April 2021

Internet Governance in the Middle East and North Africa

Michael Kende

Internet Society

I would like to thank Nermine El Saadany for her leadership and Hana Sabbagh and Hanna Kreitem for their support in the region, and Katie Watson Jordan, Konstantinos Komaitis, Andrew Robachevsky and Carl Gahnberg for their work on the Internet Way of Networking project and input on this report. Members of the Internet Society Community in the region also provided input on country characteristics.

– Michael Kende

Introduction

The Internet is a 'network of networks' made up of tens of thousands of networks that interconnect and route traffic efficiently between end points. While the interconnections and routing of traffic are intrinsically borderless, the decisions of national governments can impact key properties of the Internet. As the Internet began to develop and grow, governance mechanisms also began to develop.[1] As it then globalized, different countries and regions have adopted it and brought new approaches to governance, reflecting their traditions, economies, and societies. This paper focuses on the Internet's governance in the Middle East and North Africa (MENA).

The vitality of the Internet and the critical need to further develop and expand it has been highlighted during the pandemic.[2] Efforts to curb COVID-19 through stay-at-home orders around the world left everything and everyone almost frozen in place. The Internet helped maintain business continuity, government services, education, and social lives. The MENA region, like all others, saw quick uptake in usage, and a number of governments adopted supportive policies to help Internet Service Providers (ISPs) and content providers to serve this demand.[3] However, the response also highlighted remaining gaps in adoption and access to valuable content and services.

In order to meet the goal of increased Internet availability and adoption, ISOC has a paper entitled *A policy framework for enabling Internet access*.[4] The framework outlines three linked areas which, together, will advance access: Expanding Infrastructure; Supportive Governance; and Fostering Skills and Entrepreneurship. These three areas ensure that the Internet is available and resilient, that users have digital skills and the ability to produce and not just consume content and services, and the governance to enable this growth of the Internet.

The Internet Society established a Middle East Bureau in 2016 to better support regional efforts to develop the Internet. It recently released a paper, *Middle East & North Africa Internet Infrastructure Report*, that focuses on the first linked area of the policy framework, 'Expanding infrastructure'.[5] This paper focuses on the second area, 'Supportive Governance', and a future paper will focus on the final area, 'Fostering Skills and Entrepreneurship'.

Supportive governance should aim to promote the qualities of the Internet that have led to its success. As the Internet has grown exponentially in adoption and usage, it has transformed our lives and societies for the better. The Internet owes this impact to the strength and resilience built into its open architecture, embodied in a number of critical properties, which the Internet Society has identified and defined as the *Internet Way of Networking*.[6] These properties can be impacted by a country's policies and regulations, and this paper assesses the impact of those policies and regulations on the Internet Way of Networking as applied to the MENA region.

[1] https://www.internetsociety.org/resources/doc/2017/brief-history-internet/

[2] https://www.itu.int/en/myitu/News/2020/09/16/19/22/UN75-Partnership-Dialogue-for-Connectivity-Doreen-Bogdan-Martin

[3] https://www.internetsociety.org/resources/doc/2020/impact-of-covid-19-on-the-internet-ecosystem-in-mena/

[4] https://www.internetsociety.org/resources/doc/2016/a-policy-framework-for-enabling-internet-access/

[5] https://www.internetsociety.org/resources/doc/2020/middle-east-north-africa-internet-infrastructure-report

[6] https://www.internetsociety.org/issues/internet-way-of-networking/

Internet Way of Networking

Ecosystems, in general, are in a constant state of change. The Internet is similar – it is complex, diverse, and dynamic – and one constant feature is that it is continually changing. The main characteristics of the Internet evolve, and innovation takes place across the networks that make up the Internet. Yet, the basic principles that guide the Internet remain the same.

The Internet is inherently decentralized, and its ability to respond to the needs of the pandemic proves that this model ensures a resiliency and strength capable to support rapid growth and usage of the network. Voice and video applications enabled businesses to function and kept societies active during lock down, websites provided access to news and information, while streaming services provided well-deserved breaks. Educators, health care services, Internet companies and others provided innovative new services to address the needs of citizens. Individual networks were able to address the traffic growth, and governments helped with increased spectrum, subsidies, and other support.

The Internet Society supports and promotes the development of the Internet as a global technical infrastructure to enrich people's lives by supporting an open, globally-connected, secure, and trustworthy Internet. To ensure that the Internet is able to continue to deliver these benefits, we identified five critical properties that define the Internet Way of Networking. These constitute the necessary – though not always sufficient – conditions for the success of the Internet.

Critical Property	Benefits to the Internet Community
Critical Property 1: An Accessible Infrastructure with a Common Protocol	Unrestricted access and common protocols deliver global connectivity and encourage the network to grow. As more and more participants connect, the value of the Internet increases for everyone.
Critical Property 2: A layered architecture of interoperable reusable building blocks	Open architecture creates common interoperable services, which deliver fast and permissionless innovation everywhere. The inclusive standardization process and demand-driven adoption ensures that useful changes are adopted, while unnecessary ones disappear.
Critical Property 3: Decentralized management and distributed routing	Distributed routing delivers a resilient and adaptable network of autonomous networks, allowing for local optimizations while maintaining worldwide connectivity.
Critical Property 4: A Common Global Identifier System	A common identifier set delivers consistent addressability and a coherent view of the entire network, without fragmentation or fractures.
Critical Property 5: A General Purpose Network	Generality delivers flexibility. The Internet continuously serves a diverse and constantly evolving community of users and applications. It does not require significant changes to support this dynamic environment.

Each of these critical properties manifests itself in specific benefits, listed in the table on the previous page. A common theme among these benefits includes global connectivity, unrestricted access, common interoperable services, and evolving applications in a dynamic environment. This highlights that the technical design of the Internet is intrinsically borderless and permissionless. It was designed so that bits would be routed according to the most efficient path based on the underlying voluntary interconnections between networks, while new applications could be developed and made available to users without requiring permission from any authority.

In practice, borders do make a difference on the networks within the countries. Some differences are intrinsic to the countries. Based on economic development, geography, and history, countries differ in the availability of network infrastructure – some have near-universal fixed networks, others rely almost exclusively on mobile; some are beginning to upgrade to 5G mobile services, others have not yet completed the deployment of 3G. And users have different preferences for content and applications, depending on their culture, language, religion, and other socio-economic factors.

However, other differences depend on policy and regulatory choices of the national governments – we focus here on those choices and their impact on the critical properties of the Internet.

Internet Impact Assessment Toolkit Use Cases

The Internet Society developed the *Internet Impact Assessment Toolkit* as a way to better understand the critical properties of the Internet, or as ISOC calls it, the Internet Way of Networking.[7] The Toolkit uses the critical properties as a compass to assess the impact of regulations and other developments on the Internet's foundation. In order to demonstrate the use of the Toolkit, four use cases were developed, focused on Interconnection and Routing policies; Intermediary Liability protections; Data Localization mandates; and Content Filtering.[8] Each use case examines case studies in particular countries to evaluate the impact of the regulations.

In MENA, this paper examines six policies arising in countries that impact the Internet Way of Networking. Using the Toolkit, and drawing on the use cases, we assess each of these six sets of regulation in subsequent sub-sections below.

- **Data Localization.**[9] Organizations often aggregate data within a region or on a global basis for a number of reasons – to efficiently host the data, to be able analyze a broad data set to evaluate healthcare, to process business operations, to develop their services, among other reasons. Recently there has been a trend in countries to require localization of some or all data on their citizens, for reasons of privacy or security. In MENA countries, to-date, such restrictions have focused on sensitive financial and health data.

[7] https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

[8] Another Use Case relevant to this project will be developed, relating to regulations regarding Voice over IP services.

[9] Data Localization has been analyzed in one of the existing Internet Way of Networking Use Cases. https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/

- **VoIP Bans.** Many applications benefit from network effects – the more users, the more valuable the application is for other users – this includes Voice over IP (VoIP) services. A few countries have banned use of these applications, in order to protect the revenues of the telephone companies who sell traditional voice services. In MENA, several countries have temporarily lifted the bans on select VoIP applications during the pandemic lockdowns, but have not lifted the bans on all applications, nor made the lift permanent.

- **Internet Shutdowns.** Perhaps the most dramatic and impactful demonstration of the impact of borders comes from decisions to throttle or shutdown particular applications or the entire Internet within a country or region, often in response to internal unrest. An early example came in 2011 in Egypt for five days, in response to the protests during the Revolution. Since then, such shutdowns have been repeated globally – in 2019, Access Now documented 213 shutdowns in 33 countries around the world.[10]

- **Content Filtering.**[11] Perhaps less dramatic than Internet Shutdowns, but potentially longer lasting or permanent, Content Filtering requirements deny access to certain online content based on government regulations. The content may be filtered based on deep packet inspection (DPI) which examines traffic flowing by for sensitive content, or based on the domain name or underlying IP address being on a list of banned content.

- **IXP Restrictions.** Internet Exchange Points (IXPs) serve the important function of helping to lower the cost and latency of exchanging traffic, by localizing the exchange within a country or region and avoid using international connections for the exchange. Governments have helped to establish these IXPs in a number of countries, with positive benefits, however, restrictions on who can connect to the exchanges can limit the full benefits.

- **International Gateways.** Finally, while almost all countries have liberalized their telecommunications markets and introduced competition, the liberalization is not always complete. In particular, while there is typically competition between several mobile operators and fixed Internet service providers (ISPs), in MENA there is sometimes a monopoly or duopoly at the International Gateway, which results in higher prices for international IP transit, an important input for all Internet access.

These six issues all result from policy and regulatory decisions from governments. In part, this comes from incomplete reform of the telecom sector, in which the government retains ownership over the incumbent provider and seeks to protect it from the full results of sector reform. In part, it comes from attempts to ensure privacy and security of citizens, both in general and at times of political unrest, and to keep away sensitive content. We focus here on the impact of the decisions on the critical properties of the Internet, and not the underlying political or cultural considerations.

[10] https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

[11] Content Filtering has also been analyzed as one of the existing IWN Use Cases. https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-content-filtering/

To determine the impacts of these policies and regulations, we examine the following countries in the region, highlighting examples of the six issues and their impact on the critical properties. The countries are Bahrain, Egypt, Jordan, Oman, Palestine, Saudi Arabia, and the United Arab Emirates. As shown in the following table, these countries are fairly advanced in terms of adoption, with the presence of at least one IXP, at least one certified data center, and numerous submarine cables, albeit with some exceptions. On the other hand, according to the ITU, none of the fixed-line incumbents in these countries are private or privatized.

Table 1: Country data (Source: World Bank, InternetWorldStats, Packet Clearing House and PeeringDB, Uptime Institute, TeleGeography)

Country	Classification	Internet Users	IXP	Data Centers	Submarine Cables (Planned)
Bahrain	High income	94.9%	MN-IX	3	5
Egypt	Lower middle income	48.1%	CAIX	8	14 (2)
Jordan	Upper middle income	85.3%	None	5	2
Oman	High income	78.5%	None	1	14 (1)
Palestine	n.a.	66.3%	PIX, PSIX	1	0
Saudi Arabia	High income	91.5%	SAIX, JEDIX	Approx. 80	14 (1)
United Arab Emirates	High income	96.4%	UAE-IX, Smarthub	Approx. 60	18

The table below summarizes the situation in each of the countries with regards to the six issues. Most of the countries present challenges with respect to at least one of the six issues, and each issue has at least one challenging case.

Table 2: Country policies and regulations (Source: In Country, DataGuidance, Freedom House, Reporters Sans Frontieres, Access Now, ITU ICT Data Portal, IXP website, primary research, 2020)

Country	Data Localization	VoIP Bans	Internet Shutdowns	Content Filtering	IXP Restrictions	International Gateways
Bahrain	No	No	No	Yes	No	Competition
Egypt	No	No	No	Yes	Only ISPs are members	Duopoly
Jordan	Finance data	No	Yes	Yes	No IXP	Competition
Oman	No	Yes	No	No	No IXP	Competition
Palestine	No	No	No	No	No	Competition
Saudi Arabia	Finance / healthcare	No	No	Yes	No	Partial competition
UAE	Finance / healthcare/ free zones	Yes	No	Yes	Only international traffic	Duopoly

Data Localization

Data Localization requirements often appear in privacy and data protection laws, which could be general laws covering all sectors of the economy, or could be sector specific laws.[12] Within the focus group of countries, Bahrain and Egypt have newly passed laws, with no Data Localization requirements; Oman and Palestine have no laws in place, and no sectoral requirements either. While Jordan has no general law, financial records must be stored in the country, including by non-Jordanian financial entities. Saudi Arabia also does not have a data protection law yet, but it does have a unique Cloud Computing Regulatory Framework, that restricts the transfer of financial and health data out of the Kingdom.[13] And finally, UAE has sector-specific laws requiring hosting of financial and health data exclusively in the country, with several exceptions discussed below.[14]

[12] Data Localization requirements raise issues around international trade, where there is a balance between free flows of data against national jurisdiction and sovereignty that has not fully played out. In any case, none of the Data Localization requirements discussed here have run afoul of any existing trade agreements. For more background, see http://www3.weforum.org/docs/White_Paper_Data_Localization_Barriers_Cross-Border_Data_Flows_report_2018.pdf.

[13] https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx

[14] UAE is working on a Federal Data Protection Law, which may embed Data Localization requirements at the national level.

As noted in an Internet Way of Networking use case, Data Localization is an increasing trend, with impacts on several of the critical properties.[15]

- **Critical Property 1: An Accessible Infrastructure with a Common Protocol.** Data Localization raises costs and entry barriers for relevant services. For instance, the requirement that all financial records be stored in Jordan, including by non-Jordanian financial entities, potentially requires significant duplication of assets in Jordan, which may limit entry by financial companies into the market.

- **Critical Property 3: Decentralized Management and a Single Distributed Routing System.** The requirement to keep data exclusively in one country, as is the case with the UAE, may keep the data from being stored in the most optimal place both in terms of resilience and connectivity. A multi-national company may find it efficient to store and process data in one central location, but that would not be possible if another country's data could not be moved. In the cases examined here, Data Localization is restricted to financial and healthcare data of citizens. While it might be efficient to aggregate the data outside the country, moving the data between countries is not itself intrinsic to offering the service.

Finally, while UAE has sector-specific data protection requirements, it also has three Free Zones that have adopted their own data protection laws: The Dubai International Financial Center (DIFC); Abu Dhabi Global Markets (ADGM); and the Dubai Healthcare City (DHCC). DIFC has just implemented a new law that is consistent with European General Data Protection Regulation (GDPR), and ADGM has proposed a similar law to GDPR, in which they allow international transfer of data to certain countries or by certain companies that meet their standards. This is in contradiction to the rest of UAE, sometimes referred to as onshore UAE, which does not allow transfers of financial data. DHCC also has its own law, which like onshore UAE does not allow transfers of health data.

It is not clear how relevant data can be transferred between onshore UAE and the free zones, but it appears that it might magnify the impact of the onshore UAE restrictions discussed above, by not allowing transfer within the same country. This could magnify the complications of offering services within the country.

VoIP Bans

Two countries have bans on VoIP applications, Oman and UAE, while in Jordan it appears the operators block VoIP against the stated policy of the regulator. Saudi Arabia had a block on VoIP that was recently lifted. Such bans are meant to protect the voice revenues of the operators. In light of the need to use VoIP and video conferencing at a time of pandemic lock downs, social distancing, and when offices are closed and travel is restricted, Oman and UAE have partially lifted the bans on a temporary basis.

In this light, we note that there are two types of VoIP applications, which broadly speaking could be termed as closed or open services.

[15] https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/

- **Closed apps:** These are apps where one needs to sign up for the service, and then can only communicate with those who are also signed up for the same service. This category includes WhatsApp, Skype, Facebook Messenger, and FaceTime. These apps tend to be used for one-to-one text, voice, or video communications among friends, families, and colleagues.
- **Open apps:** These are apps where the organizer needs to be registered, but then can invite anyone to participate in the call – the only requirement is that they may need to download a software app the first time in order to be able to participate. This category includes Microsoft Teams, Zoom, BlueJeans, Skype for Business, Google Meet, and Webex, and they tend to be used for audio or video conferences with multiple participants.

It is noteworthy that the temporary lifting of the bans during the pandemic tended to focus on open apps. This may be because they are most useful for business during the pandemic, as evidenced by the steep rise in usage. On the other hand, the closed apps – with one-to-one communications, compete most closely with telecom operator offerings, and that may be why they were not included in the temporary lifting of the bans.

