THE INTERNET IN THE MIDDLE EAST AND NORTH AFRICA:

A Study of Usage, Threats and Restrictions during the First Decade of the 21st Century

By Dr Tal Pavel

ALMA MATER EUROPAEA UNIVERSITY

THE INTERNET IN THE MIDDLE EAST AND NORTH AFRICA:
A Study of Usage, Threats and Restrictions during the First Decade of the 21st Century

Scientific monograph

Author: Tal Pavel Ph.D.

Reviewed by: Michel A. Calvo Ph. D., Krunoslav Antoliš Ph. D., George-Marius Şinca Ph.D., Ilin Savov Ph.D.

Translation and proofreading: Dominatus digital d.o.o.

Technical editing: Suzanna Mežnarec Novosel

Break and design: Tjaša Pogorevc, s. p.

Edition: 1st Edition

Location: Maribor

Publisher: Alma Mater Europaea University, Alma Mater Press

For the publisher: Ludvik Toplak, Emeritus Professor

Available at: https://press.almamater.si/index.php/amp/catalog/category/informacijske-vede

Year of issue: 2025

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 245091587
ISBN 978-961-7183-75-7 (PDF)

ALMA MATER
PRESS

THE INTERNET IN THE MIDDLE EAST AND NORTH AFRICA:
A Study of Usage, Threats and Restrictions during the First Decade of the 21st Century

By Dr Tal Pavel

Maribor, 2025

TABLE OF CONTENT

INTRODUCTION

The late 20th and early 21st centuries witnessed a rapid proliferation of digital technologies that revolutionised how individuals communicate, access information, and engage with the world. The Internet emerged as a powerful tool for democratising access to knowledge, fostering global connections, and amplifying diverse voices across borders. The Internet, a symbol of the information revolution, embodies ideals like freedom of expression, innovation, and openness. In contrast, the Middle East and North Africa (MENA) region is often characterised by traditionalism and bureaucratic structures that can restrict human rights and free speech. However, such generalisations fail to capture the region's complexities. In the MENA region, where historical legacies, religious traditions, and political complexities intersect, the Internet has played a pivotal role in shaping narratives, challenging power structures, and mobilising social movements.

Therefore, the Internet in the MENA involves a detailed exploration of the multifaceted relationship between the Internet and the socio-political landscape of the region, the opportunities and challenges presented by the Internet in the MENA region as a transformative communication medium that has had profound implications for information dissemination, social interactions, and political discourse in the region.

From the early days of dial-up connections to the era of high-speed broadband, the MENA region has witnessed a rapid transformation in its digital connectivity, with implications for education, commerce, governance, and social interactions.

The Internet's emergence as a powerful tool for mass communication reshaped public discourse in the MENA region. It provided a platform for previously private discussions, potentially challenging the legitimacy of MENA regimes in ways traditional media could not. Civil society organisations, human rights advocates, and online activists leveraged the Internet for social change and advocacy in the

MENA region by mobilising and resisting traditional power structures and amplifying marginalised voices.

Initial excitement around access and potential benefits like education and economic growth was met with challenges. Uneven infrastructure left some countries behind, while limited Arabic content created a barrier. Governments, initially cautious, saw both risks and opportunities.

Indeed, the Internet reshaped governance structures and political dynamics in the MENA region, with governments responding to the digital revolution's challenges and opportunities. From online censorship and surveillance debates to digital rights and privacy protections, the MENA region has become a battleground for competing visions of the Internet's role in society, with implications for freedom of expression, access to information, and civic engagement.

While MENA countries embraced the Internet's economic, political, and social benefits, their governments also sought to mitigate potential consequences, primarily those related to political dissent, social unrest, and financial concerns.

This tension defined the era. Filtering and restrictions aimed to control harmful content, sparking censorship concerns. Despite these limitations, various local and international countermeasures emerged to enable free Internet access even during governmental restrictions.

The decade between 2000 and 2009 laid the groundwork for the Internet's future role in the MENA region. Despite infrastructure limitations, government restrictions, and limited content challenges, we have witnessed a significant rise in internet access during this period. As the decade progressed, mobile phone adoption, content localisation efforts, and digital literacy initiatives began to shape a more dynamic internet landscape. The tension between government control and the desire for an open internet would continue to define the region's digital future. By the decade's end, the groundwork was laid for a future Internet landscape in the MENA region, one still grappling with the balance between control and openness.

The book aims to provide a comprehensive overview of the historical context, technological developments, cultural dynamics, and governance challenges that have shaped the digital ecosystem in the MENA region. By delving into the complexities and nuances of Internet usage in the MENA region, this document aims to provide a holistic understanding of the opportunities, risks, and implications of the digital revolution in one of the world's most dynamic and diverse regions.

PART A – ENCOURAGEMENT: THE HISTORY

Chapter 1 - The Internet in the MENA

The Internet arrived in the MENA region in the early 1990s and experienced significant growth in the following decade. Tunisia pioneered Internet access in 1991, followed by Kuwait in 1992. Egypt, Turkey, Iran, and the United Arab Emirates (UAE) joined in 1993. Jordan and Saudi Arabia gained access in 1994, followed by Bahrain (1995), Qatar (1996), Sudan and Syria (1997), and Libya (1998) (D. L. Wheeler 2004).

The first decade of the 21st century (2000-2009) witnessed a surge in internet usage in the MENA region. Growth rates averaged a staggering 1,648 %, significantly exceeding the global average of 380 per cent. By 2009, internet penetration in the MENA region reached around 28 per cent, surpassing the global rate of approximately 26 per cent. This achievement occurred even though MENA users constituted only 3.3 per cent of international users.

However, internet penetration within the MENA region itself varied considerably. The Persian Gulf countries boasted rates exceeding 50 per cent, while Iraq and Yemen lagged at a mere one per cent.

