Forum: The Fourth General Assembly

Topic: Addressing the Impact of Digital Colonialism and Surveillance on Development and Sovereignty in the MENA Region

President

Introduction

Today, with the exponential growth of new innovations such as Big Data, Artificial Intelligence, Algorithm Development, and even improved cyber security, it is important for a country to be Digitally Dependent and be in full control of its governments and individuals' data. The world around us is developing and shifting towards a digital world. Digital colonialism in the MENA region refers to the implementation of foreign infrastructure, usually western companies or countries, looking to control data and other digital infrastructures, and therefore leading to digital colonialism, increased surveillance, and a lack of privacy. Which leads to growing the digital divide, stunting the development of underdeveloped countries, and exploiting the privacy of governments and civilians in underdeveloped regions, such as the MENA region. It is important to address this topic to ensure an equitable and safe approach for the development of the digital world, while protecting the rights of the people in the MENA region.

This issue first began in the early 2000's with western based parties such as US and European based global tech firms started to expand their digital infrastructure into the region. In the beginning, governments in the region welcomed the idea, with foreign companies such as Amazon, Google, Facebook, and Microsoft, all importing digital infrastructure such as data centers and cloud services, and telecom networks. This infrastructure was placed with very little regard to the importance of privacy and even led to these global tech giants completely dominating the digital economy of the MENA region, creating a dependence on foreign technology. Following the Arab Spring in 2011, this also raised concerns for governments, where they realized the importance of being in control of the cyberspace and local data within their borders, to maintain order and prevent uprisings. Today, MENA governments are aiming to prevent further uprisings and pushing to protect their data and digital economies, by implementing and endorsing data protection laws and data localization policies and being more careful in foreign investment in the sector.

With the rapid expansion of the digital economy, foreign governments are constantly looking to dominate the MENA market, creating a "digital cold war". This is primarily a battle between the USA and China, for the influence of the MENA region, more specifically in the implementation of the newest digital infrastructure. This can be seen in the increased involvement of US firms such as Amazon, and Chinese firms such as Huawei, both offering advanced technologies such as cloud services and internet. This essentially leads to the idea of the MENA region losing control over its digital economy and sector and leads to digital colonialism.

Definition of Key Terms

Digital Colonialism

Digital colonialism is defined as the control of data infrastructure usually in developing countries and often by dominant western parties, countries or companies. This data is used and controlled unethically, which is beneficial for these parties to translate into profits. This leaves users vulnerable to losing their data and being exploited. This in turns creates a bigger digital divide, and creates a bigger dependence on foreign infrastructure, which allows for expanded digital colonialism in the MENA region.

Digital Sovereignty and Independence

Digital sovereignty and independence is the ability of a country to fully control the digital infrastructure, technologies, and online activity within its borders. This means it does not depend on any other country for controlling its data, or online activity. This is important to take note of, as this is not the case for many of the countries in the MENA region, and one of the causes of the conflict.

Digital Divide

The digital divide refers to the difference in development of technological infrastructure between countries, and the big gap dividing these nations. This usually leads to digital dependence, a loss of digital sovereignty. This is important as one of the root causes of this issue is the big digital divide between more advanced nations and the less advanced nations in the MENA region.

Information and Communication Technology (ICT)

ICT refers to digital tools such as the internet, networks, or other software that enables communication and the exchange of information. This is a broad term with many kinds of digital infrastructure falling under its category. Strengthening these systems locally is vital in protecting countries from digital colonialism, with countries already dominating the field of ICT, this leads to the expansion of digital colonialism in the MENA region through exporting to the region and operating in it.

Data Localization

Data localization is the practice of keeping data and other digital information and infrastructure within the borders of the country, a practice that is rarely seen in the MENA region due to heavy reliance on foreign digital infrastructure which makes it difficult to grow their own sector, relating back to the issue of the digital divide and digital colonialism in the MENA region.

Digital Trade Agreements

Digital trade agreements govern the flow and trade of data, e-commerce, and other digital information, services, and infrastructure across borders. These trade agreements are in place to promote cooperation in developing the digital world, but if not used carefully, this can be a way for foreign countries to export their infrastructure and limit the development of these sectors in the MENA region, therefore it is important for the MENA region to take part in these agreements, while also balancing their own development.

General Overview

It is important to address the growth of the digital colonialism in the MENA region, caused by the digital divide and data exploitation in the region. Foreign companies implement data centers, cloud services, and internet infrastructure in the MENA region and gain control to sensitive data and information and influence the sector in the region. This leads to MENA countries falling behind in the development of their digital sector and economy. Today, these underdeveloped MENA countries depend on foreign governments and firms to import the infrastructure. This issue started many years ago, when the world began to shift towards a digital age, when firms from foreign countries such as Microsoft, Amazon, and Huawei began to battle over digital influence in the MENA region. As the digital sector developed, MENA countries began to understand the importance of digital influence and control. An example of this is the Arab Spring, which took place between 2010 and 2011, starting in Tunisia, when a street vendor burned himself in protest the president Zine El Abidine Ben Ali, which spread quickly through social media, leading to more protests in neighboring countries like wildfire, where many mass protests took place demanding regime change.

Digital Divide

The Digital Divide is the growing separation of technological infrastructure and is defined by the UN as the gap between people who have access to Information, Communication, and Technologies, and those who do not. Starting back in the early 2000's when western countries began to develop and globalize digital innovations, in comparison to countries in the MENA region lacked the expertise or the resources to keep up, leading to the Digital Divide. As a result, many countries in the MENA region lack the necessary technological advancements in sectors such as education, healthcare, government, and economic growth. This is seen in a study by "euromesco", which states that in 2024, 50% of people in the MENA region had access to the internet, whereas in Europe, 94% of households accessed the internet. (Nocetti) The Digital Divide is between MEDC's such as the USA, Germany, the UK, and China, and LEDC's such as MENA countries. Since the start of the shift to the digital world, foreign companies dominated the digital sector even in the MENA region, leading to complete dependence and a lack of digital development and sovereignty, therefore creating a huge and growing digital divide. MEDC's constantly come up with new innovations in the digital world, ranging from cloud services, data centers, and internet infrastructure, and implementing them in the MENA region, with no data localization or other data protection.

To further emphasize the digital divide, when comparing the digital economy of Germany to the entire MENA region, we see that the MENA region has grown to around $200Bn, compared to $232Bn in Germany. Although these numbers show the alarming nature of the digital divide, it is also important to note that according to a study by Redseer Strategy Consultants, the digital economy of the MENA region has grown from $91 Bn in 2021, to $200 Bn in 2025, with digital channels set to drive more than 11% of private consumption across the MENA region. (Ganediwalla) This evidence indicates the promising industry of digital infrastructure and software development, and the importance of domestic investment, to bridge the digital and economic divide. Despite clear growth, many of this comes from foreign-owned firms, with countries such as Apple, Amazon, Huawei, Google, and Microsoft, leading the development of different kinds of digital infrastructure. This reliance on foreign-owned firms raises questions over long-term sovereignty and the ability to bridge the digital divide.

Western Control

Western Countries such as the United States of America, and their firms, strongly benefit economically from their digital infrastructure. They lead the sector in exports and are constantly innovating and implementing both in the country and out, therefore, this sector is very important for these countries. For example, a study done by the OpenNet Initiative, shows that over forty countries worldwide use western made software to filter political, social, and security-threatening information found online. (York) This could lead to an increased western control of public opinion, propaganda, and political influence. It is very dangerous for this software to be imported from foreign countries and could lead to misleading algorithms and content in the MENA region which benefits the suppliers of this software. Additionally, what happens in the rest of the digital infrastructure imports such as data centers, is very similar.

Although it is important for LEDC's to import advanced infrastructure, it is also important to develop local industries and bridge the digital divide. Due to an overreliance on foreign industry and imports, this leads to an increase in the digital divide, and a decrease in digital dependence. Therefore, it is important to continue to improve international relations between MENA countries and MEDC's, but it is also important to consider privacy and safety in the MENA region, to support digital sovereignty and independence. Countries in the MENA region are already pushing to implement new digital infrastructure and bridge the digital divide, such as Saudi Arabia and the UAE. For example, according to the Gulf International Forum, in 2025, AI is set to account for 12.4% of Saudi Arabia's GDP, and nearly 14% of the UAE's GDP, showing huge development in digital economy growth in the MENA region, with countries investing in their local sectors. (White)

Data Privacy and Ethics

Data privacy and exploitation concerns are growing, with users experiencing to the unethical practices of governments and big corporations, including false end-end encryption claims, and backdoor access. Recently, many corporations and international policies have been created in order to maintain ethical practices with data and other digital infrastructures and to ensure the safety of sensitive information, but unfortunately although these international laws are supposed to be applied, large corporations and governments usually are given access to sensitive

information such as location, IP address, phone numbers, emails, home address, and more. For example, the European Union has a governing body for data protection called the General Data Protection Regulation or the GDPR, which establishes the rights of individuals for their data, and reinforces individuals' rights to access, rectify, erase, and restrict the processing of their personal data, a huge step towards digital privacy and ethical data practices. Recently, a huge scandal took place in the European Union, more specifically in France. Telegram is an end-end encrypted social messaging app, which essentially means no one can access private messages. When the Founder and CEO of Telegram arrived in Paris for vacation, he was arrested, placed in solitary confinement, and accused of taking part in the various crimes that were orchestrated through Telegram. According to numerous sources such as Freemindtronic, this could lead to stricter regulations regarding governments access to individual data, meaning companies based in foreign countries such as the MENA region, could access private information from civilians, and no longer implement the "end-end encryption". (FMTAD)

This year's AMMUN theme "Deliberate to Liberate", is strongly related to the topic of Digital Colonialism in the MENA region. The lack of digital sovereignty and independence in the MENA region, the growing digital divide, and the increase dependence on western digital infrastructure, all calls for deliberation in the MENA region. With effective planning and deliberation, comes independence and liberation. In this case, the liberation of the digital sector of the MENA region from western control. Through dialogue, education, planning, and governance, MENA states can come together to liberate the digital economy and grow it.

Major Parties Involved

Gulf Cooperation Council (GCC)

The Gulf Cooperation Council (GCC) includes countries like Kuwait, Saudi Arabia, UAE, Qatar, Bahrain, and Oman. These countries are known for their huge and rapidly growing economies, but also for their heavily oil reliant economies. Therefore, these countries are shifting away from that reliance and are looking to invest their money into advanced technology, such as more digital infrastructure. This is seen in projects such as Saudi Arabia's Vision 2030. This meant more imports from foreign countries, and more foreign countries looking to expand their cyber influence in the region. Unfortunately, the money is invested into importing digital infrastructure and bringing in foreign corporations to build data centers and apply software, rather than invest in local production and education to improve the sector domestically. This leads to more access to individual and government data for foreign parties and makes it easier for those foreign parties to access sensitive information, pushing these promising countries away from a promising digitally independent future. This party is very important as this is where the capital of the region mainly exists, and the most opportunity.

The European Union (EU)

The European Union has also played a huge role in policies for user privacy and data ethics. The General Data Protection Regulation, or GDPR is a regulation that harmonizes data protection laws across the EU and emphasizes the rights of individuals to protect their data and be fully aware of where their data goes, to avoid any dangers or harm. This regulation applies to organizations within the EU, or those based outside the EU that wish to offer their goods and services to individuals in the EU, emphasizing the commitment of the European Union to protect their individuals right to protection and privacy. This also brings us back to the digital divide, with a larger emphasis on the rights of those in the EU, and less emphasis on the rights of the

individuals in other less economically developed regions such as the MENA region, and the rights of its individuals to protect their data from unethical activity, especially from American, European, and Chinese digital infrastructure imports. Although data privacy is implemented in the European Union, it should also be implemented with strict policies emphasizing the rights of individuals for data privacy in the MENA region, to protect from foreign access to sensitive data, further bridging the digital divide.

The United States of America (USA)

The United States plays a major role in the global tech industry and has strong economic and digital ties to the MENA region. It is a leader in tech exports and many field pioneers are based in the USA, such as Apple, Amazon, SpaceX, and Microsoft. The United States is a heavily involved party as it is a very influential nation in the MENA region, and with the exports of digital infrastructure such as data centers, this could easily be used for their advantage, and for access to sensitive information either from the public, or from military or private sources to gain more influence over the country. This therefore negative impacts the digital independence and sovereignty of countries in the MENA region. It is also important to note that the USA does not have a single policy explicitly and clearly regarding data or digital privacy. It's most relatable law to this issue is The Privacy Act of 1974, which establishes rules for all federal agencies on collecting, using, and maintaining personal information.

The People's Republic of China

China and the USA had a war over digital influence in the MENA region, fighting to be the top exporter of digital infrastructure in the MENA region. Additionally, the first war took place in the UAE, where companies from the USA such as Microsoft and Amazon install digital infrastructure and data centers, to compete with companies from Beijing, such as Huawei. With the USA even including a clause for countries to prevent any Chinese digital infrastructure imports in arm trade deals, and other important political contracts, showing the extent of the battle

for digital control in the region. China is currently aiming to expand its digital influence in partner countries and regions, including the MENA region. To do so, they are currently undergoing the Belt and Road Initiative (BRI) and the Digital Silk Road (DSR) to improve the digital influence of China around the world. Both projects revolve around creating digital infrastructures around the world and implementing them in different regions, with options such as 5G internet, fiber optics, data centers, and more. Furthermore, both projects have implemented these technologies in MENA countries such as Egypt, Saudi Arabia, UAE, and Algeria. Although this does mean more advanced technologies present in the MENA region, this technology is controlled and operated by China, making it even harder for these countries to catch up. This makes the MENA region a warzone, with digital independence and sovereignty no longer an option, and leaving a question of either Chinese of American influence.

Global Cyber Alliance (GCA)

The Global Cyber Alliance (GCA) was founded in 2015 by the Center for Internet Security, the Manhattan District Attorney's Office, and the City of London Police, to prevent cybercrimes. It has since developed into a global organization for regulating and preventing cybercrime. The GCA aims to protect privacy, diversity, and inclusion. The GCA applies cyber security digital infrastructure in small businesses around the world to ensure data privacy and prevent data breaches and exploitation. Although it is based in these western countries and founded by them, the end-to-end encryption services prove as a promising solution to preventing data privacy issues and ethical concerns regarding individual privacy and foreign access to this important and sensitive data.

Timeline of Events

1980	OECD Privacy Guidelines is adopted The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal

	Data, is the first internationally recognized set of principles for privacy protection and data flow, it was originally adopted in 1980 and then updated in 2013. This acted as a foundation for future laws to be implemented and created regulations and laws for data privacy as the digital world began to develop. Although most MENA countries are not a part of the OECD guidelines, it is important that MENA countries abide by these laws to maintain strong digital trade relations with countries a part of the OECD, including many European countries.
2001	Council of Europe Convention on Cybercrime in Budapest The convention signed in Budapest in 2001, aims to implement data privacy laws to protect sensitive data, and to encourage countries that sign the convention to cooperate and work together to prevent cybercrime and ensure thorough investigation and working together to prevent computer crime. It defines cybercrimes such as illegal access, data interference, and system interference. Although the convention was initiated by the council of Europe, it has since reached global states such as the USA, Japan, and Australia.
2013	The Snowden Revelations A National Security Agency Contractor named Edward Snowden revealed classified documents to journalists that exposed the USA and other countries known as the Five Eyes Alliance, which includes the USA, UK, Canada, Australia, and New Zealand. The countries were tapping international underwater internet cables, using secret court orders to pressure organizations such as Facebook, Google, Microsoft, and Apple, to hand over private user information and sensitive data. These revelations were very alarming, especially to countries who had imported digital infrastructure from those countries, as they exposed the extent of exploitation and access to data these countries have.
2018	EU GDPR was Adopted The EU GDPR was adopted by the European Union on May 25th, 2018, and it replaced the 1995 Data Protection Directive and was designed to harmonize data privacy laws across Europe, to make for an easier cross-border data use experience. It also prioritized EU citizen's safety and protection from data exploitation. Although it is an EU regulation, it has global reach, and any company that processes data from EU residents, must comply, this even includes companies based in the MENA region that wish to do business with companies based in Europe and use European civilians and companies' data.
2021-2022	Global Cross-Border Privacy Rules (GBPR) Forum is Established A multinational effort led by APEC countries (Asia-Pacific Economic Cooperation). The

	forum was established to improve cross-border data protection and cooperation in solving cybercrime, setting ground rules for the sharing of data, and working towards the prevention of the exploitation of any personal data. Although it was originally launched by APEC, in April of 2022, a new initiative to globalize the framework was introduced by the United States, Japan, Canada, South Korea, and the Philippines, officially creating the CBPR Forum
2023 (Ongoing)	Global Digital Compact Ongoing efforts for countries to improve cooperation on preventing cybercrimes and create a safe digital world. Also aiming to minimize data breaches and create a safe and inclusive digital world. It is initiated by the United Nations, with the goal to establish a free and safe digital world for all. The compact aims to set the norm for the handling and the development of digital infrastructure such as the internet, data systems, and AI. This compact was expected to be finalized and formally adopted in September of 2024 but is instead going to be formally adopted in September of 2025, at the UN headquarters in New York City.

Attempts to solve the issue

Developments In the Field of Information and Telecommunications in the Context of International Security, 8 December 2005 (A/RES/60/45)

This resolution addresses the threat that ICT's pose against the security and digital sovereignty of states. It was a part of a series of resolutions aimed at the ways in which international law can prevent cybersecurity threats. This resolution aims to enhance international cooperation in preventing cybersecurity. This resolution was specifically pivotal for developing countries such as those in the MENA region, as it emphasized capacity building, equitable access to cyber tools and bridging the digital divide. It was adopted as part of the UN's growing recognition of the threat that cybersecurity poses if not handled correctly, and how it could become a critical point in world peace and security.

The Right to Privacy in The Digital Age, 18 December 2013 (A/RES/68/167)

This resolution relates to the mentioned Snowden Revelations and was adopted in direct response to that event. This resolution called for the prevention of data interception and collection

on a mass scale, especially when conducted without proper legal frameworks, and calls for transparent laws and legal frameworks for companies and countries to legally and safely transfer data and use other digital infrastructure. This resolution targeted MEDC's with advanced digital infrastructure, to prevent illegal tracking of data, and helped LEDC's protect their data by providing a digital rights advocacy and safety framework.

Developments In the Field of Information and Telecommunications in the Context of International Security, 5 December 2018 (A/RES/73/27)

This resolution builds upon past resolutions with different titles regarding the importance of the safe use of digital infrastructure to prevent conflict. This resolution sets the basis for the ways to prevent the misuse of digital infrastructure especially in hostile situations that could lead to conflict and calls for more dialogue and transparent communication between states regarding digital infrastructure development and the prevention of data exploitation or other forms of misuse. This resolution supports efforts for digital sovereignty, and the threat that unregulated cyber activity poses to destabilize a country.

Countering the Use of Information and Communications Technologies for Criminal Purposes, 26 May 2021 (A/RES/75/282)

This resolution was adopted in 2021 after long negotiations regarding the definition of cyber-crimes, digital sovereignty, and state surveillance, with differing opinions coming from most western countries as opposed to China, Russia, and others. This resolution formed an Ad-Hoc committee responsible for drafting a new global convention on countering the use of ICTs for crime and calls for the right of each country to have a voice in digital sovereignty and cybercrime discussions to promote global action and prevention of misuse. This resolution was quite controversial, as some argued that it could set the framework for the ability of countries to censor and control the internet.

Developments In the Field of Information and Telecommunications in the Context of International Security, 7 December 2022 (A/RES/77/36)

This resolution is reaffirming past resolutions and what they stand for, including the importance of handling cybercrimes, accordingly, pushing for global transparency, and digital sovereignty for each state. This resolution urged developing regions such as the MENA region, to develop their digital infrastructure, to facilitate regional and global cooperation regarding digital development and the prevention of cybercrimes, as well as pushing for equitable access to digital infrastructure. This resolution is very similar to the rest of the mentioned resolutions and mainly reinstates the importance of maintaining global dialogue and communication to work together to prevent cybercrime.

Possible Solutions

Enforce Data Localization Plans: Data Localization refers to the process of storing data and maintaining it within a country's borders, to prevent misuse and exploitation of data. This solution can be implemented through local firms controlling data centers where local citizens and government data is stored, ensuring a completely confidential environment where all information must stay local and private. The main objective would be to implement and enforce laws where foreign firms must abide by data localization laws. This can be done through numerous ways including leveraging global trade deals to ensure data localization; by including it is a clause or a term in the trade deal. Governments can also provide incentives to businesses based within their borders which agree to complete transparency and data localization led by local experts from domestic firms, such as tax benefits, low-interest loans, workforce development, and more. This therefore creates a win-win situation which protects the important and sensitive data of the civilians and government and provides incentives to businesses based in the MENA region.

Education Systems and Domestic Development: It is important to develop the domestic digital sector to bridge the digital divide and build towards digital independence. This can be done through educating the youth and the coming generations to develop and grow the workforce in the sector. This starts by mandating courses on digital literacy and digital sovereignty in curriculums, put together by experts and approved by the government, to ensure local benefit. MENA countries can also benefit from eachother through expert exchange programs within the MENA region, for workforces and students to benefit from the experts in the different countries in the region, ensuring even more development. Another way to develop the workforce and enhance educational systems regarding the digital world is by forming partnerships and agreements with both private and public universities to implement simple digital literacy courses, teaching students how to protect their data, and prevent the exploitation of their data. Existing courses regarding software and data could be further developed with the help of experts, and new courses could also be introduced to increase expertise. Finally, to ensure access to different members of the community, open-source educational platforms, accessible for free can be implemented in the MENA region for citizens to develop their skills and develop the workforce and the sector, building towards digital dependence.

Domestic Algorithm Audits Against Data Misuse: To ensure that no foreign party is misusing any data within the borders of each country, MENA countries should set up auditing firms to audit any data that leaves borders, further assisting data localization plans. This can be

done by implementing thorough algorithms and AI scanning of data to look for any unapproved data leaving the borders of the country. This will help ensure that data is localized and used properly. The auditing firm should be formed locally, and under the supervision of the government. The firm will have local leadership and will be developed by local software, AI, and Data engineers and experts, this will ensure the functionality of the algorithm. The engineers and leadership will be bound to keep any information private through non-disclosure agreements to ensure the prevention of any exploitation of data. These algorithms should be updated quarterly to ensure the prevention of any bugs. The algorithm will be implemented into all digital infrastructure within the borders of the country and act as a filter, alarming authorities when any data is being misused or if a firm is attempting to export any data that is meant to be localized and private.

Guiding Questions

1. What digital infrastructure is sourced from western countries or corporations in the MENA region?
2. How does digital infrastructure control lead to leakage of important data and private information?
3. How can MENA governments ensure encryption and privacy of data in digital infrastructure?
4. What international laws and regulations are relevant in sourcing data infrastructure and protecting citizens and their privacy?
5. What factors stop MENA countries from gaining digital dependence and use western digital infrastructure?
6. What can MENA countries do to gain digital sovereignty and independence?
7. How can MENA countries increase privacy in their digital sector and improve cyber security infrastructure to ensure encryption?
8. How can the lack of digital independence in the MENA region further bridge the digital divide?
9. How can western access and control over digital infrastructure in the MENA region allow foreign parties to shift public opinion, boost propaganda, and gain influence?
10. How would an increase in manufacturing digital infrastructure to implement independently help bridge the digital divide and increase control over media and cyber environment?
11. In what ways does foreign ownership of core digital platforms and undersea data cables pose a strategic vulnerability for MENA governments during political conflicts or crises?

Appendix

- https://www.isocfoundation.org/2023/06/what-is-digital-equity/?gad_source=1&gad_campaignid=16731231744&gbraid=0AAAAAoZgpaiPAwTJ3IhdgVUXWr7TRNCgj&gclid=Cj0KCQjwsNnCBhDRARIsAEzia4CiYw6dNP0zWXLBdXkOQwiZgTHlEFhO5ZhYhnWVnzsWiDHZrHQdwHwaAsYnEALw_wcB
- https://www.euromesco.net/publication/digital-sovereignty-in-the-mena-region-overcoming-paradoxes-to-ensure-digital-resilience/?utm_
- https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/?utm
- https://www.accessnow.org/publication/exposed-and-exploited-data-protection-mena/?utm
- https://www.euromesco.net/publication/digital-sovereignty-in-the-mena-region-overcoming-paradoxes-to-ensure-digital-resilience/?t
- https://www.mei.edu/publications/middle-east-cyber-sovereignty-hampers-economic-diversification
- https://neosnetworks.com/resources/blog/what-is-digital-infrastructure/
- https://influenceindustry.org/en/learn/dilemmas-personal-data-political-influence/
- https://datacentremagazine.com/top10/top-10-countries-with-the-most-data-centres
- https://markmunger.com/menas-digital-transformation/

Bibliography

"Admissions." GC_WHITE, 5 Aug. 2025, www.gchumanrights.org/preparedness/chinas-digital-influence-in-the-mena-region-a-mixed-blessing-for-mena-countries/#:~:text=China's%20technology%20outreach%20to%20the%20region&text=The%20DSR%20has%20allowed%20major,home%20to%20several%20DSR%20projects.

Bloomberg. "Consumer Data Privacy Laws." *Bloomberg Law*, 12 Dec. 2023, pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-laws/. Accessed 17 July 2025.

Coordinator, Julien, et al. *DIGITAL SOVEREIGNTY in the MENA REGION: Overcoming Paradoxes to Ensure Digital Resilience.* Aug. 2024, www.euromesco.net/wp-content/uploads/2024/10/Policy-Study36.pdf. Accessed 23 July 2025.

Council of Europe. "Full List." *Treaty Office*, 2001, www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185. Accessed 16 July 2025.

Dag, Hammarskjöld, and UN Secretary-General. "The Decision of the Secretary-General on the Report of the Committee Investigating the Bang-Jensen Case." *United Nations Digital Library System*, UN Dept. of Public Information, 18 Jan. 1958, digitallibrary.un.org/record/3993305. Accessed 23 July 2025.

FMTAD. "Telegram and Cybersecurity: The Arrest of Pavel Durov - Freemindtronic." *Freemindtronic*, 25 Aug. 2024, freemindtronic.com/telegram-cybersecurity-arrest-pavel-durov/. Accessed 15 July 2025.

Ford, Robert S., et al. "In the Middle East, Cyber Sovereignty Hampers Economic Diversification." *Middle East Institute*, 26 June 2025, www.mei.edu/publications/middle-east-cyber-sovereignty-hampers-economic-diversification.

Ganediwalla, Sandeep. "5 Predictions for MENA's Digital Economy in 2025 | Redseer." *Redseer Strategy Consultants*, 19 Feb. 2025, redseer.com/newsletters/5-predictions-for-menas-digital-economy-in-2025/. Accessed 22 July 2025.

"Legal Text." *General Data Protection Regulation (GDPR)*, 22 Apr. 2024, gdpr-info.eu/.

Hoffman, Jon. "Espionage and Repression in the Middle East Courtesy of the West." *openDemocracy*, 15 May 2020, www.opendemocracy.net/en/north-africa-west-asia/espionage-and-repression-middle-east-courtesy-west/.