The bans run counter to the Internet Way of Networking for two reasons. Indirectly, VoIP services are applications that run on top of networks. While it is the networks that are the focus of the Internet Way of Networking, the purpose of the underlying critical properties is to ensure an Internet that enables access to all applications. Access to networks is a means to an end – the end is the applications and services that deliver the benefits of the Internet. Not having access to applications in a country deprives the users in those countries of these useful applications.

The direct reason that the bans on VoIP service run counter to the Internet Way of Networking is that they require the operators of the networks to block the services. The same imposition on networks is true when limits on intermediary liability are lifted. The ban on VoIP requires network operators to monitor and block applications, which is similar to the situation examined in the Internet Way of Networking Use Case on Intermediary Liability.[16] The ban on VoIP runs counter to two of the critical properties.

- **Critical Property 2:** Open Architecture of Interoperable and Reusable Building Blocks. Under the end-to-end principle guiding Internet development, network operators are responsible for carrying traffic from end-to-end, while applications at the end points are responsible for the service. Having to block the VoIP services changes the role of network operators, while impacting the interoperability of applications, thereby undermining the end-to-end principle.[17]
- **Critical Property 5:** A Technology Neutral, General-Purpose Network. The requirement to block VoIP services adds responsibility on network providers beyond transferring data to the next destination, requiring them to carry out additional functions such as traffic inspection. The networks become more specialized and less general purpose, and there is a limit on the applications that users can access through the networks.

[16] https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Use-Case_Intermediary-Liability.pdf

[17] See for example https://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf

The pandemic has highlighted the benefits of the Internet for users. As a result of lockdowns and the need for social distancing, there is an additional premium on the ability to communicate over the Internet. While countries have temporarily lifted bans on services that enable audio and video conference calls, in order to enable work, education, and other functions to continue, the ban on closed VoIP applications remains in place. This limits the ability of families, friends, and colleagues to communicate with each other.

It is clear that traditional text and voice calls are not a full substitute, because the banned VoIP applications also enable video calls and group chats. These VoIP applications are also not just used for voice communications. For instance, the World Health Organization is using WhatsApp to provide messages about COVID-19, which is not available to users in countries where WhatsApp is banned.[18]

Internet Shutdowns

In recent years there has been an increasing tendency to shut down all or part of the Internet in certain countries, starting with the Egyptian example in 2011. While shutdowns generally come during political unrest as a way to quell dissent or prevent planning, there is at least one more prosaic example. In Jordan, in addition to shutting down the Internet during a recent protest, certain social media apps are blocked close to schools during school examinations, to prevent cheating.

Overall, such shutdowns illustrate two aspects of a country's Internet. First, the top-down authority needed to order such a shutdown, and second, a lack of resilience in the infrastructure that allows this to take place. When there are few international entry points into a country, and a select few operators offering access service, including state-owned operators, then it is easier to shut down the Internet without any leakage or pushback.

Internet Shutdowns impact the following three critical properties.

- **Critical Property 1: An Accessible Infrastructure with a Common Protocol.** The open and accessible Internet delivers global connectivity. However, when the Internet is shut down, then there is no connectivity within the country (the goal of the shutdown) and also between the country and the rest of the world. This reduces accessibility and confidence in the availability of such infrastructure not only for individuals, but also for businesses, impacting the investment and general economic climate in the country.
- **Critical Property 3: Decentralized Management and a Single Distributed Routing System.** The ability to shut down the Internet in a country demonstrates a centralized management of the relevant operators in the country, which runs counter to the distributed routing of the Internet. The result is that it blocks the routing of traffic within the country and makes it inaccessible from the outside. The presence of such centralized control impacts resilience of the networks in the country, limiting their ability to respond to changing local conditions.

[18] https://www.who.int/news-room/feature-stories/detail/who-health-alert-brings-covid-19-facts-to-billions-via-whatsapp

- **Critical Property 5: A Technology Neutral, General-Purpose Network.** A partial shutdown can limit apps that users can access through the networks, and a full shutdown blocks what is available to outside countries. The general-purpose network is of less or no value when it is shut down, and applications and services are not available, including but not limited to the ones that led to the shutdown.

The very purpose of the shutdown – to disrupt connectivity within a country – is what directly violates the Internet Way of Networking. While targeting just the applications or users involved in a protest would itself run counter to the critical properties, targeting the entire Internet results in a comprehensive end to all the benefits of the Internet for the society and economy. The impact is not just felt in the country – the rest of the world loses connectivity to the country as well.

Content Filtering

As noted above, Content Filtering is common in the MENA countries examined here. Broadly speaking, it can take two technical forms – using DPI to examine traffic for content that violates regulations, or compiling a list of websites that are blocked. In both cases, network operators in the countries are required to use the technology to filter the content. The content that is filtered could focus on international content only, or also include domestic content. While virtual private networks (VPNs) can be used by users to avoid Content Filtering, this is an incomplete solution, as not all users have the capability to use VPNs, and in some countries, websites providing VPN services are also blocked.

In Bahrain, Egypt, Saudi Arabia, and UAE, Content Filtering is achieved by blocking websites based on the domain name or IP address. In Jordan, it appears that Content Filtering is diminishing in recent years, and reserved for news websites that do not seek the appropriate license.[19] In several of the countries, access to websites of companies providing VPNs has been blocked, to help prevent their use, and in one country the use of VPNs is illegal when used to commit a crime, which has been interpreted as using a VPN to avoid censorship.[20]

As noted in the Content Filtering Use Case, Content Filtering violates several critical properties.

- **Critical Property 1: An Accessible Infrastructure with a Common Protocol.** Content Filtering restricts access to the global Internet, making it less open and accessible and undermining the "permissionless innovation" model as well as the ability of unrestricted access that has driven the growth of the Internet.

- **Critical Property 3: Decentralized Management and a Single Distributed Routing System.** Content Filtering may centralize the management of access to websites, by implementing filtering policies provided by a government authority, or even a facility that automatically enforces filtering.

[19] https://freedomhouse.org/country/jordan/freedom-net/2019#B

[20] https://freedomhouse.org/countries/freedom-net/scores

- **Critical Property 4: Common Global Identifiers.** Content Filtering using global identifiers such as IP addresses fractures the use and value of these identifiers. Using IP addresses can also lead to collateral damage, blocking other websites or content within websites using the same IP address that are not the targets of the filtering.

- **Critical Property 5: A Technology Neutral, General-Purpose Network.** Using DPI for Content Filtering complicates the role of network operators, who would no longer be simply passing data packets on, but rather examining them and potentially blocking them.

Content Filtering limits the value of the Internet, raising a national or internal border to certain types of content, changing the role of network operators and the usage of global identifiers. It may involve regulatory restrictions on content providers, who require a license in order to not be blocked, and may result in 'over-blocking' some content and services using the same IP address as targeted websites.

IXP Restrictions

The IXPs in Saudi Arabia and Egypt were deployed and supported by their governments. The largest IXP in the region, UAE-IX is hosted at the data center of the telecom operator du, one of the two state-owned operators, and sits in a Transit Zone that is for international operators. These IXPs deliver significant benefits in their countries in terms of the efficiency of routing traffic and increasing the resilience of the networks. However, changing certain policies governing those IXPs can further help to deliver the full benefits of the Internet Way of Networking.

A particular issue relates to the access to content providers. As content and services continue to grow, their providers have developed their own content delivery networks (CDNs) to deliver the content to end-users efficiently via the ISPs in a country. They can do this in several ways – by connecting directly with multiple ISPs in a country, to provide them with content; to connect to one ISP that is connected to the IXP, where the content can be delivered to other ISPs; or connecting directly to the IXP to be able to exchange content. In most countries, the content provider is free to make its own arrangements with ISPs and/or the IXP, to efficiently route its traffic.

In some cases, a government may impose conditions on the connections to the IXP. For instance, in Egypt today only the ISPs are connected to the Cairo Internet Exchange (CAiX). Content providers have to seek permission from the regulator to connect to the IXP. This is not a common requirement for content providers in other countries, and to date no content providers have sought such permission, and none are connected.[21] This impacts the routing of the content, as the content delivery networks must either sit behind an ISP to exchange their traffic through the IXP, connect to multiple ISPs to deliver their traffic, or allow the ISPs to pick up the traffic in another country. The most efficient means to exchange the traffic is not available, in violation of one critical property.

[21] http://www.caix.net.eg/index.php/caix-policy

- **Critical Property 3: Decentralized Management and a Single Distributed Routing System.** Not connecting content providers to the IXP impacts the routing of the traffic between networks, in a way that is less efficient than it could be. It is possible that no CDN traffic would go through the IXP, and some traffic may be sourced from abroad that could more efficiently be accessed locally.

While the Saudi Arabian Internet Exchange (SAIX) is also government owned, and predominantly used by ISPs, there is at least one content provider connected. Nonetheless, the government ownership and operation of the IXP removes the traditional member-driven model that is common with IXPs that can then set their own membership policies. The governance would be improved by the government stepping back and facilitating a more multi-stakeholder approach to the IXPs.[22]

Finally, while the UAE-IX is an open IXP, and one of the largest in the region, it is in a Transit Zone, which is effectively off-shore. Only international entities can exchange traffic there, and traffic can only reach UAE customers through UAE operators. The IXP has brought definite benefits to the region, but the benefits do not fully flow into the country. The content hosted at the IXP and traffic exchanged there can only enter the country through the two national providers, Etisalat and du, which results in an increase in the cost of accessing the traffic, and limits the routing options, as discussed in the next use case.

International Gateway Competition

While all the countries have at least partially liberalized their retail markets, both mobile and fixed, in several there is little or no wholesale competition, particularly at the International Gateway, where the incumbent has market power, through a combination of owning capacity in the submarine cables, or the landing stations, or the only license. The result is not just that the cost of international IP transit is higher, but also that all international traffic must route through one or several operators.

As noted above, in the Middle East the fixed incumbents are state-owned, and the lack of wholesale competition benefits them, but results in higher costs for downstream ISPs. This is particularly the case in Egypt and Saudi Arabia, where there is only partial competition, and in UAE, where there is a duopoly of operators.

The market power at the gateway harms several critical properties.

- **Critical Property 1: An Accessible Infrastructure with a Common Protocol.** The market structure imposes a barrier to entry for international and national backbone markets. Even where there is plentiful competition in submarine cable capacity, as is the case in Egypt, that infrastructure is not fully accessible to the ISPs in Egypt because they must largely route through the incumbent, Telecom Egypt, to access the submarine cable capacity of third-party operators.

[22] For more background on IXPs, see https://www.internetsociety.org/issues/ixps/publications.

- **Critical Property 3: Decentralized Management and a Single Distributed Routing System.** The market structure impacts the routing of the traffic between networks, in a way that is less efficient than it could be. Again, ISPs in countries with market power at the gateway must route their traffic through the companies with market power, who are also their competitors, centralizing the routing choices.

The remaining market power at the International Gateways reduces choices for ISPs in those countries, and also operators outside those countries seeking to reach customers in the country. In addition, the prices are generally higher as a result of the lack of competition, which raises the cost of access for users in the country. This is particularly costly in countries without IXPs or significant presence of international CDNs, because most content is then accessed from abroad at high IP transit costs.

Conclusion

The global governance of the Internet is multi-stakeholder, including the technical community, the private sector, academia and research, and the government. All stakeholders play a role, depending on the issue and the venue, and none have ownership of any issue. It is in this environment that the critical properties of the Internet Way of Networking developed that have enabled the Internet to evolve and thrive. The Internet is meant to be accessible, have an open-architecture, a decentralized management, and be general-purpose.

As a decentralized ecosystem, the Internet continues to evolve in significant ways. For instance, Internet exchange points (IXPs) arose as a way for providers to exchange traffic with one another in an efficient way. In the early days, these providers were mainly ISPs, exchanging traffic on behalf of their wholesale customers and end-users. As content grew in significance and traffic volume, content providers began to create their own CDNs and connect directly to IXPs where they could. As the Internet began to globalize, so did the spread of ISPs, CDNs, and IXPs.

Government policies play an important role in the development of the Internet in their country, both directly and indirectly, as can be further demonstrated with the case of IXPs. At the most basic level, in many countries, ISPs require licenses to operate and deliver Internet access. Further, an IXP is only needed when there are multiple ISPs to exchange traffic, and thus liberalization of the market is an important precursor to the need for a local IXP. Finally, without intermediary liability protections, CDNs are reluctant to host third-party content in a country. While government action is needed to initially create the opportunity for these developments, then the multi-stakeholder Internet governance model can develop.

