi Arabia to step up its overseas expansion”. Yahoo Finance. https://finance.yahoo.com/news/alibabas-cloud-services-business-launches-093000504.html?guccounter=1&guce_referrer=

Zawya (2022a). “Google Cloud launches center of excellence in Saudi Arabia to develop in-demand cloud skills in the Kingdom”. Zawya. https://www.zawya.com/en/press-release/companies-news/google-cloud-launches-center-of-excellence-in-saudi-arabia-to-develop-in-demand-cloud-skills-in-the-kingdom-fglgl035

Zawya (2022b). “Saudi Cloud Computing Company launches services in the region”. *Zawya.* https://www.zawya.com/en/business/technology-and-telecom/saudi-coud-computing-company-launches-services-in-the-region-k3g8dug2

Zawya (2022c) “Middle East and North Africa data center market analysis and forecast 2019-2028. Zawya. https://www.zawya.com/en/press-release/research-and-studies/middle-east-and-north-africa-data-center-market-analysis-and-forecast-2019-2028-rg7659c7

Zhang, Mary (2023a, March 2). “Top 250 Data Center Companies in the World as of 2023”. *Dgtl Infra.* https://dgtlinfra.com/top-data-center-companies/

Zhang, Mary (2023b, March 15). “How Data Centers are enabling Artificial Intelligence”. *Dgtl Infra.* https://dgtlinfra.com/data-centers-artificial-intelligence-ai/#:~:text=Data%20centers%20provide%20vast%20computing,supporting%20AI%20applications%20and%20workloads

Zheng, Weiwei (2020). “Comparative Study on the Legal Regulation of a Cross-Border Flow of Personal Data and Its Inspiration to China”. *Frontiers of law in China, Vol 15 (3),* pp. 280-312. https://csuc-url.primo.exlibrisgroup.com/permalink/34CSUC_URL/4pe823/cdi_proquest_journals_2450655284

Zuboff, Shoshana (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs.