

# **DIGITAL SOVEREIGNTY IN THE MENA REGION: Overcoming Paradoxes to Ensure Digital Resilience**

**Julien Nocetti**  
Coordinator

**Amar Rouabhi**  
**Sara Baazobandi**  
**Chloé Berger**



**DIGITAL SOVEREIGNTY  
IN THE MENA REGION:  
Overcoming Paradoxes to  
Ensure  
Digital Resilience**

**Julien Nocetti**  
Coordinator

**Amar Rouabhi**  
**Sara Baazobandi**  
**Chloé Berger**

**EuroMeSCo** has become a benchmark for policy-oriented research on issues related to Euro-Mediterranean cooperation, in particular economic development, security and migration. With 126 affiliated think tanks and institutions and about 700 experts from 30 different countries, the network has developed impactful tools for the benefit of its members and a larger community of stakeholders in the Euro-Mediterranean region.

Through a wide range of publications, surveys, events, training activities, audio-visual materials and a strong footprint on social media, the network reaches thousands of experts, think tankers, researchers, policy-makers and civil society and business stakeholders every year. While doing so, EuroMeSCo is strongly engaged in streamlining genuine joint research involving both European and Southern Mediterranean experts, encouraging exchanges between them and ultimately promoting Euro-Mediterranean integration. All the activities share an overall commitment to fostering youth participation and ensuring gender equality in the Euro-Mediterranean experts' community.

**EuroMesCo: Connecting the Dots** is a project co-funded by the European Union (EU) and the European Institute of the Mediterranean (IEMed) that is implemented in the framework of the EuroMeSCo network. As part of this project, several Joint Study Groups are assembled each year to carry out evidence-based and policy-oriented research. The topics of the study groups are defined through a thorough process of policy consultations designed to identify policy-relevant themes.

## POLICY STUDY

Published by the European Institute of the Mediterranean

**Editing:** Marco Lagae Novković

**Policy Peer Reviewer:** Felice Simonelli

**Academic Peer Reviewer:** Anonymous

**Design layout** Maurin.studio

**Proofreading** Neil Charlton

**Layout** Núria Esparza

**Print** ISSN 2938-446X

**Digital** ISSN 2696-7626

August 2024



The **European Institute of the Mediterranean** (IEMed), founded in 1989, is a think and do tank specialised in Euro-Mediterranean relations. It provides policy-oriented and evidence-based research underpinned by a genuine Euromed multidimensional and inclusive approach.


The aim of the IEMed, in accordance with the principles of the Euro-Mediterranean Partnership (EMP), the European Neighbourhood Policy (ENP) and the Union for the Mediterranean (UfM), is to stimulate reflection and action that contribute to mutual understanding, exchange and cooperation between the different Mediterranean countries, societies and cultures, and to promote the progressive construction of a space of peace and stability, shared prosperity and dialogue between cultures and civilisations in the Mediterranean.

The IEMed is a consortium comprising the Catalan Government, the Spanish Ministry of Foreign Affairs, European Union and Cooperation, the European Union and Barcelona City Council. It also incorporates civil society through its Board of Trustees and its Advisory Council.

eur@mesco  
Policy Study

# Content

<b>Executive Summary</b>	<b>8</b>
<b>List of Acronyms and Abbreviations</b>	<b>12</b>
<b>Introduction</b>	<b>14</b>
<b>Chapter 1</b> Legal Frameworks for Digital Sovereignty in the MENA Region: Towards Policy Harmonisation?	<b>18</b>
<b>Chapter 2</b> Users' Digital Sovereignty in the Middle East and North Africa	<b>40</b>
<b>Chapter 3</b> Balancing Resilience and Innovation: How Do MENA Countries Manage Cyber-Related Challenges?	<b>52</b>
<b>Chapter 4</b> Disentangling the MENA Countries' Involvement in Cyber Sovereignty Debates	<b>70</b>
<b>Policy Recommendations</b>	<b>84</b>



# Executive Summary

The past decade has proven particularly rich in the debates and policy-making related to “digital sovereignty”, understood as the ability to act independently in the digital world – or balancing technological dependencies – by implementing protective mechanisms (regulation, etc.) and offensive tools to foster digital innovation (like building tech ecosystems, financing innovation, etc.). Security challenges related to digital sovereignty have grown significantly, affecting regions worldwide. These challenges include cyberattacks on critical infrastructures, sabotage and physical attacks on network infrastructures, disinformation, cyber espionage, and so on. Economic and industrial policy challenges also prove fundamental when it comes to asserting a desired digital sovereignty. Technological advancements in the digital realm have engendered novel synergies and collaborations, concurrently spawning new forms of competition, thereby adding complexity to the international shifting power dynamics. On a social level, in turn, the rapid dissemination of digital technologies has accelerated the empowerment of citizens, providing them with new opportunities – though exposing them to new forms of surveillance and repression.

More than digital technology itself, it is its ubiquity that is ultimately at stake, behind the idea of sovereignty: digital sovereignty concerns democratic, economic and social, commercial, industrial, defence and security issues all at once. Behind the economic issue, social models and their values are at stake. Taken in their entirety, these different areas, which in their own way call into question the integrity of the competences of states and the European Union (EU), as well as their autonomy, end up constituting something fundamental and existential for them and the EU: their independence, their ability to retain control over their most fundamental competences, and to apply the values that underpin their identity and structure social relations. Needless to say, there is no wide consensus on what digital sovereignty actually means. The Internet, which defies the control of any form of authority, is not universally perceived throughout the world as a means of promoting the emancipation of peoples, an approach that concerns its cognitive layer. Distinct from the European conception, digital sovereignty as envisaged by some authoritarian regimes places the emphasis on preserving “national” informational space from foreign influences perceived as subversive.

The Middle East and North Africa (MENA) region illustrates a digital sovereignty paradox. On the one hand, it can be considered as a fertile “laboratory” to observe trends in the three above-mentioned dimensions (security and diplomacy, economic policies, citizen empowerment), while reflecting on these states’ adoption of digital tools. On the other hand, the MENA region appears as a “blind spot” on the global map of digital sovereignty debates. Global narratives tend to

focus on the Sino-United States (US) competitive framework – with the EU as a counterpoint – and on the so-called Global South. In the latest case, Sub-Saharan Africa seems to attract a relatively more significant part of policy-related analysis and media coverage.

This policy study seeks to go beyond this seemingly apparent by focusing on four case studies that aim to analyse digital sovereignty opportunities and threats in the MENA region, while maintaining a holistic approach to the issue, as digital sovereignty may often be perceived differently from the various region's capitals.

In the first chapter, the concept of digital sovereignty has emerged as a pivotal concern within the MENA region, underscoring the necessity for nations to navigate the complexities of the digital era with autonomy and strategic foresight. This concern is particularly pressing given the varying degrees of digital readiness and infrastructure development across the region, which have resulted in notable disparities in digital capabilities. Countries in the Gulf, notably the United Arab Emirates (UAE), Qatar, Saudi Arabia, and Kuwait, have distinguished themselves through robust digital infrastructure, creating a discernible divide not only with their North African counterparts but also with other nations within the Middle East itself.

In the second chapter, digital technology has been an empowering tool for social enterprise and civic activism. Particularly in relation to gender issues and financial technology, the digital realm has provided unique opportunities to the users across the board in the region. Several examples demonstrate how MENA citizens have used their autonomy and self-determination to lead social debates and shift traditional mindsets. However, the risk-averse mindset of local ruling elites turn most digital policies towards citizens' controlling strategies.

The third chapter sheds light on how the proliferation of digital technologies appears as a new source of vulnerabilities for state actors in the region, raising questions about how they seek to “domesticate” and weaponise these technologies to consolidate their authority. In this regard, the effects of cooperation, synergy, differentiation, or rivalry related to digital sovereignty could redraw the fault lines of the MENA regional security complex. To defuse misunderstandings about the supposed European “digital agenda” towards the region, EU institutions could initiate a dialogue with some MENA countries regarding the establishment of common technological norms and standards aimed at fostering MENA countries' sovereignty, autonomy and independence in the digital realm.

In the fourth and last chapter, security considerations significantly inform MENA states' role and initiatives in the global conversation on digital sovereignty-related matters. Some countries of the region contribute to all the global cybersecurity diplomacy processes – particularly Saudi Arabia, the UAE and Egypt. By contrast, MENA states have been far less prevalent in global multistakeholder cybersecurity initiatives over the past few years, showing an inclination to state-centric interactions. The regional debates on digital sovereignty and security also remain dominated by Gulf monarchies, illustrating profound imbalances within the area – which further complicates EU policy initiatives and responses.



This complex landscape – beyond obvious risks, especially when situations in Gaza and Lebanon remain dramatic – provides the EU with noticeable opportunities to advance a stronger resilience of the MENA's digital ecosystems. Digital infrastructures, education systems and implementation of the policy narratives are suggested as the main domains the EU external policy could build on to advance its own interests and harmonise its relationships with the Southern Neighbourhood.



# **List of Acronyms and Abbreviations**

<b>AHC</b>	Ad Hoc Committee
<b>ARCC</b>	Arab Region Cybersecurity Centre
<b>AI</b>	Artificial Intelligence
<b>BNPL</b>	Buy-Now-Pay-Later
<b>CCC</b>	Cloud Cybersecurity Controls
<b>CRI</b>	Counter Ransomware Initiative
<b>DESI</b>	Digital Economy and Society Index
<b>DMA</b>	Digital Markets Act
<b>DSA</b>	Digital Services Act
<b>DIFC</b>	Dubai International Financial Centre
<b>ESCWA</b>	Economic and Social Commission for Western Asia
<b>EU</b>	European Union
<b>GDPR</b>	General Data Protection Regulation
<b>GIGA</b>	German Institute for Global and Area Studies
<b>GCF</b>	Global Cybersecurity Forum
<b>GCI</b>	Global Cybersecurity Index
<b>GII</b>	Global Innovation Index
<b>GKI</b>	Global Knowledge Index
<b>GSMA</b>	Global System for Mobile Communications Association
<b>GAFAM</b>	Google, Apple, Facebook, Amazon, and Microsoft
<b>GDP</b>	Gross Domestic Product
<b>GCC</b>	Gulf Cooperation Council
<b>ICT</b>	Information and Communications Technology
<b>IFRI</b>	Institut français des relations internationales
<b>ITU</b>	International Telecommunications Union
<b>UIR</b>	International University of Rabat
<b>IGF</b>	Internet Governance Forum
<b>IAI</b>	Israel Aerospace Industries
<b>IDF</b>	Israel Defence Forces
<b>KSA</b>	Kingdom of Saudi Arabia
<b>MENA</b>	Middle East and North Africa
<b>NCA</b>	National Cybersecurity Authority
<b>NATO</b>	North Atlantic Treaty Organization
<b>OEWG</b>	Open-Ended Working Group
<b>OIC</b>	Organization of Islamic Cooperation
<b>SSL</b>	Secure Sockets Layer
<b>SME</b>	Small and Medium-Size Enterprises
<b>IRGC</b>	The Islamic Revolutionary Guard Corps
<b>TLS</b>	Transport Layer Security
<b>UAE</b>	United Arab Emirates
<b>UK</b>	United Kingdom
<b>UN</b>	United Nations
<b>US</b>	United States
<b>UAV</b>	Unmanned Aerial Vehicle
<b>VPN</b>	Virtual Private Network

# Introduction

Over the past decade, the notion of digital sovereignty has emerged as a central theme in policy discussions surrounding digital issues. It has gained popularity not only in centralised or authoritarian regimes but also in democratic nations. Nevertheless, the concept remains the subject of intense debate.

In the Middle East and North Africa (MENA) region, digital sovereignty as a concept and a political leverage has been variously understood. The digital economy has been identified as a potent catalyst for modernising local economies. The MENA region – with the exception of Israel – is still lagging behind the world's main economies and blocs when it comes to digital innovation and the presence of indigenous private companies in the sector. As such, this study seeks to explore these topics by blending four inter-related dimensions – legal/policy, socioeconomic, infrastructural/security-oriented, and diplomatic – to address the MENA region's challenges and prospects in digital sovereignty. A particular emphasis is put on the European Union (EU)'s opportunities for engagement with its Southern Neighbourhood when it comes to commercial ties, citizen's online privacy, infrastructure development, industry standards, policies, and so on, in a context of rising Sino-US competition in the technological arena.

Digital sovereignty is not merely the assertion of sovereignty online. The last few decades have taught us that the Internet changes the nature of sovereignty in a variety of ways. First, because of the global nature of the Internet, digital sovereignty almost always has global implications, whether it involves speech regulation, privacy, consumer protection, competition concerns, or law enforcement; thus, digital sovereignty can create significant roadblocks to one of the Internet's key virtues – its empowering

of global connections. Second, because the digital sphere is intermediated by corporations, the assertion of digital sovereignty typically occurs vis-à-vis corporations, not governments. Third, because daily life is increasingly permeated by the Internet, digital sovereignty can offer governments surveillance tools that far exceed any history has previously provided. Fourth, because of the dominance of the United States (US)'s technology companies globally, governments can readily weaponise the development and strengthening of their digital sovereignty to pursue protectionist goals.

As such, digital sovereignty encompasses three key dimensions: the state, the economy, and the individual, as outlined by Pohle and Thiel (2020). However, it is more of a discursive practice within the realm of politics and policy rather than a concrete legal or organisational framework – though some observers advanced the idea that European digital sovereignty could be construed around four main principles: act, access, cooperate, and own. Act refers to the ability of the EU and its member states to act in a manner unfettered by its dependencies in international relations and to act to reduce its strategic technological vulnerabilities to other international actors. Access refers to the EU's ability to condition and limit the access of non-EU parties to its market and technologies. Cooperate refers to the EU's and member states' inclination and openness towards international cooperation and multilateralism. Finally, own refers to the European control over critical technologies and (at least key parts of) their supply chains (Soare, 2022).

Digital sovereignty thus encompasses a wide array of democratic, socioeconomic, commercial, industrial, defence and security concerns simultaneously. These different areas challenge the autonomy and the integrity of states' competences and of the

EU, impacting their independence, their capacity to retain control over essential skills, and their ability to uphold the values that define their identity while shaping social dynamics. Digital sovereignty is a highly sought-after yet seldom fully achieved objective, sparking a multifaceted debate that, even in 2024, transcends expert communities and occasionally becomes entangled in overly-politicised rhetoric.

European digital sovereignty has become a central reference point for the EU's approach to global affairs at a time of "moving geopolitical plates" (Council of the European Union, 2022). While this discourse marks a striking rhetorical departure from the Union's traditional eschewal of geopolitics in its foreign policy (Bellanova, Carrapico, & Duez, 2022), it remains unclear whether it has driven concrete policy changes, although recently adopted Digital Services Act (DSA) and Digital Markets Act (DMA) may be seen as a major change in EU digital policy, with the objective of building a European digital sovereignty. Current literature has presented a fuzzy picture on this question: while some scholars have asserted that the discourse has served as an "aggregator" for the Union's digital policymaking (Bellanova, Carrapico, & Duez, 2022), others have cautioned that it conveys a "false promise" for EU global leadership in artificial intelligence (AI) (Calderaro & Blumfelde, 2022). Other debates – more pessimistic in tone – have associated the concept of digital sovereignty with the idea of servitude. Using terms such as "colony", "vassalised", or "under trusteeship", a widespread reading considers that Europe is (almost) out of digital history due to the wholesale dismemberment of its capacity for political and economic autonomy (Nocetti, 2021).

In a first chapter, Amar Rouabhi seeks to analyse how policy harmonisation can

improve digital sovereignty in the MENA region while maintaining compliance with international standards. He combines qualitative and quantitative analysis, entailing a review of existing legal statutes, directives, and policies in the MENA region concerning digital sovereignty. He shows that digital sovereignty is not an isolated aspect but forms an integral part of a country's strategic plan for digital transformation and economic competitiveness.

Next, Sara Baazobandi focuses on how individual users across the MENA region have used their autonomy and self-determination to push boundaries, lead social debates, shift traditional mindsets, and create economic opportunities – leading to a new appropriation of the digital sovereignty challenge. She nuances this assessment demonstrating that this "citizens' digital sovereignty" is challenged by governments in many respects.

In her contribution, Chloé Berger addresses the cross-cutting challenges faced by the MENA region in the digital field through the prisms of resilience and innovation. She seeks to identify similarities and discrepancies amongst MENA countries in order to identify various patterns of digital sovereignty. Against this backdrop, she argues that the effects of cooperation, synergy, differentiation, or rivalry related to digital sovereignty could redraw the fault lines of the MENA regional security complex.

Finally, Julien Nocetti explores how MENA countries have sought to articulate their domestic approach on digital sovereignty with their own involvement in regional and international debates. Here cybersecurity appears as a key vehicle for digital sovereignty; hence, diplomatic stances blur the lines between security considerations and a broader, more open conception of sovereignty in the digital field.

## Bibliography

BELLANOVA, R., CARRAPICO, H., & DUEZ, D. (2022). Digital/sovereignty and European security integration: an introduction. *European Security*, 31(3), 337–355. <https://doi.org/10.1080/09662839.2022.2101887>

CALDERARO, A., & BLUMFELDE, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security*, 31(3), 415–434. <https://doi.org/10.1080/09662839.2022.2101885>

COUNCIL OF THE EUROPEAN UNION. (2022, March). *A strategic compass for a stronger EU security and defence in the next decade*. <https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>

NOCETTI, J. (2021). L'Europe reste-t-elle une colonie numérique des Etats-Unis ?, *Politique étrangère*, 86 (3), pp. 51-63.

POHLE, J., & THIEL, T., (2020). Digital Sovereignty. *Internet Policy Review*, Vol. 9, (4), <https://doi.org/10.14763/2020.4.1532>

SOARE, S. (2022). How to achieve digital sovereignty – A European guide. In D. Broeders (Ed.), *Digital Sovereignty: From narrative to policy?* (p.21). The Hauge Program on International Cybersecurity, EU Cyber Direct.



# **Legal Frameworks for Digital Sovereignty in the MENA Region: Towards Policy Harmonisation?**

**Amar ROUABHI**

Associate Professor, Bouira University,  
Boumerdès

## Introduction

The traditional usage of the term sovereignty encountered severe criticism 25 years ago from the renowned American human rights researcher Louis Henkin (1995), who denounced it as an illegitimate term used to protect states' control at the expense of human rights protection. Similarly, the concept of digital sovereignty today faces analogous criticisms due to its utilisation by states as a pretext for digital control (Basu, 2023).

Digital sovereignty in the MENA region, therefore, transcends the mere adoption of technology; it encapsulates a broader strategy to enhance national security, economic resilience, and societal well-being through digital empowerment. This involves not only the development of local digital infrastructure and services but also the enactment of laws and regulations that safeguard data privacy, promote cyber hygiene, and ensure the equitable distribution of digital benefits among the population.

The concept of digital sovereignty has become a significant part of public discourse in most societies over the past few years. It is no longer solely the concern of major powers; rather, it is gradually crystallising in the Middle East and North Africa (MENA) region, especially after the Arab Spring revolutions. These uprisings demonstrated that the failure of governments in Egypt, Tunisia, Libya, Syria and Yemen to deal with the tech-savvy and rapidly advancing generation led to the downfall of some leaders and the alteration of others (Soliman, 2021).

To address the specific context of the MENA region, digital sovereignty can be defined as the ability of a state to regulate and control its digital infrastructure, data, and online activities within its borders, en-

suring autonomy in decision-making and protection from foreign interference. This concept is distinct from digital transformation, which refers to the broader process of adopting digital technologies across different sectors of society and the economy to improve efficiency and innovation. While digital transformation is essential for modernisation, digital sovereignty focuses on ensuring that these advancements are managed under the state's control, safeguarding data privacy, cybersecurity, and digital rights. In the MENA region, this distinction is crucial, as digital sovereignty involves navigating geopolitical and security concerns while fostering collaboration to shape a secure and independent digital space (Pohle & Thiel, 2020).

Moreover, the concept of digital sovereignty encourages the formulation of regional collaborations within the MENA region, aimed at standardising digital policies, sharing technological innovations, and building collective defences against cyber threats. Such collaborations could leverage the diverse strengths of MENA countries to foster a unified digital front, enhancing the region's overall digital sovereignty and positioning it as a formidable player in the global digital economy (Autolitano, 2023).

Since then, the issue of Internet usage in the MENA region has come under severe scrutiny, to the extent that some countries have resorted to what is termed as digital repression. For instance, in November 2019, Iranian authorities imposed a near-complete Internet shutdown for approximately a week, during which they suppressed numerous protesters and attempted to introduce an alternative to the Internet called "intranet" or the national information network. Furthermore, since September 2022, efforts have been made to curb Internet usage by disabling Virtual Private Network (VPN) technology. As protests

escalated, authorities tightened control over Instagram and WhatsApp, and blocked Google and Apple app stores (Alimardani, 2023).

On the other hand, according to Mohammed Soliman (2021), MENA region's countries are striving to avoid the American approach regarding data privacy issues and are inclined towards the European Union's General Data Protection Regulation (EU GDPR) model. The region has enacted a series of significant regulations, especially Saudi Arabia and the United Arab Emirates (UAE). Saudi Arabia, as part of its Vision 2030, aims to transition from an oil-dependent economy to a digital energy-based economy. It is expected that the digital services market in Saudi Arabia will exceed \$38 billion by 2025, with the country currently hosting more than 60 fintech startups (Haddad, 2022). Similarly, the UAE has taken substantial steps in this direction, including the implementation of its Personal Data Protection Law in 2021, which aligns closely with the GDPR. The UAE's commitment to digital transformation is evident in its ambitious National Digital Government Strategy 2025, which aims to solidify its position as a leading digital economy globally (Haddad, 2022).

Among the endeavours of leaders and government officials in the countries of the MENA region is the establishment of digital boundaries that align with their geographical borders (Douzet et al., 2023), mirroring the ongoing digital transformation. Concurrently, in light of security threats related to data protection and digital privacy, digital sovereignty necessitates coordinated efforts among these states to shape a regional digital space. Such coordination aims to create mechanisms or regulations akin to the European GDPR, particularly amidst increasing warnings from experts about the proliferation of future digital threats (Jansen, et al., 2023).

This chapter seeks to address the research question: *How can MENA countries harmonise their digital sovereignty policies to not only secure their national interests but also to position themselves competitively within the global digital landscape?* In exploring this question, the chapter will examine the current state of digital sovereignty in the MENA region, the challenges of policy harmonisation among these countries, and the potential impacts of such harmonisation on both regional and global scales.

Perhaps one of the significant challenges in shaping these policies within the MENA region lies not only in the need for coordinated efforts but also in the difficulty of regulating the influence of major digital communication companies. These companies often advance the agendas of certain countries, creating imbalances that hinder regional collaboration. As highlighted by author Hussein Zawi (2021), the ability to impose effective controls on these platforms is essential to achieving true digital sovereignty. This challenge adds another layer to the already complex task of fostering regional cooperation in the digital sphere, where previous attempts at non-digital collaboration have shown limited success.

From our perspective, traditional non-digital cooperation among the countries of this region remains a significant indicator of the feasibility of these states collaborating on policy coordination. Practical experience has demonstrated that traditional cooperation among these countries remains exceedingly weak, as evidenced by the significant gap between their declarations of cooperation and their practical applications. This is exemplified by the disparity between the assertions of cooperation made by these states and their actual practices, particularly evident in the realms of defence and security within the Gulf Cooperation Council (GCC) and the Organization of

Digital sovereignty necessitates coordinated efforts among these states to shape a regional digital space.

Digital sovereignty has become crucial for national security, economic growth, and societal health worldwide.

Islamic Cooperation (OIC). Their performance in these areas has been notably modest (Douzet et al., 2023).

Despite some individual initiatives by certain countries to advance this approach, such as Egypt's approval of a Personal Data Protection Law in 2020 and the Saudi National Cybersecurity Authority (NCA) issuing a draft document on Cloud Cybersecurity Controls (CCC), significant strides are still needed to enhance regional policy coordination in the digital realm. This chapter will begin by exploring the current state of digital sovereignty in the MENA region, focusing on policy harmonisation efforts and their impact on both regional and global strategies, particularly in relation to the EU. It will then examine the legal frameworks and cybersecurity measures currently in place, analysing their alignment with international standards. The chapter will also assess the broader implications of digital sovereignty in the MENA region, including the challenges and opportunities it presents for regional cooperation and global integration. Finally, strategic recommendations will be provided to enhance digital sovereignty in the region, emphasising the need for coordinated efforts, adherence to global norms, and integration into broader digital transformation initiatives.

## **Enhancing digital sovereignty: A comparative analysis of MENA policy harmonisation and its impact on EU and global strategies**

Digital sovereignty has become crucial for national security, economic growth, and societal health worldwide, especially in the MENA region, due to diverse digital adoption

levels. Aligning policies within the region could boost regional digital sovereignty, aiding in global competitiveness. The relationship between MENA's digital sovereignty and the EU's digital strategy shows the importance of digital autonomy in global relations, emphasising the need for international cooperation. This highlights digital sovereignty's vital role in the future's economic, political and social spheres, reflecting the evolving landscape of global digital governance.

### **Bridging the digital divide: ICT leadership in Gulf countries and challenges for North Africa**

A glance at the Global Knowledge Index (GKI) for 2023 (UNDP RBAS & MBRF) reveals that Gulf countries in the Middle East region ranked ahead of North African countries, with a significant advantage in the information and communications technology (ICT) sector. The United Arab Emirates (UAE) secured the 14th position globally in ICT, with a Knowledge Index of 70.0, followed by Saudi Arabia at 19th globally with a Knowledge Index of 65.4, Kuwait at 26th globally with a Knowledge Index of 62.4, Bahrain at 33rd globally with a Knowledge Index of 59.3, and Oman at 49th globally with a Knowledge Index of 53.0. Qatar ranked 58th globally with a Knowledge Index of 50.8. On the other hand, North African countries lagged behind, with Morocco ranking 72nd globally with a Knowledge Index of 45.4, followed by Tunisia at 81st globally with a GKI of 43.1, and Egypt at 85th globally with a Knowledge Index of 39.8.

The seven sub-indices, all of which make up the GKI, consist of numerous variables. These seven indices are as follows:

- Pre-university education
- Technical and vocational education and training

- Higher education
- Research, development, and innovation
- Information and communications technology
- Economy
- Enabling environment

These indices were chosen as a basis because achieving digital sovereignty for any country cannot be envisioned without considering its digital capabilities.

With digital skills playing a pivotal role in digital sovereignty, empowering citizens with the knowledge to navigate and contribute to the digital economy is essential.

This emphasis is reflected in Gulf countries, especially the UAE and Saudi Arabia, which prioritise digital literacy as part of their national strategies. Such skills are key to bridging the gap between regional nations and ensuring cohesive digital transformation.

These indices provide essential inputs, encompassing both the creation of knowledge (the first three indices) and its realisation (the fourth and fifth indices), as well as the provision of an appropriate environment (the sixth and seventh indices). Therefore, it is evident that these factors are critical in measuring and fostering digital sovereignty.

Empowering citizens with the knowledge to navigate and contribute to the digital economy is essential.

**Table 1.** Ranking of MENA countries in the Global Knowledge Index 2023

Country	Global ICT Ranking	Knowledge Index
United Arab Emirates	14	70.0
Saudi Arabia	19	65.4
Kuwait	26	62.4
Bahrain	33	59.3
Oman	49	53.0
Qatar	58	50.8
Morocco	72	45.4
Tunisia	81	43.1
Egypt	85	39.8

Compiled by author, sourced from UNDP RBAS & MBRF (2023).

By categorising MENA countries according to their level of income and their innovation progress based on the 2023

Global Innovation Index (GII), the distinction becomes clearer, as illustrated in the following table:

**Table 2.** Ranking of MENA countries in the Global Innovation Index by income category (2023)

Low-income	Lower middle-income	Upper middle-income	High-income
Morocco	Jordan	Bahrain	United Arab Emirates (1st)
Tunisia		Oman	Saudi Arabia (2nd)
Egypt		Algeria	Qatar (3rd) Kuwait (4th)

Compiled by author, sourced from UNDP RBAS & MBRF (2023).

These distinctions highlight the significant differences between the Middle East and North Africa in terms of income and innovation levels, further emphasizing the disparity in digital progress across the region. These differences present key challenges for achieving MENA-wide harmonisation, particularly when addressing both digital and analogue development fronts.

Despite individual efforts by some governments to enhance digital sovereignty, there is a lack of coordination and a unified approach specific to the region. The significant diversity in digital infrastructure across MENA countries mirrors the variation in their GKI rankings. Some countries, such as those in the Gulf, lead in ICT development, while others lag behind, creating a challenge for regional harmonisation efforts. To improve digital sovereignty in the Middle East and North Africa, attention must first be given to addressing these disparities in digital infrastructure. This involves developing robust and independent communication networks to ensure comprehensive citizen access to digital services, with a focus on cybersecurity to protect against cyber threats. Concurrently, the enactment of common legal frameworks among regional countries is essential to safeguard data, privacy, and enhance digital independence. Furthermore, promoting research and development in emerging technological sectors is crucial for enhancing digital sovereignty (Al Bitar, 2024).

### **Challenges and strategic initiatives in the MENA region's pursuit of digital sovereignty**

With the EU's growing concerns about the impact of external technology companies, particularly from China and the US, on its economic and social sectors, along with the increasing threats related to personal data breaches within the Union,

European leaders are considering the Union's ability to act independently in the digital age. In light of the restrictions placed on these advanced technology companies within the EU, European leaders are contemplating the creation of competitive European companies in the same field to reduce reliance on and dominance by external technology giants. The accelerated digital threats to Europe's sovereignty, exacerbated by the COVID-19 pandemic, have compelled European Commission President Ursula von der Leyen to prioritise digital policy during her tenure (2019-2024), pledging to achieve digital and technological sovereignty (Madiega, 2020).

While the concept of digital sovereignty has been used in authoritarian regimes as a tool to restrict freedom of expression, in democratic contexts it has sparked growing concerns about misinformation and digital surveillance. In this light, French President Emmanuel Macron, in 2017, called for Europe to assert its digital sovereignty, urging the continent to lead the digital transformation rather than remain subject to the dominance of external technological powers. Similarly, in 2019, German Chancellor Angela Merkel emphasised the importance of Europe adopting an open approach to digital sovereignty – one that encourages cooperation and innovation rather than isolation. The core message here is that European leaders see digital sovereignty as a pathway to gaining independence in the digital era while maintaining an open and collaborative global stance (Falkner et.al., 2022, p. 3012).

According to a 2020 European Parliamentary Research Service report, Europe's digital market growth potential will play a significant role in the global market for new digital technologies, estimated to reach €2.2 trillion by 2025. However, it is worth noting that the EU lags behind the US and China in the adoption and use of

The enactment of common legal frameworks among regional countries is essential to safeguard data, privacy, and enhance digital independence.

artificial intelligence (AI) technologies by companies and citizens (Madiaga, 2020). This relative lag in the European digital economy compared to its global competitors is attributed to Europe's heavy reliance on foreign digital technology. In 2019, the market value of the four largest American technology companies and the four largest Chinese technology companies was 17 times the market value of the top 10 telecommunications companies in the EU (Amiot, et al., 2020).

The European Commission has put its faith in the success of the European Digital Decade framework, setting ambitious policy goals for 2030 in four core fields: skills, infrastructure and capacities, public services, and business digitalisation. This framework also presents an opportunity for the EU to establish alliances and relationships with countries sharing similar digital and technological cooperation visions, despite the risks associated with digitalisation, including mass surveillance, cyberattacks on critical infrastructure, misinformation, and undermining democracy.

The rest of the European legislation is no less important than the GDPR, which is at the heart of European digital sovereignty, as is the case with the Digital Services Act (DSA). The DSA protects consumers and their fundamental rights online by setting clear and proportionate rules. It fosters innovation, growth and competitiveness, and facilitates the scaling up of smaller platforms, Small and Medium Enterprises (SMEs) and startups. The roles of users, platforms and public authorities are rebalanced according to European values, placing citizens at the centre (European Commission, n.d.a).

As for the digital market in the EU, and in order to make it fairer and more competitive, Europe strengthened its legislation with the Digital Markets Act (DMA), which establishes a set of clearly defined objective

criteria to identify "gatekeepers". Gatekeepers are large digital platforms providing so-called core platform services. The DMA is among the first regulatory tools designed to comprehensively address the gatekeeper power of the largest digital companies. It complements EU competition rules without altering them (European Commission, n.d.b)

The EU has strengthened its legal legislation to include AI, which was embodied in the Artificial Intelligence Act (AI Act), the latter of which is a European regulation governing AI and marks the first comprehensive regulation on AI introduced by a major regulator globally. The Act classifies AI applications into three risk categories. The first category includes applications and systems that pose an unacceptable risk, such as government-operated social scoring like that in China, which are prohibited. The second category covers high-risk applications, such as CV-scanning tools that rank job candidates, which must meet specific legal standards. Lastly, applications not falling under the banned or high-risk categories remain largely unregulated (European Union, n.d.).

This European approach, aimed at openness to various global alliances, comes at a time when some countries in the MENA region are seeking to embody the concept of digital sovereignty in line with the changing digital world. Unlike the EU, countries in this region have not formulated a common vision, such as the European Commission's Digital Compass 2030, which represents a facet of European policy in securing digital sovereignty through the development of key technologies and enhancing digital skills, accompanied by a significant legislative agenda (Burwell & Propp, 2022).

This vision embodied in the Digital Compass aims to achieve intermediate goals related to business digital transformation. It aspires to have over 90% of European SMEs reach at least a basic level of digital intensity

This European approach, aimed at openness to various global alliances, comes at a time when some countries in the MENA region are seeking to embody the concept of digital sovereignty in line with the changing digital world.

compared to 61% in 2019. At the same time, it aims to have approximately 250 unicorn companies (startups valued at over one billion dollars) in the EU, doubling from 2021. Regarding digital infrastructure, Europe aims to achieve high and fast Internet penetration among all European households compared to 59% in 2019, along with other goals including public service digitalisation and ensuring that 80% of the population possesses high digital skills (Emirates Policy Center, 2021).

To complement this focus on digital transformation, human capital has emerged as one of the most important indicators for assessing digitally advanced societies since 2014. This is reflected in the Digital Economy and Society Index (DESI), which, since its inception, has been a key tool for monitoring and evaluating the digital progress of the European economy and society. By 2021, the DESI's core indicators were aligned with the objectives of the 2030 Digital Agenda, emphasising four main dimensions: human capital, connectivity, integration of digital technologies, and digital public services.

Similarly, in the MENA region, enhancing human capital is also a critical component of advancing digital sovereignty, as developing digital skills and competencies is essential for building a resilient digital economy and addressing broader infrastructure issues (Kovács et.al., 2022).

However, in contrast to Europe's progress, Internet usage in the Arab region has shown considerable variation across different countries. For example, Internet users in the Arab region were estimated at 51.6% in 2019, with significant disparities among nations. Approximately 30% of the region's population remained entirely unconnected to the Internet, with global statistics indicating that 2.9 billion people worldwide were offline, 96% of whom reside in developing

countries. By 2022, Internet users in the Arab region reached 327 million people, representing 70.3%, up from 28.8% in 2012, with Internet usage intensifying during the COVID-19 pandemic (Elzahraa & Hoda, 2023).

Arab countries have embarked on strategic initiatives in recent years to assert control and independence in the digital realm, aiming to achieve digital sovereignty. These initiatives seek to advance national interests and protect cultural values, with the initial steps focusing on regulating Internet usage within state borders, framing it within significant legal frameworks, establishing regulatory structures in line with existing legislation, and introducing digital surveillance measures. Electronic surveillance intensified following the Arab Spring events, with several governments like Egypt restricting access to social media platforms such as Facebook and Twitter (Saaida, 2023).

Digital transformation processes in the Arab world began approximately a decade later compared to countries in the Northern Hemisphere. The UAE, being the only country in the region with 100% Internet user penetration, has led the way in successfully digitising its economy. The Arab region, however, has become a major target for cyberattacks, primarily focused on trade and technological secrets, which account for 63.3% of the attacks. In contrast, financial data theft accounts for only 6.2%, while personal data theft stands at 29.6% (Valiakhmetova & Tsukanov, 2022).

Due to the Gulf countries' long-term digital strategies aimed at developing their economies, these nations have found themselves increasingly integrated into the digital sphere, making them prime targets for cyberattacks. While financial data theft remains relatively low at 6.2%, the majority of cyberattacks, 63.3%, have been aimed at trade and technological secrets. In



contrast, other Arab countries that have not reached the same level of digital integration as the Gulf States are less financially targeted, which explains the lower percentage of financial data breaches and the higher focus on trade secrets.

Traditionally, Gulf countries have been primary targets for cyberattacks, which has led them to enhance their protection mechanisms. Saudi Arabia and the UAE, for example, rank high globally in cybersecurity readiness, placing 30th and 36th, respectively, in global cybersecurity indices. Other Middle Eastern countries, however, are less prepared to defend against cyber breaches and threats. These nations have become targets amidst ongoing regional and global conflicts. For instance, Iran faced a significant cyberattack on its nuclear research centre in 2010, involving the advanced Stuxnet virus (Valiakmetova & Tsukanov, 2022, p.308).

## **Digital sovereignty in the MENA region and its global ripple effects: navigating legal challenges and shaping EU digital policy**

In today's interconnected world, the imperative for legal frameworks that align with digital transformation is increasingly acknowledged by nations seeking to reinforce their sovereignty. Traditional concepts of sovereignty, once deemed adequate in governing the affairs of a state within its territorial boundaries, are being challenged by the borderless nature of the Internet. Nations now find themselves grappling with the realisation that their autonomy is intricately linked to the control and management of digital infrastructure and technology (Pohle & Thiel, 2020). This challenge

is particularly significant for both the MENA region and the EU, where the importance of digital sovereignty continues to grow.

For the EU, the pursuit of digital sovereignty is not merely an internal matter. Europe's efforts to secure its digital space and ensure independence from global tech giants, primarily from the US and China, have highlighted the need for stronger international cooperation. The EU has recognised that achieving digital sovereignty is vital for its security, economic stability, and global competitiveness. This aspiration, however, faces significant challenges. Europe's dependence on foreign technology, particularly in the areas of AI and digital infrastructure, has underscored the need for alternative strategies that can help the continent regain its autonomy in the digital realm (Autolitano, 2023).

This dynamic is not exclusive to Europe. Countries in the MENA region are also facing the pressures of digital transformation and sovereignty. The region is experiencing rapid technological advancements, especially in the Gulf countries, which are making significant investments in their digital infrastructure. Nations like the UAE and Saudi Arabia are leading the charge in digitising their economies, positioning themselves as key players in the global digital economy. This, in turn, is shifting the balance of digital power and prompting Europe to rethink its digital strategy.

This challenge is particularly pronounced given the rapid expansion of digital networks since the 1990s, which, as Julia Pohle and Thiel Thorsten (2020) explain, has led to a dilution of traditional sovereignty principles, allowing them to slip beyond the grasp of state control. This dynamic is evident in both the MENA region and Europe, where countries are grappling with the balance between controlling their digital infrastructures and navigating the increasingly bor-

Nations now find themselves grappling with the realisation that their autonomy is intricately linked to the control and management of digital infrastructure and technology.

derless nature of the Internet. In the MENA region, the issue is compounded by external pressures from global tech giants and the rapid pace of digital transformation within countries such as the UAE and Saudi Arabia. These nations are pushing forward with ambitious digital strategies, which, in turn, have begun to shift the global balance of digital power, affecting Europe's ability to retain its digital leadership.

For Europe, the influence of the MENA region's digital sovereignty is twofold. Firstly, as MENA countries assert their own digital independence, particularly through investments in cybersecurity and data privacy, they are creating new models of governance that Europe must contend with. Secondly, Europe's economic and security ties with the region are becoming increasingly dependent on digital cooperation. The more it strengthens its digital autonomy, the more Europe must adapt its policies to account for this emerging regional power. This is especially true in areas such as cybersecurity, where regional collaboration is essential to address shared threats, as well as in the regulation of global digital platforms.

The evolving relationship between Europe and the MENA region underscores the importance of digital sovereignty as a global issue. While the EU continues to advocate for greater independence from external technology providers, its efforts must now take into account the rising digital influence of regions like MENA. As Europe navigates its own challenges in achieving digital sovereignty, it must also engage with MENA as a partner, recognising that the digital futures of both regions are increasingly interconnected.

In conclusion, the quest for digital sovereignty is not just about technology but also about redefining global power structures in the digital age. The MENA region's

growing digital capabilities, particularly in the Gulf, are reshaping the global digital landscape and presenting new challenges and opportunities for Europe. As both regions work to secure their digital futures, the need for collaboration and shared governance in the digital domain becomes ever more crucial.

## **Legal frameworks, cybersecurity, and EU and global integration**

In the digital era, the MENA region faces the critical task of advancing digital sovereignty while navigating the complexities of legal and policy frameworks. This exploration unfolds through three key areas: analysing its legal provisions and digital policies, dissecting digital rights, cybersecurity, and innovation, and aligning its digital strategies with global standards, including those established by the EU. The narrative captures the efforts of MENA countries in establishing data protection laws and combating cybercrimes, underscoring the importance of digital governance. Through a comparative analysis, this discussion aims to highlight the progress and challenges in the MENA region's digital landscape, emphasising the need for regional collaboration and international alignment to ensure a secure and inclusive digital future.

## **Examination of the MENA region's legal provisions and digital policies**

According to a study conducted by "Cullen International" (Hayajneh, 2021) on the status of national legislation concerning personal data protection in 13 countries in the MENA region, eight countries have national legislation in this area. Among them, four countries –Tunisia, Morocco,

The evolving relationship between Europe and the MENA region underscores the importance of digital sovereignty as a global issue.

Qatar, and Turkey – enacted relevant laws before the General Data Protection Regulation (GDPR) came into effect in Europe in 2018, while Bahrain, Algeria, Lebanon, and Egypt enacted laws after this date.

**Figure 1.** Status of personal data protection in the MENA region

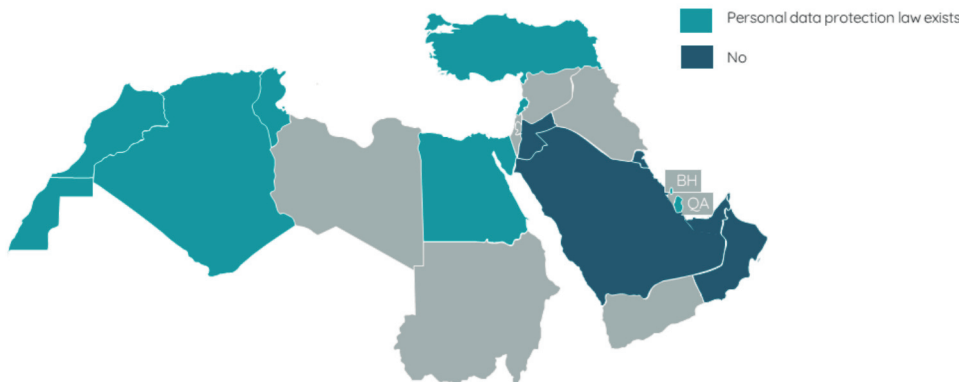


Image sourced from study by Cullen International (2021).

While digital sovereignty in MENA countries covers essential components such as data protection, cybersecurity, and regulating digital platforms, many challenges persist. For instance, several nations in the region have adopted policies addressing the storage of data locally to limit foreign access, yet cyberattack vulnerabilities remain high, particularly in countries without robust cybersecurity frameworks. Additionally, legal frameworks related to AI, electronic signatures, competition policies, and intellectual property in the digital realm are still underdeveloped, contributing to the fragmented approach to digital sovereignty.

Moreover, digital sovereignty also intersects with regional economic security. For instance, trade agreements involving the digital economy and cross-border data flows are largely governed by external frameworks, making MENA countries dependent on global giants for digital infrastructure and technology. The lack of comprehensive regional

agreements limits their capacity to protect local economies from digital monopolies and enhance their position in international negotiations. This makes the region more susceptible to economic risks tied to the digital economy, such as market concentration and technological dependency.

Furthermore, according to a study conducted by Global System for Mobile Communications Association (GSMA) (2019) on data protection in the MENA region, until 2019, the majority of countries in this region did not have direct legislation on data protection, except for Qatar, which was the first Gulf Cooperation Council (GCC) country to adopt a data protection law in 2017, followed by Bahrain, which enacted a data privacy law. In countries such as Algeria, for example, the legal response to cybersecurity threats has been robust, focusing on both cybercrime legislation and defensive infrastructure to prevent state-level threats. Algeria's introduction

This makes the region more susceptible to economic risks tied to the digital economy, such as market concentration and technological dependency.

The efforts of MENA countries in the area of cybersecurity and digital legislation demonstrate significant progress, but much remains to be done.

of Law No. 04-10 and subsequent legal frameworks highlight a concerted effort to address crimes related to information and communication technologies ICT.

Algeria, which hosted the International Conference on Digital Sovereignty on 19 February 2024, reflecting its particular attention to this new challenge, had a legal arsenal primarily aimed at combating cybercrimes. This was embodied in Law No. 04-10 on penalties dated 10 November 2010, as well as the Code of Criminal Procedure, which extended the local jurisdiction of the public prosecutor in the field of cybercrimes. Given the evolution of crimes related to ICT, Algeria strengthened its legal arsenal with Law No. 09-04 concerning rules for preventing and combating crimes related to ICT. Regarding the accompanying structures of the policy to counter crimes threatening state sovereignty, Algeria established several entities, including the Center for the Prevention of Computer and Information Technology Crimes of the National Gendarmerie, the National Institute of Forensic Evidence and Criminology, the Central Service for Combating Cybercrime, and the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies (Ahmed & Gribiz, 2022).

The efforts of MENA countries in the area of cybersecurity and digital legislation demonstrate significant progress, but much remains to be done. Digital sovereignty in the region requires stronger legal frameworks to address evolving threats, and further collaboration is needed to ensure that these frameworks are harmonised across borders. Without such cooperation, MENA countries may find themselves vulnerable to external digital influences and unable to fully protect their citizens and digital borders.

### Data analysis: digital rights, cybersecurity, and digital innovation in the MENA region

Analysing data, digital policies, and innovation in the MENA region requires disaggregating the study by dividing its countries into two parts: the Middle East countries and North African countries. This analytical division is consistent with the conceptual framework that recognises shared characteristics within each bloc, while enabling more rigorous comparative analysis both intra-regionally and inter-regionally. To achieve this, we will rely on some relevant global reports on digitisation and innovation, namely the GKI and GII in their latest releases in 2023, by selecting models from countries in the two regions for comparison and analysis.

**Table 3.** Ranking of MENA Countries in the Global Knowledge Index (2023)

Country	Rank	Rank by Sectors						
		Education Pre-University	Technical Education	Higher Education	R&D and Innovation	ITC	Economy	Empowerment Environment
United Arab Emirates	26	37	02	47	29	14	13	37
Qatar	39	20	62	28	47	58	26	20
Tunisia	81	56	76	87	73	81	86	56
Egypt	90	80	46	94	90	85	85	115

Elaborated by author, sourced from UNDP RBAS & MBRF (2023).

The UAE, with a Gross Domestic Product (GDP) of \$701.467 billion, demonstrates outstanding performance in terms of cognitive infrastructure, ranking 26th globally and 26th among 61 countries with very high human development. Among its strengths are individuals' digital skills, widespread high-speed Internet access, and a high educational attainment rate (UNDP RBAS & MBRF, 2023, p.109).

Qatar, with a GDP of \$261.688 billion, ranks 39th globally, making it the second Gulf country after the UAE. It holds the 38th position among 61 countries with very high human development. Qatar's strengths include a high per capita investment in research and development (UNDP RBAS & MBRF, 2023, p.346).

On the other hand, Tunisia, with a GDP of \$130.699 billion, ranks 81st globally and 16th among 28 countries with high human development, with its performance described as modest in the report (UNDP RBAS & MBRF, 2023, p.253). Meanwhile, Egypt, with a GDP of \$1.418.532 billion, ranks 90nd globally and 24th among 28 countries with high human development (UNDP RBAS & MBRF, 2023, p.472).

### **Aligning the MENA region's digital sovereignty with European and global benchmarks**

After reviewing relevant indexes, international documents and examining relevant national legislation in both MENA and EU countries, it becomes evident that there is a digital divide among MENA countries. Therefore, this chapter will maintain the division into two subregions – the Middle East and North Africa – to better assess the alignment of digital sovereignty with European and global standards. Additionally, the analysis will differentiate between alignment with

EU standards on the one hand and broader global benchmarks on the other.

It is worth mentioning that the relationship between MENA countries and the EU is heading in one direction. The apprehension faced by Europe, which led to the introduction of the European GDPR, is the same apprehension applicable to the MENA region. This apprehension pertains to potential digital sovereignty breaches from China, the US, and even South Korea. On the other hand, MENA countries' relationship with global standards follows a more cautious approach, if one may say so.

## **Current legal dynamics in the MENA region**

### **Evaluating existing digital sovereignty frameworks**

The concept of digital sovereignty has emerged as a pivotal concern within the MENA region, underscoring the necessity for nations to navigate the complexities of the digital era with autonomy and strategic foresight. This issue is particularly pressing given the varying degrees of digital readiness and infrastructure development across the region, resulting in notable disparities in digital capabilities. Countries in the Gulf, notably the UAE, Qatar, Saudi Arabia and Kuwait, have distinguished themselves through robust digital infrastructure, creating a discernible divide not only with their North African counterparts but also with other nations within the Middle East itself.

The advancements in digital infrastructure in these leading nations are not solely about current state-of-the-art capabilities but also reflect a deep commitment to future-oriented planning and implementation. Saudi Arabia's Vision 2030 stands as a testament to this forward-looking approach,

emphasising digital inclusivity, e-participation, privacy and data protection. This comprehensive strategy demonstrates an understanding that digital sovereignty extends beyond infrastructure to encompass the digital rights of citizens, aiming to create an inclusive digital society that safeguards privacy and enhances citizen engagement through digital means (Saudi Arabia's National Portal for Government Services, n.d.).

Similarly, the UAE's National Digital Government Strategy 2025 outlines an ambitious blueprint for establishing world-class digital infrastructure and legislative frameworks tailored to facilitate seamless digital transformation. This strategy underscores the nation's commitment to enhancing digital capabilities and skills among its population, thereby ensuring that the Emirates remains at the forefront of digital innovation and governance. The objectives outlined in this strategy mirror, to a significant extent, the ambitions of the EU regarding digital development, indicating a global convergence on the importance of digital sovereignty as a foundational pillar for future prosperity and security (Emirates Health Services, n.d.).

This highlights the need for stronger, more strategic digital alliances that can overcome these historical limitations and create a unified front in the realm of digital sovereignty.

These initiatives reflect a broader regional trend towards recognising the strategic importance of digital sovereignty, not just in terms of technological infrastructure but also in fostering a digitally literate society, protected by robust data protection laws and engaged in the digital economy. The readiness of the UAE, and to a lesser extent Saudi Arabia and Qatar, is an important indicator that could contribute to building a regional strategy – if the willingness existed –, unlike the case of their North African counterparts. As MENA countries strive to close the digital divide within the region and align more closely with global digital leaders, the emphasis on comprehensive digital strategies that address infrastructure, legal frameworks,

and human capital development becomes increasingly crucial. This approach not only enhances national competitiveness but also contributes to a more balanced and equitable global digital landscape.

### **The necessity for harmonised policy-making for a solid digital infrastructure**

The imperative for harmonised policy-making within the MENA region to establish a resilient digital infrastructure becomes increasingly salient against the backdrop of evolving global digital dynamics. The analysis underscores a fundamental shift from the traditional concept of sovereignty – anchored in the physical dominion and political autonomy – to a nuanced understanding of digital sovereignty, emphasising control over digital spaces and data. In this context, the historical formation of regional blocs such as the Organization of Islamic Cooperation and the Arab League, which consolidated traditional sovereignties, finds a contemporary parallel in the urgent need for similar alliances focused on digital sovereignty within the MENA region. However, just as these pre-digital alliances faced challenges in achieving effective collaboration and coordination, particularly in areas of defence and security, the same issues of fragmented interests and lack of cohesive policy-making may persist in the digital age. This highlights the need for stronger, more strategic digital alliances that can overcome these historical limitations and create a unified front in the realm of digital sovereignty.

This necessity is underscored by the global landscape, particularly in Europe, where the amalgamation of advanced nations harbours deep concerns over breaches of digital sovereignty. The European experience, characterised by concerted efforts to safeguard digital domains through stringent

regulation and collective action, highlights the critical importance of unity and shared vision in confronting digital threats. Europe's regulatory frameworks, notably the GDPR, exemplify a concerted response to the challenges of digital sovereignty, showcasing the potential of regional collaboration in establishing robust digital defences.

Drawing inspiration from the European model, MENA countries are called upon to expedite their efforts towards formulating and implementing harmonised digital policies. Such initiatives are not only essential for countering external digital hegemony but also for capitalising on the region's significant potential in digital transformation. Indeed, certain MENA countries boast capabilities that parallel, and occasionally surpass, those of European nations in terms of digital infrastructure and innovation. However, the efforts to harness these capabilities at a regional level have been modest and sporadically successful at best, often failing to capture the collective imagination or commitment of the Arab world.

The scientific symposium of the Arab States Broadcasting Union held in Tunisia in December 2023 and the International Conference on Digital Sovereignty convened in Algeria in February 2024 serve as emblematic instances of these efforts. While these initiatives reflect a growing awareness of the importance of digital sovereignty, they also highlight the challenges of achieving regional cohesion and collective action. The modest reception of these efforts underscores the necessity for a more integrated and strategic approach to digital policy-making within the MENA region.

To navigate the complexities of the digital age effectively, MENA countries must embrace a vision of digital sovereignty that transcends national boundaries, fostering regional alliances and policy harmonisation.

By doing so, they can establish a solid digital infrastructure that not only protects against external encroachments but also promotes economic growth, innovation, and societal well-being. This approach requires a concerted effort to build consensus, share knowledge, and align strategies, ensuring that the MENA region can assert its place in the global digital landscape with confidence and collective strength.

## Strategic recommendations

### Enhancing digital sovereignty in the MENA region

The advancement in digital technologies across the MENA region – reflected through various indicators such as digital infrastructure, research and development, innovation, and educational institutions – serves as essential inputs for governments to establish and strengthen digital sovereignty. While traditional sovereignty is realised through diplomatic and security readiness, digital sovereignty depends on digital preparedness and capability. For example, the EU's goal of achieving 100% digital literacy among its citizens demonstrates the importance of digital skills in consolidating digital sovereignty.

As observed, countries like the UAE, Saudi Arabia, and Qatar are significant models that have made significant strides in digital transformation. Therefore, it is imperative for other countries in the region to follow suit to achieve digital convergence. This can only be accomplished by addressing the most crucial challenge: digital infrastructure. Various reports have indicated that countries with weak digital infrastructure tend to lag behind in global rankings.

While traditional sovereignty is realised through diplomatic and security readiness, digital sovereignty depends on digital preparedness and capability.

Secondly, another aspect that must be addressed to enhance digital sovereignty is overcoming traditional disputes among countries, including issues related to geographical boundaries. Digital sovereignty also necessitates understanding and coordination in digital boundaries. For example, Internet lines between Gulf countries often pass through a hub in Bahrain, making it a central communication point in the region due to Bahrain's strategic location.

### Adhering to global norms

The European GDPR has become a significant global standard, leading Europe to curb the global digital wave emanating from Chinese and American giants. It serves as an important model for countries in the MENA region to formulate similar regulations, at least within organisations like the Organization of Islamic Cooperation or other blocs. This is particularly crucial as countries in this region do not hold the same digital status as the EU. Individual initiatives within countries are insufficient since the digital space transcends geographical boundaries.

The responsibility for setting global standards in digital sovereignty should arguably rest with countries most affected by technological and digital penetration. In the case of the EU, where leading Chinese and American tech companies dominate the digital landscape, it would have been more prudent for it to adopt a robust digital strategy aimed at curbing this digital dominance, thereby safeguarding its digital sovereignty. Early signs of this shift are already evident through recent legislation, policies, and regulations. From an economic standpoint, this can be viewed as a defensive strategy within the "SWOT" framework, focused on strengthening digital sovereignty. This has led Europe to counter the dominance of American and Chinese tech giants by

implementing regulations like the GDPR.

However, this has not prevented the existence of some global initiatives aiming to establish global standards in digitisation and AI in general. For instance, on 29 September 2021, the US and the New Technology and Trade Council of the European Union held their first summit, which opposed AI that does not respect human rights.

### Integrating into broader digital transformation initiatives

Countries in the MENA region remain aware of the ongoing digital transformation, as evidenced by the existence of domestic legislation and the hosting of relevant summits and conferences on digital sovereignty. However, global observers note that the key movements in digital transformation are predominantly driven by Europe, China, and the US. While the Gulf region has made progress in digital transformation, this progress has largely been on an individual basis rather than through coordinated efforts among countries. The lack of coordinated action, combined with the significant digital gap between regions like North Africa and the Middle East, could leave some MENA countries, particularly those that are digitally lagging, vulnerable. The individual readiness of certain Middle Eastern countries might attract interest from non-MENA countries to form digital blocs, which could further isolate the less prepared countries in the region from global or regional initiatives.

Therefore, integration into global initiatives is a form of international decision-making, notably highlighted by the growing interest of countries in digital healthcare, especially after the COVID-19 pandemic. One such global initiative in alignment with digital

The responsibility for setting global standards in digital sovereignty should arguably rest with countries most affected by technological and digital penetration.



sovereignty is the World Economic Forum's initiative to enhance digital health transformation based on AI in healthcare systems in January 2024. By participating in these global efforts, countries not only advance their digital transformation but also strengthen their digital sovereignty by ensuring control over healthcare data, securing technological infrastructure, and fostering independent decision-making in the digital domain.

## Concluding remarks

### Summary of key findings and perspectives

As a final note on digital sovereignty in the MENA region, and considering global experiences, particularly the EU's approach to digital transformation in general and digital sovereignty in particular, it becomes apparent that discussing digital sovereignty in MENA countries cannot be done without the presence of digital inputs and assets. These include digital infrastructure, research and development, ICTs, as well as legal and structural accompaniments. Here are some key observations:

- Varied digital infrastructure across the MENA countries: Various relevant international reports confirm this, with countries like the UAE, Saudi Arabia, and Qatar leading in digital transformation compared to European countries. For instance, the UAE ranks 14th globally in the ICT Development Index (2023), surpassing European countries like Austria (ranked 18th), France (20th), Belgium (32nd), and even advanced countries like Canada (29th). On the other hand, some North African countries fall behind in the same sector, with Morocco ranking 72nd and Tunisia 81st globally in the ICT sector.

- Digital empowerment: The European policy on digital sovereignty emphasises empowering European citizens with digital skills. Similar emphasis on digital empowerment can be observed in the MENA region, particularly among Gulf countries.

- Digital initiatives in two phases: MENA countries should initiate digital projects specific to the region, led by pioneering countries in this field as a first phase. This could later expand into partnerships or agreements within regional blocs like the EU.

### Future implications of digital governance

The presence of digital governance generates both internal and external implications. Domestically, it fosters a digitally aware society, resilient to foreign cyber threats, adaptable in commercial and economic dealings, and enhances transparency and access to information. Externally, it reinforces traditional sovereignty with digital sovereignty, subjecting it to the existence of standards and regulations governing responsibility in case of breaches in global digital platforms. There is a possibility of future digital suppression in some countries if policies are not coordinated and regulated, potentially leading to the blocking of certain platforms and websites under the pretext of protecting digital sovereignty.

However, the future of digital governance, in our view, is contingent upon the readiness of the state in both material (such as technological infrastructure) and non-material (digital literacy and preparedness of citizens) aspects. This must also align with the dictates of digital transformation in the external world and related digital initiatives, all supported by feasible laws and implementation mechanisms.

There is a possibility of future digital suppression in some countries if policies are not coordinated and regulated.

### **Link to European digital policies and international alliances**

After a comprehensive review of digital policies worldwide, it becomes evident that MENA countries remain isolated from European and American digital policies. Moreover, there is a lack of convergence among countries in this region within existing blocs (such as the Organization of Islamic

Cooperation and the Arab League). However, the World Bank's report released in March 2022, entitled "Positive Aspects of Digital Technologies for the Middle East and North Africa," highlights the potential benefits of adopting digital technologies in MENA countries. These include significant social and economic benefits amounting to billions of dollars annually, with full digitization of the economy potentially increasing per capita GDP by at least 46% over 30 years.

## Bibliography

AHMED, S., & GRIBIZ, M. (2022). Internet Challenges to State Sovereignty (Digital Sovereignty). *Journal of Legal and Economic Research*, 5 (1), pp. 302-322

AL BITAR, N. (2024, February). *Towards adopting a unified Arab strategy for digital sovereignty*.

ALIMARDANI, M. (2023). Aggressive New Digital Repression in Iran in the Era of the Woman, Life, Freedom Uprisings. In S. Feldstein (Ed.), *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms* (pp.5-10). Carnegie Endowment for International Peace

AMIOT, E., PALENCIA, I., BAENA, A. & DE POMMEROL, C. (2020) *European Digital Sovereignty: Syncing values and value*. Oliver Wyman. <https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/october/European%20Digital%20Sovereignty.pdf>

AUTOLITANO, S. (2023, April 10). *Why the EU should stop talking about digital sovereignty*. Council on Foreign Relations. <https://www.cfr.org/blog/why-eu-should-stop-talking-about-digital-sovereignty>

BASU, A. (2023). Defending the 'S Word': The Language of Digital Sovereignty Can be a Tool of Empowerment. In S. Feldstein (Ed.), *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms* (pp.19-22). Carnegie Endowment for International Peace.

BURWELL, F. G., & PROPP, K. (2022). *Digital sovereignty in practice: The EU's push to shape the new global economy*. Atlantic Council Europe Center.

DOUZET, F., PÉTINIAUD, L., SALAMATIAN, K., & SAMAAN, J.L. (2022). Digital routes and borders in the Middle East: the geopolitical underpinnings of Internet connectivity. *Territory, Politics, Governance*, 11(6), 1059–1080. <https://doi.org/10.1080/21622671.2022.2153726>

ELZAHRAA, Y. F., & HODA, E. N. (2023, September). *Driving Digital Transformation in the Arab Region*. United Nations Development Program. <https://www.undp.org/arab-states/stories/driving-digital-transformation-arab-region>

EMIRATES HEALTH SERVICES. (n.d.). *The UAE digital government strategy 2025*. <https://www.ehs.gov.ae/en/about-us/the-uae-digital-government-strategy-2025>

EMIRATES POLICY CENTER. (2021). *The European Union digital empowerment strategy: Objectives and challenges*.

EUROPEAN COMMISSION (n.d.). *Digital Markets Act*. [https://digital-markets-act.ec.europa.eu/index\\_en](https://digital-markets-act.ec.europa.eu/index_en)

EUROPEAN COMMISSION. (n.d.). *The Digital Services Act*. [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en)

EUROPEAN UNION (n.d.). *EU Artificial Intelligence Act*. EU Artificial Intelligence Act. <https://artificialintelligenceact.eu/>

FALKNER, G., HEIDEBRECHT, S., OBENDIEK, A. & SEIDL, T. (2024). Digital sovereignty - Rhetoric and reality. *Journal of European Public Policy*, 31(8), 2099–2120. <https://doi.org/10.1080/13501763.2024.2358984>

GSMA. (2019). *Data Privacy Frameworks in MENA : Emerging approaches and common principles*. <https://www.gsma.com/about-us/regions/middle-east-and-north-africa/wp-content/uploads/2019/06/GSMA-Data-Privacy-in-MENA-Full-Report.pdf>

HADDAD, J. (2022, June). Will Saudi Arabia tap into its potential and lead the charge toward digital sovereignty?. Arab News. <https://www.arabnews.com/node/2094801>

HAYAJNEH, A. (2021, September 13). *Personal data protection in the Middle East and North Africa*. Cullen International. <https://www.cullen-international.com/news/2021/09/Personal-data-protection-in-the-Middle-East-and-North-Africa.html>

HENKIN, L. (1995). *International law: Politics, values, and functions: General course on public international law*. Martinus Nijhoff Publishers.

JANSEN, B., KADENKO, N., BROEDERS, D., VAN EETEN, M., BORGOLTE, K., & FIEBIG, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4), 101862. <https://doi.org/10.1016/j.giq.2023.101862>

KOVÁCS, T. Z., BITTNER, B., NAGY, A. S., & NÁBRÁDI, A. (2022). Digital transformation of human capital in the EU according to the DESI index. *Issues in Information Systems*, 23(4), 293-311. [https://doi.org/10.48009/4\\_iis\\_2022\\_125](https://doi.org/10.48009/4_iis_2022_125)

MADIEGA, T. (2020, July). *Digital Sovereignty for Europe*. European Parliamentary Research Service. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/ EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/ EPRS_BRI(2020)651992_EN.pdf)

POHLE, J., & THIEL, T., (2020). Digital Sovereignty. *Internet Policy Review*, Vol. 9, (4), <https://doi.org/10.14763/2020.4.1532>

SAAIDA, M. (2023). Digital Sovereignty. *Science for all publications*, 6 (1), pp.1-12. [https://www.researchgate.net/publication/377019471\\_Digital\\_Sovereignty](https://www.researchgate.net/publication/377019471_Digital_Sovereignty)

SAUDI ARABIA'S NATIONAL PORTAL FOR GOVERNMENT SERVICES (n.d.). *Digital government strategy 2023-2030*. <https://www.my.gov.sa/wps/portal/snp/aboutksa/digitaltransformation/?lang=en>

SOLIMAN, M. (2021, January). *In the Middle East, cyber sovereignty hampers economic diversification*. Middle East Institute. <https://www.mei.edu/publications/middle-east-cyber-sovereignty-hampers-economic-diversification>

Telecommunications Regulatory Commission. (2023). *ICT Development Index 2023 (Information and communication technologies for development)* (p. 12). [https://trc.gov.jo/EchoBusV3.0/SystemAssets/%D8%AA%D9%82%D8%B1%D9%8A%D8%B1%202023\\_compressed.pdf](https://trc.gov.jo/EchoBusV3.0/SystemAssets/%D8%AA%D9%82%D8%B1%D9%8A%D8%B1%202023_compressed.pdf)

UNITED NATIONS DEVELOPMENT PROGRAMME – REGIONAL BUREAU FOR ARAB STATES (UNDP RBAS) & MOHAMMED BIN RASHID AL MAKTOUM KNOWLEDGE FOUNDATION (MBRF). (2023). *Global Knowledge Index 2023*. Knowledge for All. <https://www.knowledge4all.com/gki>

VALIAKHMETOVA, G. N., & TSUKANOV, L. V. (2022). Digital Challenge for the Arab World: Integration or Differentiation Factor?. *Vestnik RUDN*. International Relations, 22(2), 303-319. doi: 10.22363/2313-0660-2022-22-2-303-319

ZAWI, H. (2021, July 4). The gamble of digital sovereignty in the Middle East. *Khaleej Times*.

**Figure 01.** CULLEN INTERNATIONAL. (2021). *Status of personal data protection in MENA countries*. <https://www.cullen-international.com/news/2021/09/Personal-data-protection-in-the-Middle-East-and-North-Africa.html>

**Table 01.** UNITED NATIONS DEVELOPMENT PROGRAMME – REGIONAL BUREAU FOR ARAB STATES (UNDP RBAS) & MOHAMMED BIN RASHID AL MAKTOUM KNOWLEDGE FOUNDATION (MBRF). (2023). *Global Knowledge Index 2023*. Knowledge for All. <https://www.knowledge4all.com/gki>



# **Users' Digital Sovereignty in the Middle East and North Africa**

**Sara BAZOOBANDI**

Research Fellow, German Institute for Global  
and Area Studies (GIGA) Institute for Middle  
East Studies, Hamburg

## Digital sovereignty, a global debate

The term digital sovereignty has generated a debate amongst policy-makers, particularly in Western societies. It refers to the ability to control one's destiny in digital space. The term describes the capacity of individuals, organisations and states to own their digital assets (e.g., data, infrastructure, technology), obtain decisive advantages, (Scholze, 2023) and maintain control over their content, data, hardware and software (Fleming, 2021). Digital sovereign has been traditionally associated with states, but it is increasingly used to define the rights of non-state members (i.e., product and service providers as well as users) of the international digital community.

At individual level, digital sovereignty is focused on the role of consumers of digital services and their need for protection. In the European discourse around the extent and definition of digital sovereignty, the individual aspect is heavily influenced by the question of protecting consumers' data. European governments refer to digital sovereignty as a concept that allows states to use their authority over cyber space to protect their local citizens and businesses (Pohle, 2020). This somewhat contradicts the independence and flexibility of digital space.

At the state level, the notion of digital sovereignty goes beyond protecting citizens in digital space. It has been reinstating the nation-state by increasing the authority of states in the cyber realm. Through laws and regulations that allow governments to intervene in cyber sphere, the states have constantly conveyed the idea that such interventions are necessary to protect the culture, prosperity and security of nations. Further, this discourse puts a strong emphasis on the state's power and desire to

maintain technological independence from foreign powers.

In the 1990s, the global political debate was shifted towards the concept of post-sovereign, which emphasised the decline of states as the most superior power in the world system (MacCormick, 1993). "Cyber Exceptionalism", which is based on the fundamental differences between the digital and analogue spheres, emerged from this shift. It assumes that advancement of communication technology is inevitably leading to the demise of state and decline of its sovereignty (Katz, 1997). Considering the pace of digital technologies' advancement, and the limitations of national jurisdictions to regulate the digital sphere (Post, 2012) for a long-time digital exceptionalism dominated the global understanding on the state's capacity to control the digital sphere. However, in recent years, the concepts of sovereignty and statehood have reappeared in the global discourse, and digital sovereignty has been adopted in the political narratives of democratic and authoritarian governments alike.

As noted, digital sovereignty is formed around the idea of state's protection of citizens, though in practice it may well lead to more government control over citizens. Considering the complexity of this concept, digital sovereignty ought to be explained and adjusted according to societal and political realities. Therefore, its claims must be adjusted based on the capacity for digital self-determination by states, companies and individuals.

Edward Snowden's revelation in 2013 demonstrated the extent to which hegemonic power can indeed utilise the immense opportunities for data gathering and analysis for surveillance and control. It demonstrated that through collaborations between the intelligence agencies and tech companies, states can conduct sophisticated surveil-



lance and monitoring of individuals globally (Pohle & Thiel, 2020). As such, his revelations added another aspect to the ongoing debate that is based on the need for protective mechanisms against foreign and domestic surveillance or manipulation of information, infrastructure and policies.

Another approach to digital sovereignty claims, which is the focus of this study, departs from a state-centred understanding of sovereignty and acknowledges the autonomy of digital technologies and service users. It emphasises freedom of self-determination of the users and assumes that individuals can take independent and conscious actions in cyber world (Pohle & Thiel, 2020).

Through a “citizen-centric” approach in analysing digital sovereignty, this chapter seeks to answer two questions:

1. How are the citizens of the Middle East and North Africa (MENA) region practising their digital sovereignty?
2. How are the governments in the MENA region utilising the citizen’s digital sovereignty to pursue their own political agenda?

## Digital sovereignty in practice by MENA citizens

Digital technology has been a liberating phenomenon for the citizens of the region as it provides free flow of information and connects people across the society and to the outside world. The region is home to a relatively young population. One third of the population is reportedly under 30 years of age with a mobile phone penetration of around 68%. As of 2022, there are nearly 60 million fixed broadband sub-

scriptions in the region (World Bank, 2022). Use of Internet in the region has gone beyond urban educated elite, with more people across the region turned to digital space for information, opinion sharing, connecting with the global community, entertainment, and economic activities. Facebook, WhatsApp and Instagram accounts have been leading some of the most significant public debates across the region. They also have allowed people to create their own brand and promote new norms and discourse.

Digital technology has been an empowering tool for social enterprise and civic activism. Particularly in relation to gender issues, and financial technology, the digital realm has provided unique opportunities to the users across the board in the region. In this section, several examples are explored to demonstrate how individual users in the MENA region have used their autonomy and self-determination to push boundaries, lead social debates, shift traditional mindsets, and create economic opportunities.

### Social enterprise and civic activism

The debate about social issues, particularly those related to gender and sexuality, has been openly led by the citizens of the region in the digital sphere. Various individuals, interest groups and Non-Governmental Organizations (NGOs) have used the digital technology to raise awareness on topics that have been previously considered social taboos such as: women’s independence, honour killing, and femicide. In Egypt, cases of femicide have prompted open and frank discussions in the digital sphere (Smith, 2022). In Lebanon, where a combination of economic hardship, and culture of “militarised masculinity” (Davies, 2023) has boosted domestic violence, digital technology has provided the tools

Particularly in relation to gender issues, and financial technology, the digital realm has provided unique opportunities to the users across the board in the region.

for a public debate on these issues. Short videos and hashtags that are created for advocacy on women's right issues, and demanding government accountability to protect female citizens are widely distributed across the region. For decades, regional and international advocacy groups, NGOs, and international organisations have sought, but never fully managed, to prompt such wide-reaching debate. The situation of women across the region highlights the need for such debates and awareness-building, and the digital technology has visibly contributed towards building wide-reaching awareness. Considering the social and cultural dynamics, such debates are vital components for addressing some of the deep-rooted social, economic, and political ongoing challenges. The digital sphere has become a widely used space for those debates. The debate has also led to some tangible results and practical initiatives. A great example of such initiatives is the creation of TOOQ App, a mobile application designed by the Arab Trade Union Confederation, which is providing emergency response to women and girls facing violence.

In addition to raising awareness and demanding protection for women, digital technology is also providing the citizens of the region with platforms, where social taboos (e.g., LGBTQ issues) can be discussed. For example, Sowt, a widely popular Jordanian podcast network, has a variety of shows on such topics. Amongst those topics are "Ahwal" (Sowt.com, 2022), the personal status laws in Jordan (Davis, 2022), pregnancy outside wedlock, and generally what is considered "eib" (literally meaning taboo in Arabic) (Sowt.com, 2023) in the context of gender and sexuality. Such programmes offer surprisingly frank, cutting-edge, and progressive discussions on various social issues in Arab and Muslim societies, which would

not have been wide-reaching without the digital technological advancement.

Moreover, several digital TV channels and YouTube blogs have been created in recent years, which also open new spaces for discussions on social and cultural issues. For example, AB Talks (Bukhash, 2019), a widely popular digital chat show with over a million viewers across the region, has been covering a whole host of topics including religion, gender roles, gender stereotypes and division of domestic responsibilities, in conversations with personalities from the Arab world.

Internet penetration, access to less regulated content, and the global COVID-19 pandemic have boosted demand for digital entertainment. The share of digital revenue from total entertainment in the region has increased from 37% in 2019 to 46% by 2024 (About her, 2022). This has also led to increase in digital media content production as it is perceived by the public to be relatively free and less biased. Widespread use of digital technology has also opened space for debates around taboo subjects such as sexual health, reproductive health, and managing life after divorce in digital space.

Broadcast media in the region is heavily regulated and securitised by governments. As a result, there is a general lack of trust in the local broadcast media. Furthermore, the debates in digital platform have been increasingly influencing broadcast media. In many instances, after a subject or an event goes viral, digital space debates are then picked up by broadcast media. For example, issues such as assault on women in public spaces, particularly after Tahrir Square incidents, has been widely discussed across the broadcast media after the topic was raised openly in digital media. The impact of social media on public debates that is carried on the broadcast

media indicates the power and influence of social and digital media across the region.

Several campaigns have started in digital space, which specifically aim to raise awareness about rape. For example, in 2022, a campaign that featured Nour Arida, Lebanese model and Instagram influencer living in France, started as an anti-sexual assault advocacy project (About her, 2022). Such campaigns address a variety of issues, including female rape victims' guilt and lack of support for sufferers.

Moreover, since the Arab uprising that sparked multiple crises across the region and led to the rising outflow of Arab immigrants, Arab speakers in diaspora have also turned to digital space as a channel to remain connected to their old communities. Arab immigrants who have relocated because of regional crises have been looking for a platform to remain connected with their community while establishing a life in their new environment. They have also turned to digital media for entertainment, news, and participation in regional public debates. A Syrian YouTuber in Germany, Jilan Channel (Channel, 2023), with more than 300,000 subscribers, is a great example of use of digital space by Arab immigrants. Moreover, using online platforms for teaching and learning the Arabic language has become popular amongst Arab immigrants who reside outside of the region. Digital technology has provided some solutions for the challenge faced by the second-generation Arabic-speaking immigrants that are raised in non-Arab speaking countries to learn their mother tongue. For example, an innovative language programme called "Arabee" has been created in accordance with the Common European Framework of Reference for Languages in the United Arab Emirates (UAE) to be used by children, teachers, and parents (Tesorero, 2020).

There has been a rising trend in family content creators (formed by husbands, wives, and usually children) in the region, who are showcasing the dynamics of family life via social media. Family content producers and social media influencers, based in (or who come from) countries like Egypt, Saudi Arabia and the UAE, have become popular in recent years. Some of them have been influential in promoting socio-cultural changes on issues such as gender-based division of labour, lifestyles and prejudices against working mothers, and patriarchal bargain.

In addition to taboo topics, and family-related issues, lifestyle improvements, health and self-care have been widely covered by digital content producers across the region. Healthy eating and exercising at home have become widely discussed on digital platforms. The digital space has been instrumental in shifting the public mindset in the region from weight loss to lifestyle management and health.

This study revealed that there are some limitations to the progressivism of the digital media. Whilst it has had a profound impact on shifting the debate and opening space for discussions that were until recently considered as taboo (such as the rights and lives of the LGBTQ community), regional users broadly speaking refrain from endorsement of homosexuality and gender identity. This indeed varies across the region. Female Lebanese influencers with local audience are more likely to talk about religion or LGBT issues than for example those based in the UAE or Saudi Arabia. Moreover, there are signs of sectarianism and identity politics across the digital space amongst the regional users, which has been visibly exacerbated since October 2023.

Beyond the social debates, issues such as accountability and transparency of the

The digital space has been instrumental in shifting the public mindset in the region from weight loss to lifestyle management and health.

political and economic systems have been frequently discussed amongst the citizens of the region in the digital space. Online platforms are offering a unique space to continue a public debate on some of the fundamental political and economic issues. However, the MENA governments often view such debates as a sign of public discontent, and therefore closely monitor them. Critical views for the governments that are raised in the digital space are frequently used to prosecute individuals. There is a lack of transparency on the definition of political crime in the region. Therefore, fear of consequences for citizens' activities in the digital space hampers some aspects of the rapidly evolving debates in the digital sphere.

All in all, there is an egalitarian model to promote a value shift across the region in the digital space. The audience of digital content that is produced across the region is very mixed and comes from the broader Arabic-speaking countries. Widespread use of digital technologies has empowered individual users to debate personal and collective issues in an environment that is less regulated by the government compared with previously existing channels like printed and broadcast media. The citizens of the region have been practising their digital sovereignty to lead debates and shift traditional narratives within their own digital communities. As noted above, individual users in the MENA region have used their self-determination to push boundaries, lead social debates, and shift traditional mindsets. The next section will focus on how such self-determination has been creating new economic opportunities for the regional citizens.

### Financial technology

As many economies in the region embark upon their digitalisation journey, Financial Technology (FinTech) is gaining significance

in people's digital lives. Digital financial services such as money transfer, online lending, digital marketplaces, insurance services, Buy-Now-Pay-Later (BNPL) options, and digital wallets have been widely used across the MENA region. By the end of 2021, about 55% of the region's population were using mobile phones (GSMA Intelligence, 2022). Access to mobile phones and the global COVID-19 pandemic have boosted usage of contactless payments and cash alternatives (e.g., payments to domestic workers, drivers, and purchases from home businesses). Understandably, countries with more advanced digital infrastructure such as Saudi Arabia and the UAE, followed by countries like Egypt and Jordan, have been leading the regional FinTech market (Mordor Intelligence, 2020).

Due to technological solutions that are provided via smart mobile phones, the FinTech ecosystem is developing fast across the region. By 2020, about 465 financial startups were operating across the region. Ride sharing, peer-to-peer and small and medium-size enterprises (SME) lending services, and delivering companies are widely used by the young and tech savvy population across the region (see top FinTech startups [Forbes Middle East 2021] and trends [Lewis, 2021] in the MENA region).

The future of FinTech in the MENA region heavily depends on future investments (Netzer, 2021). Value of investment in FinTech companies have increased in the MENA region to over \$80 billion in 2022. The MENA digital banking sector grew more than 50% between 2021 and 2023 (FinTech News, 2023). Moreover, due to the strong focus on national security and state's control in cybersecurity and privacy regulations, FinTech ecosystems are exposing the region to a new set of risks, in addition to traditional security concerns (Skowron, 2021). Having said that, regional

Due to technological solutions that are provided via smart mobile phones, the FinTech ecosystem is developing fast across the region.

governments and central banks are adopting strategies to support this evolving ecosystem.

The Central Bank of Egypt launched an initiative called Instapay, a digital payment platform, for cash alternative payments. Some local mobile phone providers like Vodafone have already introduced such services that are widely used in the country. By 2023, 6.2 million Egyptians used InstaPay for over 300 million transactions (Egypt Independent, 2023). With nearly half of the nation being on social media platforms, negligible transaction costs and ease of service, digital payment platforms are expected to attract more users in the years to come.

Digitalisation of the economy could boost economic growth through creation of jobs, particularly among women and youth. Economic conditions have been deteriorating in many countries in the MENA region. In Egypt, for example, currency depreciation as well as inflation has led to shortage and inflation of imported goods. New space has been opened for local and home businesses that offer more affordable goods and services. Such possibilities are providing innovative practices by small businesses and creating job opportunities. Advancement of FinTech in the MENA region demonstrates the ability of citizens in practising their digital sovereignty to create innovative economic prospects. It is also worth noting that digitalisation of the economy exposes the region to a new set of challenges in the long run. Limitation of access to technology, the challenges associated with gig work, the threat of job loss with the increase in automation indicate that the promise of technology for digital sovereignty is not absolute. In the next section, several cases and examples will be reviewed to demonstrate how the governments in the MENA region seek to utilise citizens' digital sovereignty to pursue their own political agenda.

## Challenges to citizens' sovereignty in the digital realm

The two main positive impacts of user-based digital sovereignty in the MENA region have been discussed. This section will explore how the governments in the region have been challenging users' right to self-determination in the cyber world. Digital technologies have provided a variety of tools for state monitoring and surveillance. From Cairo to Tehran, regional governments have been seeking to control and monitor the citizens in the digital world. Over the past decade, so-called "cyber armies" have been formed across the region. The region's cybersecurity market is projected to reach from \$7.5 billion in 2022 to \$31 billion by 2030. That is a compound growth rate of 20% per year (Cabral, 2023). Moreover, several governments have begun to introduce new laws to regulate the cyber sphere within their jurisdictions. Most governments have enforced laws that endorse surveillance and give the state the right to censor digital content (von Finckenstein, 2019). Several countries have also introduced data protection measures. The Egyptian government approved the Personal Data Protection Law in 2020, which limits personal data transfer outside the country. In Saudi Arabia, the government has introduced measures for cloud computing security (Saudi National Cybersecurity Authority, 2020), and in the UAE various data protection measures have been put in place by the government, including the Dubai International Financial Centre (DIFC) data protection law (DIFC, 2020). While data localisation is presented by regional governments as measures to protect their citizens in the digital sphere, in the present form, they limit innovation and isolate digital econ-

Advancement of FinTech in the MENA region demonstrates the ability of citizens in practising their digital sovereignty to create innovative economic prospects.

omies along national borders (Soliman, 2021).

Examining the governments' strategies towards users' digital sovereignty indicates attempts to manipulate the domestic and international narratives. Such manipulation attempts are evident in the case of the Syrian government. The war in Syria took more than half a million lives, displaced more than 10 million people, destroyed the country's critical infrastructure, and pushed the economy into a crippling state. To change the country's international image, in recent years the government has been allegedly sponsoring Internet influencers to showcase an image of Syria that does not embody war and dictatorship (Roy, 2023).

The government has recruited several popular travel influencers from Western countries, which coincided with the normalisation with the Arab League, to showcase the country's attractions, with no mention of exacerbated inequality. Syria lost substantial tourism revenue because of the war. The government has implemented tight visa vetting to limit access to foreign journalists. There has also been heavy-handed digital surveillance in place to filter out unfavourable reporting from inside Syria (Fullerton, 2022). YouTube has been criticised by Syrian activists for deleting video footage of the war in Syria, to limit spread of extremism (Al Khatib & Kayyali, 2019). All in all, the strategies of the Syrian government demonstrate a clear case for the ways in which governments in the MENA region may seek to utilise citizens' digital sovereignty to pursue their own political agenda.

Another aspect of pursuing government political agenda in the region is through content regulation policies. The MENA governments have strict regulations on

criticising the government and senior government officials. Violation of these regulations is prosecuted according to the local legislations, which in most cases involves the removal of the content. Moreover, creating content that is considered by the local government to be damaging to its international reputation is also penalised. The reputation of the political system has been of high significance for most of the MENA governments, as it is an instrumental factor in shaping their international political and economic relations. Most MENA governments have been pursuing strategies that help maintain their reputation as holders of value-based agendas, open and tolerant political systems, which are continuously improving issues such as transparency and accountability. The digital space is closely monitored to stop a distorting narrative and inflict a sense of control and fear amongst the citizens to prompt self-censorship that challenge such a reputation, regardless of the realities on the ground in their respective countries.

## Conclusions

All in all, the users' digital sovereignty and MENA citizens' right to self-determination in the cyber space is undeniable. It is empowering the users and has been clearly effective in promoting a value shift. However, the citizens' digital sovereignty is challenged by the governments in some other respects such as public debates on the government's performance, its reputation, and accountability of its senior politicians. Moreover, some of the examples that are reviewed in this chapter reveal that governments' strategies towards users' digital sovereignty can be directed at manipulating the domestic and international narratives towards the respective governments.

This chapter concludes that the underlying cause for such challenges are rooted in the state-citizens' relationships in the MENA region and the conflict of perceptions and interests between the government leaders and the public. Democratic processes across the region have failed or stalled. As such, the political leaders are becoming increasingly detached

from their constituents. This detachment motivates the governments to focus on power preservation rather than social and economic improvement. Citizens' controlling strategies, including those in the digital realm may remain the usual code of conduct across the MENA region, but, nevertheless, users' digital sovereignty will ultimately prevail over government control.

## Bibliography

ABOUT HER. (2022). Anti-Rape Campaign Disrupts Arab World Online Sphere <https://www.abouter.com/node/55661/entertainment/music-film-television/anti-rape-campaign-disrupts-arab-world-online-sphere>

AL KHATIB, H & KAYYALI, D. (2019). YouTube Is Erasing History. *The New York Times*. <https://www.nytimes.com/2019/10/23/opinion/syria-youtube-content-moderation.html>

BUKHASH, A. (2019). AB Talks. YouTube. <https://www.youtube.com/hashtag/abtalks>

CABRAL, A. (2023). Middle East Cybersecurity Market to Hit \$31bn by 2030 as Government Initiatives Grow. *The National*. <https://www.thenationalnews.com/business/technology/2023/03/14/middle-east-cybersecurity-market-to-hit-31bn-by-2030-as-government-initiatives-grow/>

DAVIES, L. (2023). Burned, Suffocated, Beaten: Why Women in Lebanon Are Dying at the Hands of Their Partners. *The Guardian*. <https://www.theguardian.com/global-development/2023/feb/27/lebanon-women-dying-partners-domestic-abuse>

DAVIS, D. (2022). "Elephant in the Room": Jordanian Women and Equal Rights. *Aljazeera*. <https://www.aljazeera.com/news/2022/2/18/elephant-in-the-room-jordanian-womens-struggle-for-rights>

DIFC. (2020). *Data Protection Law DIFC law no.5 of 2020*. [https://edge.sitecore-cloud.io/dubaiintern0078-difcexperie96c5-production-3253/media/project/difcexperiences/difc/difcwebsite/documents/laws—regulations/data\\_protection\\_law\\_final.pdf](https://edge.sitecore-cloud.io/dubaiintern0078-difcexperie96c5-production-3253/media/project/difcexperiences/difc/difcwebsite/documents/laws—regulations/data_protection_law_final.pdf)

EGYPT INDEPENDENT. (2023). CBE Reveals Number of InstaPay Users & Volume of Egyptian Transactions. <https://www.egyptindependent.com/cbe-reveals-number-of-instapay-users-volume-of-egyptian-transactions/>

FINTECH NEWS. (2023). Digital Banking Grows 52% in the Middle East. <https://fintechnews.ae/17805/fintech/digital-banking-grow-in-the-middle-east/>

FLEMING, S. (2021). What Is Digital Sovereignty and Why Is Europe so Interested in It?. *World Economic Forum*. <https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/>

FORBES MIDDLE EAST. (2021). Top 20 fintech startups in the Middle East. <https://www.forbesmiddleeast.com/list/top-20-fintech-startups-in-the-middle-east>

FULLERTON, S. (2022). Influencers Are Whitewashing Syria's Regime, with Help from Sponsors. *Washington Post*. <https://www.washingtonpost.com/opinions/2022/08/08/travel-influencers-whitewash-syrian-war/>



GSMA INTELLIGENCE. (2022). *The Mobile Economy in Middle East and North Africa*. [https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/05/GSMA\\_MENA\\_ME2022\\_R\\_WebSingles.pdf](https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/05/GSMA_MENA_ME2022_R_WebSingles.pdf)

JCHANNEL, J. (2023). *Jillan Channel*. YouTube. [https://www.youtube.com/@Jilan\\_channel](https://www.youtube.com/@Jilan_channel)

KATZ, J. (1997). Birth of a Digital Nation. *Wired*. <https://www.wired.com/1997/04/netizen-3/>

LEWIS, S. (2021). 7 Popular Middle East Fintech Trends 2021. *FinTech News*. <https://fintechnews.ae/10313/fintech/7-popular-middle-east-fintech-trends-2021/>

MACCORMICK, N. (1993). Beyond the Sovereign State. *Modern Law Review* 56(1): 1–18. <https://doi.org/10.1111/j.1468-2230.1993.tb02851.x>

MORDOR INTELLIGENCE. (2020). *MENA Fintech Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)*. <https://www.mordorintelligence.com/industry-reports/mena-fintech-market>

NETZER, N. (2021). *The Future of FinTech in the Middle East: Trends That Are Here to Stay*. *Middle East Institute*. <https://www.mei.edu/publications/future-fintech-middle-east-trends-are-here-stay>

POHLE, J. (2020). Digital Sovereignty. Konrad Adenauer Stiftung. <https://www.kas.de/documents/252038/7995358/Digital+sovereignty.pdf/a8d0cb4b-c777-3e72-1bc7-b5fda656329a?version=1.0&t=1608034389334>

POHLE, J., & THIEL, T., (2020). Digital Sovereignty. *Internet Policy Review*, Vol. 9, (4), <https://doi.org/10.14763/2020.4.1532>

POST, D.G. (2012). Governing Cyberspace: Law. *Santa Clara High Technology Law Journal* 24(4), 883–913.

ROY, J. (2023). *The Two Faces of TikTokers Promoting Syrian Tourism*. *New Lines Magazine*. <https://newlinesmag.com/argument/the-two-faces-of-tiktokers-promoting-syrian-tourism/>

SAUDI NATIONAL CYBERSECURITY AUTHORITY. (2020). *National Cybersecurity Authority Controls for Cloud Computing*. Saudi National Cybersecurity Authority. <https://dcybersecurity.sa/nca-cybersecurity-controls-for-cloud-computing-ccc/>

SCHOLZE, M. (2023). *Why It Pays to Be Independent: Digital Sovereignty*. PWC. <https://www.pwc.de/en/digitale-transformation/open-source-software-management-and-compliance/digital-sovereignty-why-it-pays-to-be-independent.html>

SKOWRON, J. (2021). *FinTech in the Middle East – The Rise & Prospects in Digital Banking*. Code and Pepper. <https://codeandpepper.com/fintech-in-middle-east/>

SMITH, A. (2022). *Third Femicide in Egypt in 3 Months after Young Woman Says “No” to Marriage Proposal*. Middle East Monitor.

<https://www.middleeastmonitor.com/20220905-third-femicide-in-egypt-in-3-months-after-young-woman-says-no-to-marriage-proposal/>

SOLIMAN, M. (2021, January). In the Middle East, cyber sovereignty hampers economic diversification. *Middle East Institute*. <https://www.mei.edu/publications/middle-east-cyber-sovereignty-hampers-economic-diversification>

SOWT.COM. (2022). Ahwal. <https://podcasts.apple.com/gb/podcast/ahwal-%D8%A3%D8%AD%D9%88%D8%A7%D9%84/id1290797957>

SOWT.COM. (2023). Eib. <https://www.sowt.com/en/podcast/eib>

TESORERO, A. (2020). App Launched in UAE to Make Learning Arabic Fun and Easy. *Gulf News*. <https://gulfnews.com/uae/education/app-launched-in-uae-to-make-learning-arabic-fun-and-easy-1.75021368>

VON FINCKENSTEIN, V. (2019). *Cybersecurity in the Middle East and North Africa*. Konrad Adenauer Stiftung. <https://www.kas.de/documents/284382/284431/Policy+Paper+on+Cybersecurity+in+the+Middle+East+and+North+Africa.pdf/50199440-b10e-3dea-52ca-c0e3714ebc75?version=1.0&t=1564581818218>

WORLD BANK. (2022). Fixed Broadband Subscriptions - Middle East & North Africa. World Bank. <https://data.worldbank.org/indicator/IT.NET.BBND?locations=ZQ>

# **Balancing Resilience and Innovation: How do MENA Countries Manage Cyber-Related Challenges?**

**Chloé BERGER\***

Assistant Professor, National Defence College  
of the United Arab Emirates

\*The opinions expressed are those of the author and do not reflect the views of the National Defence College or the United Arab Emirates government.

## Introduction

Since the late 1990s, digital technologies have gained considerable importance in statecraft and international relations. Digital transformation of societies has brought both new opportunities and challenges. Over the past decade, security challenges related to digital sovereignty have grown significantly, affecting regions worldwide. These challenges include cyberattacks on critical infrastructures, sabotage and physical attacks on network infrastructure, disinformation, cyber espionage, and cyber warfare. Faced with the rapid development of these new threats, often referred to as “hybrid threats”, states have often found themselves in a reactive position, forced to urgently deploy cybersecurity and cyber defence countermeasures, as well as to protect critical connectivity infrastructures (such as physical infrastructure protection and oversight of connectivity project investments). Over time, many countries and security organisations (such as the North Atlantic Treaty Organization [NATO] and the European Union [EU]) have developed strategies to protect personal data, defend against cyber threats, and enhance their space-based capabilities (NATO, 2024).

Technological advancements in the digital realm have engendered novel synergies and collaborations, concurrently spawning new forms of competition, thereby adding complexity to the international shifting power dynamics. Primarily, the incorporation of digital technologies into governance mechanisms and institutions has equipped governments with tools and methodologies to enhance the efficiency of public institutions, optimise asset and resource management, improve the delivery of public goods and services, and more meaningfully engage citizens in the decision-making process. The gradual transition towards governance models increasingly underpinned by digital technologies (artificial intelligence [AI], Big

Data and analytics, blockchain, cloud computing, Internet of Things [IoT], quantum computing, and so on) (Saeed et al., 2023) is anticipated to refine the policy decision-making process by enhancing simulation and analytical abilities, consequently bolstering the legitimacy of governments in the eyes of their citizenry.

Hence, the digitalisation of statecraft and the rise of networked societies are likely to profoundly impact foundational concepts such as the social contract and the sovereignty of the nation-state. While some highlight the augmented potential for control and surveillance that the digitalisation of societies offers to state apparatuses, pointing out the emergence of forms of digital authoritarianism (Shahbaz, 2018), whose repressive capabilities would be merely amplified by AI (Funk, 2023), others argue that the widespread dissemination of these technologies contributes to the erosion of the centrality of nation-states, as shown by the heightened amount of cyberattacks reported against state facilities and interests, and private corporations. This erosion is facilitated by supporting the development of transnational dynamics that enhance the influence of non-state actors, and also due to the nature of the systems of development, production, and exploitation of these technologies.

The study seeks to reflect on the implications of the growing digitalisation of both the security and civil spheres on MENA countries' resilience and ability to govern innovation. Taking stock on the significant differences between countries across the region (economic structures and performance, degree of societal connectivity, barriers and/or support for innovation, military structures and composition of their arsenals, etc.) in terms of digitalisation progress, the research attempts to identify various profiles or patterns of “digital sovereignty” and to reflect on how they concur to modifying

MENA countries' traditional understanding of sovereignty.

## Exploring the various facets of the MENA region's security landscape digitalisation

Since the middle of the last decade, in response to an international technological ecosystem predominantly dominated by the United States (US) and China, certain European states have begun to express concerns over the risk of a "technological vassalisation of Europe". The "geopoliticisation" of technology has raised apprehensions regarding the control and exploitation of citizens' personal data, as well as the capability of Europeans to contribute to innovation and the establishment of norms and standards in the digital realm. This European aspiration to better ensure Europe's strategic autonomy in the digital domain has manifested in the initiation of a debate concerning the "protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)" (Madiaga, 2020).

Three areas are of particular concerns for the EU (Madiaga, 2020) and its member states: firstly, the influence of non-EU tech companies (mainly Chinese and US companies) on EU data economy, research and development capabilities and digital infrastructure; secondly, the leading contributions of these non-EU companies to EU member states' digital transformation raises concerns with respect to data collection and protection; and thirdly, the over-reliance on infrastructure built and owned by non-EU companies exposes EU member states to critical vulnerabilities in terms of data control and infrastructure protection and resilience against cyberat-

tacks. If cyber threats represent a growing portion of the strategic challenges that states must confront and the cyber defence and security tend to acquire more and more importance in national security strategies, one should also acknowledge the increasing mobilisation of the "cyber" theme in national strategic narratives, in particular with respect to combating terrorism and countering hybrid threats.

The dual nature of digital technologies compels a re-evaluation of the concept of digital sovereignty from the perspective of strategic and security studies, reflecting on the implications of a potential securitisation of these issues for societal resilience and the ability of societies to govern innovation. The promotion of norms and standards lies at the heart of the EU's foreign policy and its soft power. Consequently, it is intriguing to examine how the concepts promoted by the EU are apprehended and perceived by its partners, as well as its competitors.

From this perspective, we argue that the Middle East and North Africa (MENA) region presents a particularly interesting analytical terrain for several reasons. First of all, MENA countries compose the direct periphery of Europe; as a result, any societal evolution holds potential repercussions for Europe's stability and security. Moreover, EU member states have vested economic, diplomatic and security interests in the region. European states continue to play a significant role in the development of the innovation ecosystems and digital markets of their Mediterranean neighbours, as well as in the development, exploitation and protection of the critical infrastructure of North African countries, and to a lesser extent, the Levantine countries. However, they face increasing competition from the Gulf States, China or the US as telecommunication actors in the development and deployment of digital infrastructure and

The "geopoliticisation" of technology has raised apprehensions regarding the control and exploitation of citizens' personal data.

Given the multifaceted challenges faced by countries in this region, coupled with the significant growth and development opportunities linked to digital transformation, it is imperative for European institutions and EU members to engage more productively with MENA actors.

technologies in the MENA region. Given the multifaceted challenges faced by countries in this region, coupled with the significant growth and development opportunities linked to digital transformation, it is imperative for European institutions and EU members to engage more productively with MENA actors. Currently, technological competition around AI technologies primarily involves Gulf countries (and to a lesser extent, Israel). However, European countries can bring their unique normative expertise to help MENA partners build more inclusive and fair digital societies and economies.

### **The MENA region: a unique laboratory for warfare experimentations**

Information and communications technologies (ICT) have rapidly become integrated into the strategies and regular operations of both state and non-state actors in the region. In that respect, we argue that the Syrian conflict has marked a turning point in the integration of digital technologies into the operational strategies of combatants. More generally speaking, both conflicts in Syria and Libya have provided unique opportunities for states to test new autonomous systems and to experiment with associated warfare techniques.

The interest of regional actors in computing and cyber capabilities is not a recent development. Israel has been using computing technology since the mid-1960s (Midbon, 2020). During the 2006 war in Lebanon, Hezbollah had already demonstrated its capability to launch multiple cyberattacks against the communication systems of the Israel Defence Forces (IDF) and certain Israeli allies, as well as exploiting vulnerabilities in websites to disseminate the messages of Al Manar channel more broadly. Since then, its capabilities – and competencies – in cyber defence and cyberwarfare have continuously evolved, benefiting from Iran's expertise.

From the late 2010s, Iranian cyber warfare capabilities have been on the rise, benefiting especially from the lessons learned from operations conducted in the region by the Israelis,<sup>1</sup> as well as from the opportunities for real-world experimentation on the Syrian battlefield. Iran claims to possess the fourth largest cyber force in the world. Compared to its neighbours, Iran has quantitatively more developed digital capacities, as evidenced by the number of secure Internet servers registered in Iran (203,430 units in 2020 versus 113,823 units for Israel<sup>2</sup>). However, according to most observers, the level of Iranian cyber capabilities and operational methods remains limited in comparison to its Israeli counterpart. Through its support of numerous groups

<sup>1</sup> See operations Orchard and Stuxnet. Iran is said to have started developing its cyber capabilities in 2009, following the Stuxnet operations which targeted about 20,000 devices in 14 nuclear facilities and large-scale protests of the "green movement". Building on these experiences, The Islamic Revolutionary Guard Corps (IRGC) had taken control over the Telecommunications Company of Iran, supported the development of the "autonomous" Iranian Cyber Army. Iranian authorities created a Cyber Defence Command (2010) for the armed forces, and a Cyber Police Force (2011). As a reflection of the importance of the cyber domain for the Iranian leadership, the Supreme Leader heads the Supreme Council for Cyber Space (2012), created to "fully exploiting the positive potential of Iranian cyberspace" and "protecting the country and people from the negative potential of cyberspace", comprised of representatives of (semi-)governmental institutions dealing with cyber issues (IISS, 2018).

<sup>2</sup> Although a significant disparity is observed when figures are adjusted for population size, it is important to remember that in Iran, cyber capabilities are primarily controlled by the Iranian authorities. Despite these limitations, Iran nevertheless ranks far ahead of its Gulf neighbours (UAE, with 13,901 servers; KSA, with 7,977) (World Bank, 2020).

within the region, Iran has clearly contributed to a broader dissemination of cyber warfare tactics among various factions, including Hamas, the Houthis in Yemen, and Shiite militias in Iraq, among others. While Israel and Turkey remain the leading regional manufacturers of Unmanned Aerial Vehicles (UAVs) in the region, Iran has also played a pivotal role in the acculturation of non-state actors within the region to UAV technologies (El Doh, 2024). In the attacks of 7 October, 2023, Hamas forces utilised drones to breach the fence around Gaza. Subsequently, Hezbollah in South Lebanon, the Houthis in the Red Sea, as well as Shiite factions in Syria and Iraq have employed drones for reconnaissance and surveillance operations, as well as for targeted attacks. In recent carefully calibrated retaliations against the targeting of the Iranian consulate in Damascus, Iran launched an impressive fleet of 170 armed drones against Israel (Brown & Neff, 2024), demonstrating the potential of “low-cost” strategic swarming operations. Although drones themselves do not directly serve as instruments of cyber warfare, their operational deployment indispensably relies on the utilisation of digital technologies.

## **The transformational impact of social media**

With the “Arab Spring”, social media emerged as a pivotal conduit for mobilising collective action, contributing to a grassroots re-politicisation that transcended national borders, social classes, and generational divides within the region’s societies. Social media and digital technologies paved the way for the emergence of a low-cost information warfare. With the heightened challenges to access theatres of conflict, activists who employ social media to disseminate images of the conflict have gradually supplanted conventional media war correspondents. Since the beginning of

the Arab Spring, there was a proliferation of a significant number of online media outlets – magazines, newspapers, observatories, databases; news channels; not to mention videos filmed by individuals, ranging from amateur to professional, on the ground which are now being distributed virally on traditional social media platforms such as Facebook, YouTube, Instagram, but also on WhatsApp.

As social media platforms have gradually superseded traditional media outlets (television channels and newspapers) as the primary source of information in MENA societies where more than 60% of Internet users primarily rely on social media (Herbert & Ghouli, 2019)- particularly among the youth – one can easily imagine how the heightened visibility of conflicts on these networks may have simultaneously led to a normalisation of violence and a sense of “compassion” fatigue among the public both within the region and abroad. Regional conflicts’ “hyper-visibility” has also provided a fertile ground for disinformation campaigns and informational operations. Intriguingly, the increase in Israeli surveillance resources dedicated to monitor Lebanese theatre since the 7 October 2023 has unexpectedly affected the daily life of both populations, leading, for instance, to a blending of the profiles of Lebanese and Israeli users on Internet applications (Dagher & Dorandeu, 2024), revealing the scope of the potential manipulation of users’ personal data.

More importantly, the omnipresence of war imagery and narratives have popularised a specific aesthetic of war while fostering a sense of despair among young people, encouraging the radicalisation of certain groups, and facilitating the recruitment of local and international combatants (Airbus Defence and Space, 2020). The ongoing conflict in Gaza has recently demonstrated the power of mobilisation around conflict dynamics well beyond the societies of the

region. As emphasised by Andrej Zwitter (2014), “Big Data has induced a hyper-networked world society, in which it is easier than ever before to engage in common political causes irrespective of national boundaries.”

### **Are Big Data, AI and unmanned vehicles game changers?**

Big Data is fundamentally altering the strategic landscape by primarily affording state actors, and increasingly non-state actors, the potential to achieve near “omniscience”. Consequently, it has become increasingly common for state actors (or state sponsored actors) to employ techniques aimed at controlling the flow of information online, by reducing the bandwidth available to regular “consumers” during specific periods<sup>3</sup> or more simply shutting down the access to the local service providers, or Internet filtering practices (Noman, 2019) to prevent contents considered “hostile” to reach domestic audience through the use of proxy servers and DDoS attacks.<sup>4</sup>

Furthermore, AI-related technologies possess transformational potential due to their capacity to process/manage vast volumes of data, their velocity (enabling almost real-time data collection and processing), and their adeptness at handling a wide variety of both structured and unstructured data. Digital technologies afford the opportunity to rethink the collection, production and dissemination of information in a “low-cost” manner, bringing it closer to the field. These technical possibilities have not gone un-

noticed by key stakeholders: the United Nations (UN), for instance, has supported the development of “peace tech” projects (UN Global Pulse, 2019) designed to facilitate access to field data, enhance the understanding of conflict dynamics, and contribute to the improvement of security for humanitarian actors on the ground.

AI and associated technologies are at the nascent stage of revealing the breadth of innovative opportunities they present for enhancing the operational efficiency of armed forces on the battlefield, augmenting force preparedness and readiness, and improving the intelligence cycle. Notably, the reported deployment by the Israel Defence Forces (IDF) of AI-driven technologies to refine their identification and targeting capabilities during their ongoing operations in Gaza – referred to as the “Lavender” system (Abraham, 2024) – has elicited significant concerns due to the substantial civilian casualties resulting from the conflict. More broadly, these technological advancements have sparked extensive debates concerning the risks associated with the application of emerging and disruptive technologies in military contexts.

The MENA region has been actively engaged in these discussions, witnessing a growing interest in the defence and security potential of emergent technologies such as AI, Big Data, and UAVs. The MENA region is one of the global areas where defence and security expenditure, along with the procurement of materials and technologies, rank among the highest worldwide. This has fuelled an intense competition

The MENA region is one of the global areas where defence and security expenditure, along with the procurement of materials and technologies, rank among the highest worldwide.



among the world's leading AI actors to secure influence in MENA countries' future AI-related projects, primarily the US and China, followed by European countries, then Israel and Turkey.<sup>5</sup> Currently, only the most technologically advanced countries in the region, such as Israel, the United Arab Emirates (UAE), and the Kingdom of Saudi Arabia (KSA), have seriously begun to develop their AI industries. Israel, often referred as the "StartUp Nation" (Senor & Singer, 2011; Regenbaum, 2023), holds an undeniable advantage in research and development, supported by a robust ecosystem comprising research institutions, universities, startups, and leading companies in both civilian and defence digital technologies. On the other hand, the digital powerhouses of the Gulf have unparalleled investment capabilities. Supported by the substantial resources of their sovereign wealth funds, the UAE and Saudi Arabia have embarked on a race to develop cutting-edge digital technologies – AI,

quantum computing, Big Data –, with backing from leading players in the field. In this context, Morocco benefits from its strong relations with both Israel<sup>6</sup> and the UAE to accelerate its digital transformation.

### Towards a growing “securitisation” of digital technologies in the MENA region?

Moreover, the fast and significant progress of digitalisation within MENA societies and economies, as well as the significance of the region in global energy markets, have rendered certain MENA countries – the UAE, KSA, Israel, Turkey, and Egypt – among the primary targets for advanced persistent threats (APTs, i.e. states-sponsored cybercriminals and hacktivists) in the world (15% of global cyberattacks in 2023) (Clewlow, 2024).

**Table 1.** Concentration of damages due to web cyber-attacks by industry by region (2022-2023)

Affected industry	MENA	East Asia	South-East Asia	Africa	Eastern Europe
Government/Military	48.9%	29.8%	57.3%	78.8%	36.8%
Financial	15.4%	11.1%	16.8%	0%	19.1%
Telecommunications	10.4%	1.8%	2.3%	5.8%	3.8%
Medical	6.6%	5.3%	7.1%	3.8%	8.1%
Retail	4.0%	17.5%	5.5%	5.8%	12.0%

Table adapted from study by Shim & Oh (2024).

Malign cyberspace actors aim primarily to illegally acquire data (data thefts and breaches) from governmental entities and business enterprises to blackmail

organisations (ransomware) or leak highly sensitive data (data leaks) to disrupt daily operations. In 2023, Turkish financial organisations, Iraqi and Saudi govern-

mental institutions, and Israel's telecommunication industry were the primary targets in the region (Shim & Oh, 2024). Emanating from a complex galaxy of actors, where criminal organisations and

"mercenary" hackers operate on behalf of state interests, cyber threats primarily target critical infrastructure and key economic sectors of the countries in the region.

**Table 2.** Concentration of damages due to web cyber-attacks by country and industry (2022-2023)

Affected industry	MENA	Türkiye	Iraq	UAE	KSA	Israel
Government/Military	48.9%	47.0%	69.7%	16.7%	52.4%	42.6%
Financial	15.4%	19.7%	3.0%	16.7%	4.8%	13.0%
Telecommunications	10.4%	1.5%	27.3%	25.0%	4.8%	13.0%
Medical	6.6%	13.6%	0.0%	16.7%	19.0%	3.7%
Retail	4.0%	3.0%	0.0%	8.3%	0.0%	7.4%

Table adapted from study by Shim & Oh (2024).

There is a widespread "securitisation of digital technology" evident through the development of legal frameworks dedicated to combating cybercrime and cyberterrorism.

The escalating frequency of cyberattacks has fostered the development of national cybersecurity capabilities, primarily oriented towards enhancing the resilience of the institutions and economies of the region. In the MENA region, cyber-defence remains for the moment the prerogative of the most militarily advanced countries – Israel, Iran, the UAE, KSA, Turkey. The digitilisation of security and defence apparatuses, reflecting the broader digital transformation of the region's countries, reveals significant disparities among these actors. However, there is a widespread "securitisation of digital technology" evident through the development of legal frameworks dedicated to combating cybercrime and cyberterrorism. These legislative developments entail imposing stringent regulations on the usage of social media, broadening the surveillance powers of government security services for the purposes of information oversight, and the aggregation of personal data from citizens.

Digitalisation of the economies and military advances in the cyber and space domains challenge MENA countries' traditional missions and modes of intervention of armed forces and security apparatuses,

while also impacting the resilience of states and societies. More importantly, they tend to deepen inequalities within the societies of the region, and even more so between the countries of the region, considering that only those with innovation ecosystems will have the capacity to meet the challenges associated with emerging "disruptive" technologies such as AI, quantum computing, robotics, and so on. Thus, the digital transformation of MENA societies and economies does not escape the dynamics of rivalries and arms races characteristic of this region, posing considerable challenges to the sovereignty of MENA countries.

## Identifying the critical enablers of MENA countries' digital transformation

Over the last decade, the digital transformation has advanced at a rapid pace across the MENA region, with Israel and the Gulf countries of the forefront of this development. The number of Internet users has grown from over 58 million in 2009 to

over 100 million in 2013, and then to over 200 million in 2021 (Statista, 2024). There was a leap to 349.57 million between December 2021 and June 2022, driven by the deployment of fastest connections (4Gs) in most of the MENA countries.<sup>7</sup> Since the end of the COVID-19 period, major progress has been accomplished by MENA countries, driven by huge investments in AI, and other digital technology in the Gulf. On average, 77% of the region's inhabitants use the Internet daily, spending almost four hours daily surfing on average (Statista, 2024), with the exception of Israel, Gulf Cooperation Council (GCC) countries and Egypt where users spent more than seven hours a day on the Internet. However, about 30% of the regional population remain "digitally excluded" (Yassin & El Nahlawy, 2023), increasing their marginalisation. Significant disparities remain between the Gulf countries, where 100% of the population is connected, and countries like Yemen, Syria and Libya, where less than a third of the population has Internet access.

In 2018, the Arab League unveiled the "Arab Digital Economy Vision" (League of Arab States, 2020), which pledges to a sustainable, inclusive, and secure digital future for the region. Similarly, most countries in the region have formulated national digital strategies, with some even advancing to develop AI strategies. While potential benefits of the digital economy are well acknowledged – such as growth, job creation, and reduction of social inequalities – governments' commitments to advancing the digital transformation in the governance

and economic domains have yielded mixed results, due to several factors.

### **MENA countries' digital infrastructure limitations: geography and legacy**

First of all, the state of infrastructure and the varying density of its distribution across national territories remain key variables: in the Palestinian Territories, where infrastructure is dense despite ongoing instability, 89% of the population is connected, compared to just over 70% in Egypt and Algeria, where Internet coverage remains limited in many rural areas. The distribution of telecommunications infrastructure has often replicated the unequal dynamics that characterise territorial development, despite corrective measures implemented by some governments, such as Egypt's "Digital Egypt 2030" plan (American Chamber of Commerce in Egypt, 2021). This initiative aims, among other goals, to develop "tech parks" (data centres and innovation ecosystems) across the country, to enhance connectivity and increase the attractiveness of medium-sized cities such as Minya, Mansoura and Aswan.

Consequently, fixed broadband subscriptions are limited (14.67 fixed broadband subscriptions on average per 100 people) in the MENA region, with fewer than 10 subscriptions per 100 people in most countries of the region, except in Israel (nearly 30 per 100 people), Tunisia (13.67 per 100 people), and Iraq (14.35 per 100 people) (Gelvanovska, Rogy, & Rossotto,

About 30% of the regional population remain "digitally excluded", increasing their marginalisation.

2014; World Bank, 2023). MENA users access the Internet primarily through mobile cellular devices (124 subscriptions per 100 people on average in 2022), with over 205 subscriptions per 100 people in Libya, compared to 152 for Israel. However, while cellular use is highly developed in North Africa (more than one subscription per person) (World Bank, 2023), it remains more limited in the rest of the region. Although prices have significantly decreased over the past two decades, cellular subscriptions remain expensive due to the limited competition in the mobile telephony market; often, national and historical operators have maintained a dominant position, having no incentive to lower their prices. In this regard, Iraq presents a unique case due to the considerable investments made in the telecommunications sector, particularly in Iraqi Kurdistan since the late 2000s.

These disparities reflect the crucial role that national and international operators play in the development of telecommunications infrastructure in the MENA region. Capitalising on the progress made over the last decade, operators from the Gulf countries, equipped with the financial resources and expertise necessary for managing mega infrastructure projects in the digital realm, have played a leading role in the development of interconnectivity projects across the region. Yet, they must contend with the presence of Chinese and European competitors. For historical reasons, these European entities enjoy privileged positions within the telecommunications sectors of the region's countries, which have long been dominated by national state operators. In the Middle East, as well as in North Africa, the granting of licences remains closely linked to sovereignty considerations

and the variable geometry of diplomatic relations.

Second, historic partnerships with Europe have decisively contributed to shaping the network infrastructures of the region according to North-South dynamics. As a result, the velocity and data volume of Internet connections remain constrained by the geography of submarine cables and the limited numbers of local IXPs (Internet Exchange Points),<sup>8</sup> data centres and Content Delivery Networks (CDNs) in the MENA region. Most of the Internet traffic in the MENA region still transits through international (mainly European) routes. Despite this, the Mediterranean has become the principal hub for submarine cables linking Asia, Africa, and Europe (with more than 18 submarine cables transiting through the basin), with the Suez Canal acting as the main chokepoint connecting the Gulf region, which is a primary landing point for Asian undersea cables (Aluf, 2023; Tele-Geography, 2023). Egypt thus aims to capitalise on its geostrategic position to become a “data centre hub” and attract leading players in cloud computing and data storage.

If for the moment, Egypt and Israel remain the most secure options for connecting digital infrastructure linking Asia, Africa and Europe, the development of alternative corridors through Jordan, Iraq, Syria and Lebanon could help circumvent the Suez Canal bottleneck. At the Western edge of the basin, Morocco, owing to its geographical proximity to the Strait of Gibraltar – a critical passageway for undersea cables towards the Atlantic – also offers privileged access to the West African market. The new Atlantic strategy’ (Rmiche & Oukerzaz, 2023) announced by King Mohammed VI

Egypt and Israel remain the most secure options for connecting digital infrastructure linking Asia, Africa and Europe, the development of alternative corridors through Jordan, Iraq, Syria and Lebanon could help circumvent the Suez Canal bottleneck.

in November 2023 positions Morocco effectively as a digital infrastructure “hub” between West African countries (Mauritania, Senegal) and Europe. Understandably, telecommunications operators from the Gulf, the US, Europe or China all have vested interests in the stabilisation of the MENA region.

### **The MENA region’s “digital paradox”**

These developments have led to a “digital paradox” (Cusolito et al., 2021), with Internet speed and data volume limitations still hampering the development of the digitalisation of numerous economic sectors while prospects of economic growth linked to economic digitalisation are considerable. The World Bank estimated in 2021 that MENA countries’ “GDP per capita could rise by more than 40 percent, manufacturing revenues per unit of factors of production could rise by 37 percent, employment in manufacturing could rise by 7 percent, and tourist arrivals could rise by 70 percent, creating jobs in the hospitality sector. Long-term unemployment rates could fall to negligible levels, and female labor force participation could double to more than 40 percent” (Cusolito et al., 2021).

Well-developed in Gulf countries and Israel, applications for governmental services, digital payment systems, and FinTech<sup>9</sup> are still in their early stages in most of the MENA region. These sectors often lack

public trust, and the development of e-commerce, e-banking services, and FinTech requires both adapted legal frameworks and appropriate infrastructure. The digitalisation of an increasing number of societal sectors presents heightened challenges concerning data processing, management, storage, and deployment, which raises concerns about data privacy protection and online user security. At the moment, as underlined by a recent GSMA report, “the position in most of the Middle East North Africa (MENA) jurisdictions is that the privacy of an individual and the safeguarding of their personal data are provided under general provisions of law rather than specifically focused on the issue of ‘data privacy’ or ‘data protection’.”<sup>10</sup> However, most MENA countries’ governments have recognised the need to develop specific regulations to protect their data sovereignty (both from an institutional and an individual perspective), all the more that data storage related operations are usually handled by data centres and CDNs operated by foreign actors.

Moreover, low public confidence in e-services (public services, economy, finance, etc.) may also be correlated with the level of online security provided by national websites, as reflected by the number of secure Internet servers in various MENA countries (publicly-trusted TLS/SSL<sup>11</sup> certificates). Unsurprisingly, Israel exhibits a significant number of publicly-trusted TLS/SSL certificates (about 113,000), far surpassing Morocco (over 16,000) and the UAE

(almost 14,000), followed by Libya, Tunisia, and Egypt (between 4,000 and 5,000) (World Bank, 2023). These figures reveal the potentialities and limitations of the MENA countries' digital ecosystems. After Israel, the UAE, Tunisia and Morocco have the highest number of scientists (over 1,000 individuals per million people) engaged in R&D projects. This underscores the significance of well-established universities and research centres, benefiting from multinational collaborations for advancing the dissemination of digital technology but also for enabling countries to upgrade their industrial production.

Furthermore, it emphasises the necessity for MENA countries aspiring to lead regional digital transformation to consistently invest in their education systems. While the number of technicians and scientists (per million people) has more than doubled or tripled in countries such as Egypt, Jordan and the Palestinian Territories compared to Tunisia and Morocco, this disparity suggests that more selective educational programmes aimed at excellence, rather than mass average skills, might be more effective laying the grounds for dynamic digital ecosystems. Foreign partnerships would also play a critical role in ensuring the access and the socialisation with critical and up-to-date technologies – knowledge and hardware. However, as demonstrated by the recent rapprochement between the UAE's leading AI company G42, Microsoft, and other major US technology and AI

firms, access to critical technological expertise and hardware requires certain geopolitical alignments. G42's Chief Executive highlighted in December 2023 that having to severe relations with Chinese partners such as ByteDance or Huawei meant that: "[we] cannot work with both sides" (Cornish & Wiggins, 2024).

The effects of cooperation, synergy, differentiation, or rivalry related to digital sovereignty will thus increasingly contribute to redraw the fault lines of the MENA regional security complex. Faced with Sino-American competition, European major technological players have a vested interest in positioning themselves as a middle option, enabling regional governments to successfully carry out their digital transformations while taking the time to strengthen their digital ecosystems. In this context, leading European actors in the digital technology domain stand to benefit from developing partnership frameworks and strategies with Gulf actors, whether through public-private partnerships<sup>12</sup> or investment consortia<sup>13</sup> similar to those already established in the energy sector.

## Conclusion

Digital transformations initiated by MENA countries have contributed to modifying the conventional understanding of the sovereignty concept. First of all, digital transformations underline statecraft limitations and question the distribution of power pre-

Foreign partnerships would also play a critical role in ensuring the access and the socialisation with critical and up-to-date technologies – knowledge and hardware.

rogatives between state and non-state actors. The larger dissemination of digital technologies across MENA societies suggests an empowerment of actors at the more local level, considering that digital tools could be a means to both address state shortfalls and enhance societal resilience from the grassroots/community level. In a region torn by protracted conflicts, digital technologies have proved key in ensuring the survival of vulnerable communities and enabling bottom-up post-conflict reconstruction processes.

More importantly, social networks have demonstrated their critical role in enabling the creation of local aid networks, especially for refugees, internally displaced persons, and other vulnerable communities. The ongoing conflicts in Gaza and South Lebanon testify for the role of social networks in conveying live information that protect people in conflict zones, while facilitating communications and relationships with diasporas and supporting groups abroad – financial transfers or humanitarian aid collect, for instance. If digital technologies multiply the effects of informational operations and disinformation campaigns, they can also critically enhance community cohesion and resilience, especially under challenging circumstances.

Finally, as the concept of “digital sovereignty” has gained traction across the MENA region, not only among government elites and national security communities, but also among public opinions, European institutions and member states should explore avenues to defuse misunderstandings about a European “digital agenda” towards the region. With that respect, European legal concerns regarding citizens’ data protection are sometimes regarded as additional ways to impose requirements on governance issues. Interestingly, digital sovereignty is often perceived in the MENA region as a form of resistance against Western attempts – with the US often at the forefront – at subjugating countries through the development of technological dependencies. In that respect, MENA countries and EU member states seem to share similar concerns regarding exposure to technological dependencies. These issues could lay the ground for a constructive dialogue with some MENA countries regarding the establishment of common norms and standards. Through initiatives such as the Global Gateway, and with the support of Gulf partners, European institutions can promote infrastructure, R&D and digital literacy projects aimed at fostering MENA countries’ sovereignty, autonomy, and independence in the digital technology realm.

Through initiatives such as the Global Gateway, and with the support of Gulf partners, European institutions can promote infrastructure, R&D and digital literacy projects aimed at fostering MENA countries’ sovereignty, autonomy, and independence in the digital technology realm.

## Bibliography

ABRAHAM, Y. (2024, April 3). 'Lavender': The AI machine directing Israel's bombing spree in Gaza. *+972 Magazine*. <https://www.972mag.com/lavender-ai-israeli-army-gaza/>

AIRBUS DEFENCE AND SPACE. (2020). *Mapping extremist communities: A social network analysis approach*. NATO Strategic Communications Centre of Excellence. <https://stratcomcoe.org/publications/mapping-extremist-communities-a-social-network-analysis-approach/63>

ALUF, D. (2023). *China's subsea cable power play in the Middle East and North Africa*. Atlantic Council. [https://www.atlanticcouncil.org/wp-content/uploads/2023/05/ChinasGrowingInfluence\\_052423-1.pdf](https://www.atlanticcouncil.org/wp-content/uploads/2023/05/ChinasGrowingInfluence_052423-1.pdf)

AMERICAN CHAMBER OF COMMERCE IN EGYPT. (2021). *Harnessing digital Egypt*. <https://www.amcham.org.eg/publications/industry-insight/issue/41/harnessing-digital-egypt>

BROWN, C., & NEFF, W. (2024, April 16). What to know about Shahed-136 drones, which Iran used to attack Israel. *The Washington Post*. <https://www.washingtonpost.com/world/2024/04/16/iran-israel-drone-attack-shahed-136/>

CALABRESE, J. (2024, June). How the "new" Eastern Mediterranean can serve as a bridge between the Gulf and Europe. *Manara Magazine*. <https://manaramagazine.org/2024/06/how-the-new-eastern-mediterranean-can-serve-as-a-bridge-between-the-gulf-and-europe/>

CAMARATE, J., STANLEY, M., KHADIGE, A., & KEATING, P. (2022). *Fintech in the Middle East: Building on the momentum*. Strategy & PwC. <https://www.strategyand.pwc.com/m1/en/strategic-foresight/sector-strategies/financial-services/fintech-in-the-middle-east/fintech-middle-east.pdf>

CLEWLOW, A. (2024). *Surge in ransomware, leaks and info stealers targeting the Middle East and Africa*. Intelligent CIO. <https://www.intelligentcio.com/me/2024/02/29/surge-in-ransomware-leaks-and-info-stealers-targeting-middle-east-and-africa/>

CORNISH, C. & WIGGINS, K. (2024, February). Abu Dhabi AI group G42 sells its China stakes to appease US. *Financial Times*. <https://www.ft.com/content/82473ec4-fa7a-43f2-897c-ceb9b10ffd7a>

CUPLER, S. (2022). *Internet shutdowns to prevent cheating during exams: The impact on society and economy in the MENA region*. SMEX. <https://smex.org/internet-shutdowns-to-prevent-cheating-during-exams-the-impact-on-society-and-economy-in-the-mena-region/>



CUSOLITO, A. P., GÉVAUDAN, C., LEDERMAN, D., & WOOD, C. A. (2021). *The upside of digital for the Middle East and North Africa: How digital technology adoption can accelerate growth and create jobs*. International Bank for Reconstruction and Development & World Bank. <https://openknowledge.worldbank.org/server/api/core/bitstreams/a0c31a05-b4cf-5d78-8308-c2e5aaa1444a/content>

DAGHER, L., & DORANDEU, G. (2024, March 8). Israeli Tinder profiles in Beirut: Just a swipe away or GPS spoofing? *L'Orient Today*. <https://today.lorientlejour.com/article/1370788/israeli-tinder-profiles-in-beirut-just-a-swipe-away-or-gps-spoofing.html>

EL DOH, M. (2024). *Iran's UAV diplomacy resonating in conflicts in MENA and beyond*. Geopolitical Monitor. <https://www.geopoliticalmonitor.com/irans-uav-diplomacy-resonating-in-conflicts-in-mena-and/>

FERNÁNDEZ, E. (2023, June). Morocco and Israel certify the creation of an AI innovation center. *Atalayar*. <https://www.atalayar.com/en/articulo/new-technologies-innovation/morocco-and-israel-certify-the-creation-of-an-ai-innovation-centre/20230525124444185364.html>

FORTINET. (n.d.). *What is DDoS attack?* <https://www.fortinet.com/resources/cyber-glossary/ddos-attack>

FUNK, A. (2023). *Advances in AI are compounding internet freedom's decline. But they don't have to*. Freedom House. <https://freedomhouse.org/article/advances-ai-are-compounding-internet-freedoms-decline-they-dont-have>

GELVANOVSKA, N., ROGY, M., & ROSSOTTO, C. M. (2014). *Broadband networks in the Middle East and North Africa: Accelerating high-speed internet access*. World Bank. [https://www.worldbank.org/content/dam/Worldbank/document/MNA/Broadband\\_report/Broadband\\_MENA\\_annexes.pdf](https://www.worldbank.org/content/dam/Worldbank/document/MNA/Broadband_report/Broadband_MENA_annexes.pdf)

GSMA. (2019). *Data privacy frameworks in MENA: Emerging approaches and common principles* (p. 5). <https://www.gsma.com/mena/wp-content/uploads/2019/06/GSMA-Data-Privacy-in-MENA-Full-Report.pdf>

HERBERT, M., & GHOULIDI, A. (2019). *Social media bridges North Africa's divides to facilitate migration*. Institute for Security Studies (ISS). [https://issafrica.org/iss-today/social-media-bridges-north-africas-divides-to-facilitate-migration?utm\\_source=BenchmarkEmail&utm\\_campaign=ISS\\_Today&utm\\_medium=email](https://issafrica.org/iss-today/social-media-bridges-north-africas-divides-to-facilitate-migration?utm_source=BenchmarkEmail&utm_campaign=ISS_Today&utm_medium=email)

IISS. (2018). *Cyber Power Report* (pp. 115-116). <https://www.iiss.org/global-assets/media-library--content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---iran.pdf>

JERVIS, V., MILLER, T., CHAN, Y. S., KAUR, A., & SCHOENTGEN, A. (2022). *Roadmaps for awarding 5G spectrum in the MENA region*. GSMA.

[https://www.gsma.com/connectivity-for-good/spectrum/wp-content/uploads/2022/01/spec\\_mena\\_5g\\_report\\_01\\_22-1.pdf](https://www.gsma.com/connectivity-for-good/spectrum/wp-content/uploads/2022/01/spec_mena_5g_report_01_22-1.pdf)

KENDE, M. (2020). *Middle East & North Africa internet infrastructure*. Internet Society. [https://www.internetsociety.org/wp-content/uploads/2020/09/Middle\\_East\\_North\\_Africa\\_Internet\\_Infrastructure\\_2020-EN.pdf](https://www.internetsociety.org/wp-content/uploads/2020/09/Middle_East_North_Africa_Internet_Infrastructure_2020-EN.pdf)

KUMAR, P. (2024). *Masdar to invest \$900m in solar projects in Egypt*. AGBI. <https://www.agbi.com/renewable-energy/2024/09/masdar-to-invest-900m-in-solar-projects-in-egypt/>

LEAGUE OF ARAB STATES. (2020). *Arab vision for digital economy: Towards a sustainable, inclusive and secure digital future* (2nd ed.). <https://www.arab-digital-economy.org/2020/17.pdf>

LEVESQUE, E. (2024). *African renewables are ripe for investment, says Irena*. AGBI. <https://www.agbi.com/renewable-energy/2024/04/african-renewables-are-ripe-for-investment-says-irena/>

MADIEGA, T. (2020). *Digital sovereignty for Europe* (EPRS Ideas Paper, p. 2). European Parliamentary Research Service. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

MIDBON, M. (1991, October). Who made Israel's computer models for the 1967 war? *Computers & Society*, 21(2-4). <https://dl.acm.org/doi/pdf/10.1145/122652.122656>

NATO. (2024). *NATO's approach to space*. [https://www.nato.int/cps/en/natohq/topics\\_175419.htm](https://www.nato.int/cps/en/natohq/topics_175419.htm)

NOMAN, H. (2019). *Internet censorship and the intraregional geopolitical conflicts in the Middle East and North Africa*. Berkman Klein Center for Internet & Society. <http://dx.doi.org/10.2139/ssrn.3315708>

REGENBAUM, A. (2023, March 29). *Israel, the innovation system*. Mind The Bridge. <https://mindthebridge.com/israel-the-innovation-nation/>

RMICHE, A., & OUKERZAZ, H. (2023, November 7). *Façade atlantique de l'Afrique: Le Maroc pour l'émergence d'un nouvel espace de croissance, de paix et de prospérité*. *Le Matin*. <https://lematin.ma/nation/facade-atlantique-de-lafrique-les-ambitions-du-maroc/199481>

ROSSON, Z., ANTHONIO, F., & TACKETT, C. (2023). *Weapons of control, shields of impunity: Internet shutdowns in 2022*. KeptOn Report. <https://www.access-now.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf>

SAEED, S., ALTAMIMI, S. A., ALKAYYAL, N. A., ALSHEHRI, E., & ALABBAD, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*, 23(15). <https://doi.org/10.3390/s23156666>

SENIOR, D., & SINGER, S. (2011). *Start-up nation: The story of Israel's economic miracle*. Grand Central Publishing.

SHAHBAZ, A. (2018). *The rise of digital authoritarianism - Freedom on the Net 2018*. Freedom House. <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism>

SHIM, S. & OH, J. (2024). *Dark Web Cyber-attacks targeting MENA region – Region Analysis-January*. Medium. <https://medium.com/s2wblog/region-analysis-january-dark-web-cyber-attacks-targeting-mena-region-english-ver-d9bb2e725395#:~:text=Data%20leaks%20from%20%27Government%2FMilitary,%25%20of%20all%20leaks%2C%20respectively.>

STATISTA. (2024). *Internet usage in MENA - statistics & facts*. <https://www.statista.com/topics/5550/internet-usage-in-mena/#topicOverview>

TELEGEOGRAPHY. (2023). *Submarine Cable Map*. <https://www.submarinecable-map.com/ready-for-service/2023>

UN GLOBAL PULSE. (2019). *E-analytics guide: Using data and new technology for peacemaking, preventive diplomacy, and peacebuilding*. Reliefweb. <https://reliefweb.int/report/world/e-analytics-guide-using-data-and-new-technology-peacemaking-preventive-diplomacy-and>

WITT, S. (2022, May). The Turkish drone that changed the nature of warfare. *The New Yorker*. <https://www.newyorker.com/magazine/2022/05/16/the-turkish-drone-that-changed-the-nature-of-warfare>

WORLD BANK. (2020). *Secure Internet servers - Middle East & North Africa*. [https://data.worldbank.org/indicator/IT.NET.SECR?locations=ZQ&most\\_recent\\_year\\_desc=false](https://data.worldbank.org/indicator/IT.NET.SECR?locations=ZQ&most_recent_year_desc=false)

WORLD BANK. (2023). *Fixed broadband subscriptions (per 100 people) - Middle East & North Africa*. [https://data.worldbank.org/indicator/IT.NET.BBND.P2?locations=ZQ&name\\_desc=false](https://data.worldbank.org/indicator/IT.NET.BBND.P2?locations=ZQ&name_desc=false)

YASSIN, F. E., & EL NAHLAWY, H. (2023). *Driving digital transformation in the Arab region*. UNDP. <https://www.undp.org/arab-states/stories/driving-digital-transformation-arab-region>

ZWITTER, A. (2014). Big data ethics. *Big Data & Society*, 1(2). <https://doi.org/10.1177/2053951714559253>



# **Disentangling the MENA Countries' Involvement in Cyber Sovereignty Debates**

**Julien NOCETTI**

Senior Associate Fellow at Institut français  
des relations internationales (IFRI)

## Introduction

The Middle Eastern and North African (MENA) region is not immune to the global policy- and economic-related issues and tensions affecting the digital economy and cybersecurity landscapes. The Sino-American commercial and technological disputes on all-things tied to the Internet and emerging technologies (artificial intelligence [AI], telecommunications standards, microchips, etc.), intricately with the COVID-19 pandemic and then the full-scale Russian invasion of Ukraine, have impacted global tech ecosystems, most notably supply chains, including in the different sub-areas framed under the MENA acronym (Maghreb, Levant, Gulf).

Digital sovereignty concerns now innervate most of these debates which closely tie domestic, regional, and global levels. This is the case with MENA states but seemingly with contradictions for observers seeking to disentangle the substance of their discourse and policy initiatives.

A first one touches the discrepancy of digital sovereignty-related debates between the MENA and other regions, starting with the European Union (EU), where these have become widespread for over a decade (Broeders et al., 2022). In a certain way, the MENA region appears as a “blind spot” on the global map of digital sovereignty debates. Global narratives tend to focus on the Sino-US competitive framework – with the EU as a counterpoint (Broeders et al., 2022; Nocetti, 2023; Velliet, 2023) – and on the Global South. In the latest case, Sub-Saharan Africa seems to attract a significant part of policy-related analysis and media coverage (Soulé, 2024; Venske, 2023).

This blind spot might be tied to scattered, fragmented domestic debates on these issues. The digital sovereignty

challenge even rarely appears in public discourse: in recent years, only Morocco, Algeria and Jordan have publicly stressed concern over strengthening their own “digital sovereignty”. In the case of Morocco, this is illustrated through a cybersecurity lens as well as the need to develop sufficient and skilled human resources in the broader digital field (As-sahifa, 2024). National academia have recently emphasised the topic – such as the Moroccan think tank Institute of Strategic Intelligence, which published a policy paper seeking to identify the main areas in which the country may assert digital sovereignty, though failing to mention any external relations-related dimension to this effort (Mouad Agouzoul, 2024). For its part, Algeria ties digital sovereignty to its national digital transition strategy drafted by the country’s president (Algeria Press Service, 2024). Finally, in a June 2023 public statement, Jordan representatives framed digital sovereignty around a collective “Arab quest” for strengthening an issue broadly conceived of as a potential societal risk (The Jordan Times, 2023).

In MENA countries, overall, the discrepancy mentioned above is tied to a gap between discursive policy and policy-making. Official narratives may well emphasise need for digital sovereignty, but this rhetoric does not prevent regional governments from continuing to seize the dividends of global tech interdependencies. In times of contested multilateralism and regime shifting, MENA governments’ policies consist of navigating this paradox.

Closely tied to digital sovereignty concerns, digital – and data – “colonialism” has permeated global debates, illustrating an analytical shifting centre of gravity from a state-centric perspective to taking into account the influence exerted by

major technological companies (Mejias & Couldry, 2024). As such, digital colonialism would refer to a modern-day “scramble for Africa” where large-scale tech companies extract, analyse, and own user data for profit and market influence (Coleman, 2019). Here again, the MENA region does not appear to feature high among analysts – with the notable exception of linking “colonialism” to specific telecommunications infrastructure such as submarine cables, so as to highlight the growing trend of digital surveillance by most of the region’s governments (Felsberger, 2020).

Algorithmic surveillance, propaganda, and digital repression indeed remain major trends across the region – trends which largely determine the outside world’s vision of the “digital MENA” and which far outperform the digital sovereignty stake (Jones, 2022). Over the past decade, governments of the MENA region have employed digital information and communication technologies as a tool to reinforce control over their citizens. This digital authoritarianism aspect, although a matter itself deserving a dedicated study, has actually become an external relations challenge, as model projection through and about the digital field is now blended with ideology and geopolitics.

Security considerations thus significantly inform MENA states’ role and initiatives in the global conversation on digital sovereignty-related matters. The objective of this contribution is precisely to shed light on the interrelations between the domestic and international stances of MENA countries regarding digital sovereignty. “Digital sovereignty” will be comprehended in a holistic way, with the purpose of “translating” the positioning of these governments into international/multilateral cyberspace

governance fora which seek to advance norms.

A first section will examine how digital sovereignty has become a foreign relations’ matter, triggering debates among like-minded states at times leading to formal or informal alliances.

A second section will specifically focus on MENA countries’ stances and approaches. Despite their many differences, MENA states have similarities regarding Internet/cyber governance. On the one hand, they cooperate with the Russia-China bloc in international governance platforms; on the other, many of them cooperate with the West in terms of cyber operations and intelligence-sharing relations. These states have developed deliberately ambiguous national cybersecurity strategies that disguise differences between domestic cybersecurity priorities and those of their international partners. Additionally, these states have appropriated international norms on cybercrime, specifically the Council of Europe’s Budapest Convention of 2001, in order to counter political opposition and restrict their online public spheres through new cybercrime legislation.

Finally, building from a geopolitical perspective on these issues, we suggest to highlight the opportunities for the EU diplomacy in building, reinforcing, or (re)adapting ties with MENA countries on digital sovereignty. In a twofold rising Sino-American competition and resurgence of the Russian threat contexts, some MENA countries like Egypt or Algeria might be tempted to choose one side against another. Rising anti-Western sentiments, an aggressive Russian behaviour, and the dissemination of Chinese technologies (in particular surveillance software and telecommunications equipment) form a complex equation for countries in the region.

## Digital sovereignty as a foreign policy issue

### Digital sovereignty in the diplomatic “value chain”

Digital sovereignty has become one of key friction points in geopolitical relations. This characteristic has been clearly reinforced during the COVID-19 pandemic crisis and through its multiple consequences (Chander & Sun 2023). Two of these are particularly noteworthy.

The first is the rise of the geo-economic factor in international relations, which goes beyond the digital economy to encompass the “weaponisation” of key economic interdependencies (Pfeiffer, 2023). In other words, the vectors of globalisation (financial and technological flows, exports of agricultural and energy raw materials, as well as information networks) are used as weapons (Farrell & Newman, 2023). According to this approach, coercive economic measures – such as sanctions – are no longer a substitute for war, but an extension of it.

The aim is to drain the resources that an enemy can mobilise for combat, and thus to increase the burden of war from the economic dimension (Galeotti, 2022). The aim is also to weaken the morale of the enemy population, so as to undermine their fighting spirit and support for the government. In this context, digital sovereignty can be a political and industrial response to a situation of externally imposed constraint, with a view to “self-sufficiency” (a term used by the Chinese authorities since 2015) or “import substitution” (a term used by Russia since 2014).

The second implication concerns the interactions between systemic digital platforms and states. It is the former that, during the COVID-19 crisis, ensured connections between countries, individuals and organisations. They shape political and social relations, and are now at the heart of power plays. Cooperation, competition and confrontation between China and the US are all played out through them. The challenge of regulating GAFAMs<sup>14</sup> is increasingly perceived – particularly in Europe – as one of imposing a digital sovereignty that the continent has long lacked. It is therefore becoming a classic international relations issue, regularly liable to spark controversy and strain relations between allies (EU-US, for example). Since 2019, the EU has made digital regulation one of the geopolitical axes of the EU Commission. The EU’s many initiatives in this area are now part of a drive to defend Europe’s “digital sovereignty” in the face of the predatory technological and innovation strategies of American and Chinese ecosystems.

### Digital sovereignty: competing models

Digital sovereignty is not merely a domestic policy issue; it also concerns the projection of a vision and a model on the global stage. In this respect, some of the recent debates have focused on the opposition of values between the approach defended by liberal democracies and that projected by authoritarian states (Pearson, 2024). More precisely, the dividing line is articulated on two levels. The first concerns the degree of openness of digital ecosystems to global interdependencies – or, at least, the ability of states to master their critical dependencies. Authoritarian regimes such as China, Russia and Iran have, since the late

Digital sovereignty is not merely a domestic policy issue; it also concerns the projection of a vision and a model on the global stage.



1990s and to varying degrees, been seeking to free themselves from their dependence on American technologies, perceived as a means of intrusion or even subversion.

The second has to do with differences of opinion about what digital sovereignty actually means. The Internet, which defies the control of any form of authority, is not universally perceived throughout the world as a means of promoting the emancipation of peoples. This approach concerns the cognitive layer of the Internet. Distinct from the European conception, digital sovereignty as envisaged by authoritarian regimes such as Russia and China thus places the emphasis on preserving “national” informational space from foreign influences perceived as subversive – while following international trends observed over the last decade (re-localisation of data, greater importance given to digital infrastructures, etc.). This Sino-Russian approach is also distinguished by its unabashed use of the law, which is mobilised in all directions to strengthen the primacy of politics in the digital domain and maintain the stability – if not the survival – of regimes. In these two countries, the “securitisation” of the national digital space has manifested itself in the use of the rhetoric of existential threat to justify actions and provisions that are more restrictive of freedom of expression and assembly. Once again, hostility to US policy – promoting the free flow of information, the central role of the private sector, etc. – structures the political line of these countries.

This form of digital authoritarianism – incorporating a specific conception of sovereignty – is projected exponentially into international debates. On the one hand, a state like Russia has been projecting the notion of information “sovereignty” or “security” in international forums, particularly the United Nations (UN), since 1998, seeking to rally already American-sceptical countries to its own position (Nocetti,

2015). A dividing line in debates on global Internet governance, “sovereignty” is also exploited by the same states for foreign policy purposes. For example, before it was banned in the EU in March 2022, the Russian state channel RT broadcast programmes and articles in France pointing out the “absence” of digital sovereignty in Europe, with the various spying scandals involving its allies as a counterpoint to the already polarised debates about the US.

Over and above this dichotomy linked to the nature of regimes, the European approach is distinguished by a complex nuance and a political line that is now its own. The absence of leading European digital players has led the EU to defend a specific model of digital society based on values (protection of personal data, fair competition, adequate taxation, etc.), the defensive dimension of which is sometimes perceived as a form of anti-Americanism. In February 2021, Charles Michel, President of the EU Council, declared that there is “no strategic autonomy without digital sovereignty,” officially placing the concept of “strategic autonomy” at the heart of debates, which denotes a security or even military connotation – here applied to digital policy and data infrastructures. The cursor placed on the ambition of “autonomy” suggests a geopolitical reading that should enable the EU to compete with the two digital superpowers, China and the US, while protecting its own vital interests. However, not all member states support the development of European strategic autonomy, with disagreement on what entails, or on the level of geographic and functional ambition they should adopt to implement it. The attitude to be adopted towards the US is at the heart of discussions on European strategic autonomy and is one of the points of tension regarding the risks it could pose for transatlantic relations, particularly in the area of defence (Danet & Desforges, 2020).

## In the international arena, MENA states closely articulate digital sovereignty with cybersecurity

In official EU documents, cyber is identified as a “key enabler” for European digital sovereignty. In most of the MENA countries, the articulation between digital sovereignty and cybersecurity is a tight one, as digital sovereignty mostly remains conceived as a range of policy instruments enabling a “securitised” digital environment. This approach translates into a cyber diplomacy that seeks to provide MENA governments with an additional platform to exert influence on the international scene. This external relations dimension to digital sovereignty debates and challenges does raise questions about political alliances in the region, with “Arab” cybersecurity initiatives juxtaposed against cybersecurity relationships across former geopolitical divides, such as the 2020 Abraham Accords.

### A greater MENA involvement in international debates?

First of all, MENA states contribute to all the global cybersecurity diplomacy processes. The current cybersecurity process in the UN First Committee, an Open-Ended Working Group (OEWG) led by Singapore, is under pressure to deliver tangible results in a tight timeline after previous iterations merely maintained momentum. The OEWG is supposed to transition to a Programme of Action in 2025, although the latter’s mandate and scope remain unclear. These processes may be superseded by a Global Digital Compact, scheduled for unveiling at the UN Summit for the Future at the end of 2024, which addresses many of the same issues in addition to AI and other

emerging technologies. At the same time, in the UN Third Committee, an Ad Hoc Committee (AHC) to agree a global cybercrime convention appears to be imploding, with long-running divisions between democratic and open approaches to Internet governance and more authoritarian stances – present in all these venues – showing no sign of alleviating sufficiently to reach agreement.

In these diplomatic games, if Iran and Syria have traditionally been key proponents of more state-centred, authoritarian perspectives, along with Russia and China, two other blocs can be distinguished. On the one hand, Egypt occupies a split role, a long-standing champion for less developed states across Africa – and not only the Arab world –, and a familiar interlocutor for European and American diplomats, but with a growing closeness to the authoritarian approaches above.

On the other hand, the Gulf States advocate for restrictive cybercrime measures while also looking to leverage their financial power to shape more inclusive conversations. For example, the UN Internet Governance Forum (IGF), the preeminent multi-stakeholder Internet governance meeting since 2005, will convene in Riyadh in December 2024. The nomination of Saudi Arabia as the IGF’s latest rotating location was highly controversial, with 88 civil society organizations (CSOs) worldwide signing a joint letter to the UN Secretary General calling on him to reverse this decision due to Saudi Arabia’s history of human rights violations and Internet censorship (Access Now, 2023).

Beyond the UN General Assembly, and IGF venues, MENA states particularly engage in the International Telecommunications Union (ITU). The ITU operates a Global Cybersecurity Index (GCI) which ranks all states’ cybersecurity capacity, based on

This external relations dimension to digital sovereignty debates and challenges does raise questions about political alliances in the region.

answers to a 30-page questionnaire submitted by relevant government agencies. The fourth GCI was published in 2020, with the next version due in September this year. In the 2020 edition, Saudi Arabia came joint-second worldwide, with the United Arab Emirates (UAE) joint-fifth. In the MENA region, Oman, Egypt and Qatar also scored higher than 90 points out of 100. The GCI is relevant not because of the robustness of its results – indeed, the questionnaire allows room for countries to maximise policy commitments rather than practical action – but because it is a highly visible and simple way to compare neighbours. Many cybersecurity agencies in the Middle East, especially in the Gulf, have included improvement in the GCI index as a key performance indicator, meaning that these states are much more oriented towards the ITU as a cybersecurity locus than they are towards other UN processes.

In contrast, MENA states have been far less prevalent in global multistakeholder cybersecurity initiatives over the past few years. Only six MENA states signed the Paris Call for Trust and Security in Cyberspace, launched by the Paris Peace Forum in November 2018 (UAE, Kuwait, Lebanon, Morocco, Qatar and Tunisia). The 2024 United Kingdom (UK)-France Pall Mall Process on commercial cyber intrusion capabilities had the Gulf Coordination Council in attendance as an organisation, with Saudi Arabia and the UAE individually also reportedly supportive, despite their extensively-reported reliance on such capabilities for surveillance and repression.<sup>15</sup> This relative lack of MENA presence is due partly to the low priority such initiatives receive in a government-dominated policy landscape, as well as discomfort within those initiatives in welcoming authoritarian states (like the IGF above). Where multi-

stakeholder cybersecurity collaboration is less politicised, some MENA states do contribute. Egypt, Jordan, the UAE and Israel all participate in the US-pushed International Counter Ransomware Initiative (CRI), with the UAE and Israel jointly contributing to an information sharing platform developed with Microsoft to the CRI (Israel Defense, 2023).

Overall, MENA states are starting to contribute more centrally to global cybersecurity diplomacy, led by Saudi Arabia and the UAE. This does not, however, mean that cybersecurity diplomatic processes themselves will run more smoothly, given the balancing act these states strike between Western security alliances and authoritarian Internet instincts (Shires, 2022). The ability of especially these two states to host – and financially support – major international conferences means that they are likely to be a regular presence in the cybersecurity diplomatic scene in the near future, and projecting their own approach to sovereignty-related issues around all-things digital.

### **When global debates intertwine with regional venues: the UN Economic and Social Commission for Western Asia**

The multilateral organisations above (ITU, IGF, etc.) have regional ramifications focusing on the MENA region, which have also developed substantial cybersecurity activities over the past decade. The Arab IGF has waxed and waned since its creation in 2012, with the most recent in Lebanon in 2021 as part of a broader Digital Cooperation and Development Forum, hosted by the UN Economic and Social Commission for Western Asia (ESCWA), based in

Beirut. ESCWA has long sought to improve cybersecurity awareness and governance among Middle East governments, publishing a “regional roadmap” for Internet governance in 2010 that was soon overtaken by the Arab Spring events. However, cybersecurity – as an issue closely connected to national sovereignty and international security – is technically outside ESCWA’s remit, meaning that many events, such as a September 2023 workshop on “building trust in digital public services” must tackle cybersecurity issues in all but name (UN ESCWA, 2023).

ESCWA’s main partners in this workshop, the Arab Information and Communication Technologies Organization, based in Tunisia, and the Arab chapters of the Internet Society, a global multistakeholder organisation, have each developed their own regional initiatives. In March 2020, the Internet Society released guidelines for securing Internet infrastructure addressed specifically to Arab states, seeking to build support for its technical measures for routing security – although no direct link to “sovereignty” is being made (Internet Society, 2020). In January 2024, the ICT Ministers’ Council of the Arab League approved an Arab Cybersecurity Strategy following the publication of similar national strategies in the region (and, in some cases, multiple iterations) (AICTO, 2024). A separate Arab League Council of Ministers for cybersecurity was established in September 2023, championed by Saudi Arabia, meaning that over the coming years the usually lethargic League may devote greater attention and resources to the issue (Noureldin, 2023).

ESCWA also partnered with the ITU for its 2023 workshop, which has a far more extensive history of developing regional cybersecurity efforts. The ITU established an Arab Region Cybersecurity Centre (ARCC) in Oman in 2013, which has conducted many joint cyber drills with other countries and holds an annual regional cy-

bersecurity conference, as well as leading the way in cybersecurity awareness campaigns that have now been taken up by other states, such as the UAE. The ARCC both benefits and suffers from its location in Oman. While lacking the financial resources of its richer neighbours, the ARCC is nonetheless able to establish connections between technical practitioners in more diplomatically difficult states, such as Iran, and via broader networks such as the Organization of Islamic Cooperation and a global network of computer incident response teams, FIRST (which includes nearly all MENA states as members, and regularly offers training in the region).

More recently, Saudi Arabia has launched several other initiatives that re-centre the locus of cybersecurity diplomacy towards the kingdom. In 2020, it led the creation of the Digital Cooperation Organization, an ostensibly global multilateral organisation with half its member states in the MENA region – the current presidency is held by Bahrain. Saudi Arabia’s annual Global Cybersecurity Forum (GCF), also inaugurated in 2020, has dominated the regional cybersecurity landscape and attracted businesses and politicians from outside the region, even during its Western diplomatic isolation after the killing of Jamal Khashoggi in 2018. In 2023, the GCF launched a stand-alone Institute to continue its activities outside the annual event. Added to the UAE’s annual GISEC conference and Bahrain’s Arab International Cybersecurity Summit, the calendar is full of competing events, all seeking to promote their state sponsors as the most advanced in the region. The Gulf countries all compete at a commercial level too, aiming to attract individuals with cybersecurity skills – offensive and defensive – that are in short supply worldwide.

This competition extends beyond summit diplomacy into other areas of cybersecurity

This competition extends beyond summit diplomacy into other areas of cybersecurity governance.

governance. A regional trend for centralisation of national cybersecurity policy and decision-making into a single authority or centre – each with its own international cooperation department – not only follows best practice worldwide, but also illustrates the integral role non-diplomats play in cybersecurity diplomacy. These organisations indirectly affect cybersecurity diplomacy by setting national standards, regulations and controls that are then adopted by businesses and adapted by other states. More generally, cybersecurity capacity-building – the subject of much attention at the UN OEWG – is garnering greater attention in the MENA, with states like Saudi Arabia and the UAE looking to increase regional influence by offering training, equipment and collaboration to other states in the region and beyond. Such capacity-building efforts are promising, but with several obstacles: they run not only the risks of duplication and inefficiency, but also the misuse or abuse of capabilities to increase cyber insecurity.

## **Navigating the MENA contradictions: opportunities for EU diplomacy**

Perhaps no other state as Egypt does embody the “digital sovereignty-paradox” in the MENA region. James Shires first argued that Egypt occupies a middle ground within the bipolar cybersecurity governance spectrum, exhibiting practices, laws, institutions, and technologies congruent with the cyber sovereignty model, while also maintaining close cybersecurity cooperation with states firmly within the multistakeholderism camp (Shires, 2018). The mass censorship of websites and legalisation of these information controls places Egypt squarely within the Chinese model of cyber sovereignty,

whereby the state exerts strong national control over the Internet. Yet, Egypt’s extensive links with Western liberal democracies – the reliance on American military aid, security cooperation, foreign investment, and international development aid – complicate the country’s impulse to wholly wall off its Internet à la China and Iran. The US and Egypt maintain strong cybersecurity linkages, including joint cybersecurity exercises and agreements between EG-CERT and US-CERT, and Western cybersecurity firms enjoy a significant presence in the country. Because of this cybersecurity cooperation with multistakeholderism-aligned states, Egypt’s positioning within the cyber sovereignty pole is muddled (Shires, 2018).

This further complicates EU external policies in this field, as the region illustrates the wide spectrum of policy approaches one can encounter in digital sovereignty. It is true that one cannot dissociate cybersecurity from freedom of expression and public liberties in each country of the MENA region. When pushing for stronger legal regulation of the Internet/cyberspace, policy-makers, civil society and the private sector should be very cautious to likely restriction of civil rights.

The very term “cybersecurity” can also be ambiguously and imprecisely understood in the region. This lack of consensus about what constitutes a legitimate security threat in the digital domain has helped authoritarians legitimise various strategies for achieving their political goals, such as weaponizing anti-Western sentiments, disseminating technologies – in particular Chinese surveillance software and telecommunications equipment –, and fuelling counter-responses by the US administration.

As Patryk Pawlak puts it, the EU’s maturity in cyber diplomacy has been moderate –

When pushing for stronger legal regulation of the Internet/cyberspace, policy-makers, civil society and the private sector should be very cautious to likely restriction of civil rights.

in contrast with the Union's resilience strategy which so far has effectively sought to advance maturity through internal market regulation (Pawlak, 2024). The more hostile international environment has shifted the EU's cyber diplomacy from a comprehensive approach to a more targeted one focused on diplomatic responses to malicious cyber activities and cyber capacity-building (Pawlak, 2024). This more "technical" approach by the EU could effectively be politicised as authoritarian narratives on sovereignty and security in the digital field are strengthening and seeking to gain traction across the Global South.

## Bibliography

ACCESS NOW. (2023). *Internet Governance Forum must reverse decision to make Saudi Arabia its next host* [Joint Statement]. <https://www.accessnow.org/campaign/igf-reverse-saudi-arabia-host-decision/>

AICTO (ARAB INFORMATION AND COMMUNICATIONS TECHNOLOGIES ORGANIZATION). (2024). *Arab ICT Ministers' Council approves the Arab Cybersecurity Strategy*. <http://www.aicto.org/arab-ict-ministers-council-approves-the-arab-cybersecurity-strategy-elaborated-by-aicto/>

ALGERIA PRESS SERVICE. (2024, February). *Algeria seeks to strengthen digital sovereignty through national digital transition strategy*. <https://www.aps.dz/en/health-science-technology/50936-algeria-seeks-to-strengthen-digital-sovereignty-through-national-digital-transition-strategy>

ASSAHIFA. (2024). *Cybersecurity, digital sovereignty are Morocco's core concerns, minister says*. <https://www.assahifa.com/english/morocco/cybersecurity-digital-sovereignty-are-moroccos-core-concerns-minister-says/>

BROEDERS, D., CSERNATONI, R., IRION, K., KAMINSKA, M., MONTI, G., ROBLES-CARRILLO, M., SOARE, S. R., & TIMMERS, P. (2022). *Digital sovereignty: From narrative to policy?* EU Cyber Direct. <https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy>

CHANDER, A., & SUN, H. (Eds.). (2023). *Data sovereignty: From the digital silk road to the return of the state*. Oxford University Press.

COLEMAN, D. (2019). Digital colonialism: The 21st century scrambles for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race & Law*, 24(2). <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1294&context=mjrl>

DANET, D., & DESFORGES, A. (2020). Souveraineté numérique et autonomie stratégique en Europe: Du concept aux réalités géopolitiques. *Hérodote*, 177-178, p.179-195.

FARRELL, H., & NEWMAN, A. (2023). *Underground empire: How America weaponized the world economy*. Penguin.

FELSBERGER, S. (2020). *Colonial cables: The politics of surveillance in the Middle East and North Africa* (No. 10). Austrian Institute for European and Security Policy. <https://www.aies.at/download/2020/AIES-Studies-Colonial-Cables.pdf>

GALEOTTI, M. (2022). *The weaponisation of everything: A field guide to the new way of war*. Yale University Press.

- INTERNET SOCIETY. (2020). *Internet infrastructure security guidelines for Arab states*. <https://www.internetsociety.org/resources/doc/2020/internet-infrastructure-security-guidelines-for-the-arab-states/>
- ISRAEL DEFENSE. (2023). *Israel, UAE Part of Global Anti-Ransomware Platform*. <https://www.israeldefense.co.il/en/node/58799>
- JONES, M. O. (2022). *Digital authoritarianism in the Middle East: Deception, disinformation and social media*. Hurst.
- MEJIAS, U., & COULDRY, N. (2024). *Data grab: The new colonialism of big tech and how to fight back*. The University of Chicago Press.
- MOUAD AGOUZOUL, M. (2024). *Souveraineté numérique: Pourquoi le Maroc ne peut y échapper - Recommandations pour un État-stratège*. Institut Marocain d'Intelligence Stratégique. [https://imis.ma/wp-content/uploads/2024/05/IMIS\\_Souverainete-Numerique\\_VF.pdf](https://imis.ma/wp-content/uploads/2024/05/IMIS_Souverainete-Numerique_VF.pdf)
- NOCETTI, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, 91(1), p.111-130.
- NOCETTI, J. (Ed.). (2023). *La souveraineté numérique : Dix ans de débats, et après ?* Annales des Mines. <https://www.annales.org/enjeux-numeriques/2023/en-23-09-23.pdf>
- NOURELDIN, O. (2023, September 11). Arab League forms Cybersecurity Ministerial Council to combat growing threats. *Forbes Middle East*. <https://www.forbesmiddle-east.com/innovation/cybersecurity/arab-league-establishes-council-of-arab-ministers-of-cybersecurity-to-combat-growing-threats>
- PAWLAK, P. (2024). A mature cyber power? Drivers, strategies and tools of the EU's international cyber engagement. *Etudes françaises de renseignement et de cyber*, 1(2), p.23-42.
- PEARSON, J. (2024). Defining digital authoritarianism. *Philosophy & Technology*, 37(2), p.1-19.
- PFEIFFER, C. (2023). *Geoeconomics in international relations*. Routledge.
- SHIRES, J. (2018). *Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States*. War on the Rocks. <https://warontherocks.com/2018/10/between-multistakeholderism-and-sovereignty-cyber-norms-in-egypt-and-the-gulf-states/>
- SHIRES, J. (2022). *The politics of cybersecurity in the Middle East*. Oxford University Press.
- SOULÉ, F. (2024, June). *Digital sovereignty in Africa: Moving beyond local data*



*ownership* (Policy Brief No. 185). Centre for International Governance Innovation. [https://www.cigionline.org/static/documents/PB\\_no.185.pdf](https://www.cigionline.org/static/documents/PB_no.185.pdf)

THE JORDAN TIMES. (2023, June). Shboul highlights 'quest for digital sovereignty' at 53rd Council of Arab Media Ministers. <https://jordantimes.com/news/local/shboul-highlights-%E2%80%98quest-digital-sovereignty%E2%80%99-53rd-council-arab-media-ministers>

UN ESCWA. (2023). *Building trust in digital government services*. <https://www.unescwa.org/news/building-trust-digital-government-services>

VELLIET, M. (2023). *Digital sovereignty: European policies, American dilemmas*. IFRI. <https://www.ifri.org/en/publications/notes-de-lifri/digital-sovereignty-european-policies-american-dilemmas>

VENSKE, T. (2023, October). *Navigating digital sovereignty in Africa: A review of key challenges and constraints* (The Africa Governance Papers, Vol. 1, No. 4). Good Governance Africa. [https://digitalmallblobstorage.blob.core.windows.net/wp-content/2024/03/TAGP-4\\_1\\_Research\\_Venske\\_US-China-techwar.pdf](https://digitalmallblobstorage.blob.core.windows.net/wp-content/2024/03/TAGP-4_1_Research_Venske_US-China-techwar.pdf)



# Policy Recommendations

The manifestations of enhancing digital sovereignty in the MENA region are visible, firstly in the notable disparity in digital advancement among its countries. As observed, countries like the United Arab Emirates (UAE), Saudi Arabia and Qatar appear as relevant models that have made significant strides in digital transformation. In this context, it is imperative for other countries in the region to follow suit to achieve digital convergence. This convergence could be first achieved through building and strengthening the resilience of the region's digital infrastructure, which is lagging behind in terms of development and is remaining vulnerable to cyber threats.

Historic partnerships with Europe have decisively contributed to shaping the network infrastructures of the region according to North-South dynamics. As a result, the velocity and data volume of Internet connections remain constrained by the geography of submarine cables and the limited numbers of local Internet Exchange Points (IXPs), data centres and Content Delivery Networks (CDNs) in the Middle East and North Africa (MENA) region. Most of the internet traffic in the MENA region still transit through international (mainly European) routes. Despite this, the Mediterranean has become the principal hub for submarine cables linking Asia, Africa and Europe with the Suez Canal acting as the main chokepoint connecting the Gulf region. Egypt thus aims to capitalise on its geostrategic position to become a "data centre hub" and attract leading players in cloud computing and data storage. This specific feature could well attract EU interest in terms of capacity-building, which is one of the major pillars of the Union's external policy. In turn, Morocco, also positioning itself as a digital infrastructure "hub" between West African countries (Mauritania, Senegal) and Europe, should be more actively engaged in terms of infrastructure- and expertise- providing.

Beyond industrial stakes or even geopolitical power plays, another major recommendation lies in increasing and diversifying investment in the region's education systems. Digital sovereignty and resilience are also built "from the bottom", i.e. through educating populations to the variety of challenges brought by the digital field. This specific challenge is well comprehended by the US and, increasingly, China. Faced with Sino-American competition, European major technological players have a vested interest in positioning themselves as a middle option, enabling regional governments to successfully carry out their digital transformations while taking the time to strengthen their digital ecosystems. In this context, leading European actors in the digital technology domain stand to benefit from developing partnership frameworks and strategies with Gulf actors (whether through public-private partnerships or investment consortia similar to those already established in the energy sector) and with North African counterparts, while navigating the diverse set of political tensions within and outside the region.

Digital regulation and data protection also appear as key topics about which EU institutions could build on to favour a rapprochement with MENA countries. The recent adoption of both the DSA (Digital Services Act) and the DMA (Digital Markets Act) in the EU may ideally be paving grounds for cross-sharing, constructive perspectives on both sides of the Mediterranean – with the consistent aim of improving technical standards and legislative norms in MENA countries.

Finally, as narratives become key in the world conversation about all-things technological, the EU should take time in advancing its full-fledged "digital agenda" towards the MENA region, as this can be understood as a disguised way to push

for “Northern” attempts to subjugate de- narrative which is already entering informa-  
veloping economies – a “post-colonial” tional battles on social networks and media.



# eur@mesco

Policy Study