Government policy nevertheless can have an ongoing impact on Internet governance, impacting the provision of networks and availability of content and services. Broadly speaking, policy can be driven by economic or social considerations. Governments generally seek to improve economic conditions in their countries, and provide social protections for their citizens. These imperatives – economic and social – clearly drive the six issues described above in the Middle East countries examined.

- **Data Localization.** The reason for Data Localization of sensitive information including financial and health data is often social, for privacy and data protection of citizens, while there may also arguably be an economic incentive to develop or protect a local data market.
- **VoIP Bans.** The incentive behind these bans is clearly economic, to protect the revenues of licensed telecom providers, both mobile and fixed. In the Middle East countries, where the fixed incumbents are state owned, there is a direct revenue benefit for the government.
- **Internet Shutdowns.** The reasons used to justify shutdowns are in social terms, during times of unrest and protest.
- **Content Filtering.** Similar to the reasons used to justify Internet Shutdowns, content may be filtered based on social terms, relating to cultural or political restrictions on expression.
- **IXP conditions.** IXPs can enable content providers and other organizations to directly exchange traffic without having to purchase transit. The IXP can thus be a viewed as a way to reduce reliance on the incumbent from buying transit, and thus governments that do not develop or authorize an IXP or restrict its usage may be driven by economics.
- **International Gateways.** The International Gateways in the countries where there is little competition are controlled by the fixed incumbent, and thus help to support the revenues on those operators.

We have discussed the impact of these social and economic interventions on the critical properties of the Internet. The impact on end-users is not abstract. Protection of the state-owned incumbent keeps prices high, ultimately limiting adoption and usage of the Internet. Limiting the services available in a country limits choice for end-users, which is particularly impactful during the lockdowns, while a shutdown can have significant impacts on the benefits of the Internet across society and the economy. Further, restricting an IXP can impact the resilience of the network, while not having an IXP hinders resilience even more so.

Full liberalization of Internet markets lowers prices and increases choices. Without Data Localization, companies can still protect data privacy while storing and processing data efficiently.
As demonstrated by the European GDPR, governments can still control the conditions under which data is transferred to other countries. VoIP enables customers choices of low cost or free calling, with new features and services. Eliminating shutdowns or removing filters can ensure continual access to the Internet services that are an integral part of society. Removing barriers at International Gateways and within IXPs will help to lower the cost of access and latency for traffic exchange and make the Internet more resilient.

The benefits of the Internet for users, businesses, and government services are significant and growing. Internet access has been critical during pandemic lockdowns, and will help countries to rebound when the pandemic is over. Countries in MENA that address the issues covered in this paper and promote the Internet Way of Networking will increase the economic and social benefits that the Internet delivers their citizens.

Use Case	CP1: An Accessible Infrastructure with a Common Protocol	CP2: Open Architecture of Interoperable and Reusable Building Blocks	CP3: Decentralized Management and a Single Distributed Routing System	CP4: Common Global Identifiers	CP5: A Technology Neutral, General-Purpose Network
Data Localization	Raise costs and entry barriers for relevant services	n.a.	May not be stored in the most optimal place	n.a.	n.a.
VoIP Bans	n.a.	Impacts interoperability of applications, undermining end-to-end principle	n.a.	n.a.	Networks would become less general purpose, and it limits apps that users can access through the networks
Internet Shutdowns	Disrupts the common platform while the infrastructure is not accessible	n.a.	Blocks routing of traffic and makes country inaccessible from outside	n.a.	Blocks what is available in other countries
Content Filtering	Restricts access to the open and accessible global Internet	n.a.	Centralized management of Content Filtering policies or facilities	Fractures the value of the global identifiers by blocking access to some of them	Using DPI to filter content complicates the role of network operators
IXP Restrictions	n.a.	n.a.	Impacts routing of traffic between networks (ISPs and CDNs)	n.a.	n.a.
International Gateway	Imposes barriers to entry for international and national backbone market	n.a.	Impacts routing decisions of networks in the country for international traffic	n.a.	n.a.