Hu, Mo. "Eyes Everywhere: The State Surveillance of Human Rights Defenders in Jordan." *HuMENA*, 20 Dec. 2024, humena.org/eyes-everywhere/.

Humena. humena.org/wp-content/uploads/2024/02/Report-on-the-Situation-of-the-LGBTQI-1.pdf. Accessed 29 June 2025.

Jason, Pr. "China's Digital Influence in the Middle East: Implications for US Relations." *Stichting Jason*, 24 Jan. 2024, jasoninstitute.com/chinas-digital-influence-in-the-middle-east-implications-for-us-relations/.

Langendorf, ByStefan Lukas andManuel, and ByMark Kennedy. "Cloud Competition Is Heating up in Mena and China Expands Its Presence." *Wilson Center*, 18 Feb. 2025, www.wilsoncenter.org/article/cloud-competition-heating-mena-and-china-expands-its-presence.

"Mena's Digital Transformation – Mark Munger – Valcros." *Mark Munger Valcros*, 10 Nov. 2024, markmunger.com/menas-digital-transformation/.

Middle East & North Africa Internet Infrastructure. www.internetsociety.org/wp-content/uploads/2020/09/Middle_East_North_Africa_Internet_Infrastructure_2020-EN.pdf. Accessed 29 June 2025.

"Mission/Vision - GCA: Global Cyber Alliance: Working to Eradicate Cyber Risk." *GCA | Global Cyber Alliance*, 16 May 2025, globalcyberalliance.org/mission-vision/.

OECD. "Science, Technology and Innovation." www.oecd.org/en/topics/science-technology-and-innovation.html. Accessed 20 July 2025.

Pheaden. "Consumer Data Privacy Laws." *Bloomberg Law*, 3 Jan. 2025, pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-laws/#:~:text=The%20Privacy%20Act%20of%201974%20establishes%20rules%20for%20collecting%2C%20maintaining,the%20ability%20to%20request%20corrections.

Sandeep Ganediwalla. "5 Predictions for MENA's Digital Economy in 2025 | Redseer." *Redseer Strategy Consultants*, 19 Feb. 2025, redseer.com/newsletters/5-predictions-for-menas-digital-economy-in-2025/. Accessed 22 July 2025.

Smith, Mary Kate. "A Gulf Apart: Analyzing AI in Saudi Arabia and the UAE." *Gulf International Forum*, 7 Feb. 2025, gulfif.org/a-gulf-apart-analyzing-ai-in-saudi-arabia-and-the-uae/. Accessed 21 July 2025.

Tidy, Joe. "Telegram Founder Durov Allowed to Leave France Following Arrest." *BBC News*, BBC, 17 Mar. 2025, www.bbc.com/news/articles/cg703lz02l0o.

UNCTAD. "Digital Economy Report 2021." *UNCTAD*, 2021, unctad.org/publication/digital-economy-report-2021. Accessed 19 July 2025.

United Nations. "Global Digital Compact | Office for Digital and Emerging Technologies." *Un.org*, 2024, www.un.org/digital-emerging-technologies/global-digital-compact. Accessed 21 July 2025.

"The Digital Economy in Germany." *German Trade and Invest*, 2025, www.gtai.de/resource/blob/63904/e140931b97cb704e85c0b7e9d9e8cc63/20250519_FS_Germany%C2%B4s_Digital_Economy_WEB.pdf. Accessed 18 July 2025.

The Editors of Encyclopaedia Britannica. "Arab Spring." *Encyclopædia Britannica*, 14 Jan. 2015, www.britannica.com/event/Arab-Spring. Accessed 19 July 2025.

"West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011." *OpenNet Initiative*, opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011. Accessed 30 June 2025.

"What Is Data Protection and Privacy?" *Cloudian*, 26 May 2025, cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/.

Contact Information

Hamzah Abu-Irshaid

hamzah_abuirshaid@abs.edu.jo

+962 777779000