The high Internet penetration rates in many MENA countries are unexpected, considering the region's lower Internet user base than the global average (3.3 per cent). Unlike Western countries, where penetration has matured, the MENA region likely possesses significant room for further growth. This contrasts with regions like Europe, North America, and Australia, where high penetration rates are accompanied by slower growth.

Internet penetration within the MENA region varied considerably. Some countries, like the UAE, with a 61 per cent penetration rate, approached saturation, experiencing a slower growth rate of 298 per cent from 2000 to 2009 (one of the lowest in the region).

In contrast, other countries exhibited explosive growth. Iran and Syria witnessed the highest surges, with penetration rates increasing by 12,780 per cent and 11,783 per cent, respectively (from 30,000 to 3.56 million users in Syria). These countries emerged as regional leaders in Internet adoption.

A 1999 study revealed that a young demographic dominated the Internet user base in the Middle East. Seventy per cent of users fell between the ages of 21 and 35, starkly contrasting with only 4.5 per cent exceeding 45 years old. The UAE exemplified this trend, with an average user age of 27.

Early Internet access in the region often relied on Internet cafes. In Sudan, for instance, these cafes were predominantly male spaces. While families might occasionally use a single computer together, societal norms often discouraged women from visiting cafes alone, especially during evenings when crowds were more prominent. This perception varied geographically and temporally.

Overall, Internet users in the MENA region during this period were primarily young (15-35 years old), better educated, and concentrated in capital cities. High costs outside major urban centres limited Internet access for many.

In pursuit of regional technology leadership, **Bahrain** heavily invested in communication infrastructure and services through its state-owned telecommunications company, Batelco. Batelco held a dominant market position, controlling 75 per cent of the cellular and 90 per cent of the wired telephony markets. Their investments targeted three key areas: mobile, broadband, and information systems and technology.

To solidify its position as a regional technology leader, Batelco announced a series of investments in 2003 to bolster communication infrastructure. These investments targeted upgrades to Internet connectivity and cellular networks. Specifically, Batelco, a major telecommunications company in Bahrain, planned to (Bahrain Tribune 2005b; 2005c):

- **Enhance communication infrastructure** between Bahrain and significant global cities by 2006, aiming to improve Internet speed and availability for broadband users (private and business customers).
- **Expand and improve the cellular network** across Bahrain.

Furthermore, Batelco committed to cost reduction initiatives in 2005. These initiatives included:

- **A 50 per cent reduction in Internet connectivity costs** for small and medium-sized businesses (SMBs) utilising ADSL.
- Lowered prices for international dialling and calling cards.

Bahrain distinguished itself by achieving one of the highest Internet penetration rates in the region, reaching 55 per cent by 2009. This impressive figure was nearly double the regional average. While the country's Internet usage growth rate from 2000 to 2009 remained significant at 907 per cent, it fell short of the staggering regional average of 1,648 per cent. This discrepancy can be attributed to two factors: (1) Bahrain's already high starting point with Internet penetration. (2) Its role as an alternative Internet access point for some Saudi Arabian citizens.

Data from the early 2000s reveals Bahrain's leadership in technology adoption within the MENA region. The country boasted the second-highest Internet penetration rate behind the UAE, with both nations significantly exceeding their MENA counterparts.

Bahrain's dominance extended to other key metrics. Among the 17 MENA countries analysed, it possessed the highest number of mobile phones and the highest human capital index per thousand people. Notably, Bahrain's computer ownership rate per capita (160.4 per thousand) rivalled Qatar's (180.3) and surpassed developed nations like the UAE (135.5) and Kuwait (119.6).

Egypt's position as a regional leader in media and communication technologies aligns with its broader role as a political and cultural power in the MENA region. This leadership has manifested in the government's active promotion of new

mass communication technologies, including radio, television (particularly satellite), telephones, and computers, especially among the student population (Abdulla 2005a).

In October 1993, Egypt established its first Internet connection. This initial link connected the Egyptian Universities Network (EUN), managed by Cairo University, to France with a bandwidth of 9.6 kilobits per second (kbps). At the time, with a population of approximately 63 million, Internet subscribers ranged from 2,000 to 3,000, with university users constituting the majority (S. Kamel 1997).

In 1994, Egypt implemented a structured approach to its Top-Level Domain Country Code (.eg) by dividing it into three main categories (Saleh 2003):

- **Academic institutions:** Websites belonging to universities used the "eun.eg" subdomain (e.g., Egyptian Universities Network), and research institutions used "sci.eg."
- **Commercial entities:** These websites used the “com.eg” subdomain.
- **Government websites:** Government entities were assigned the "gov.eg" subdomain.

Commercial Internet access remained unavailable initially. The sole Internet service provider (ISP), In-Touch, could only offer email services by connecting to a US server, resulting in high usage costs. However, a significant infrastructure upgrade in September 1994 increased Internet speed from 9.6 kilobits per second (kbps) to 64 kbps. This improvement opened the door for non-governmental organisations and private businesses to connect, transitioning the Internet from a purely academic resource to a public one (T. Kamel 1997).

1995 marked a turning point for Internet access in Egypt. The government launched the ambitious “Information Highway Project” with three key objectives:

- **Developing fast communication networks:** This aimed to improve Internet infrastructure nationwide.

- **Enhancing online information security** by creating secure online data storage and communication environments.
- **Building a skilled workforce:** The project aimed to develop human resources capable of supporting and maintaining the information highway, potentially including IT specialists and engineers.

Significantly, 1995 also witnessed the arrival of private Internet service providers (ISPs) in Egypt. Telecom Egypt, the state-owned telecommunications company, announced licensing 12 private ISPs, fostering competition and potentially lowering user costs.

These initiatives yielded positive results. By 1996, Internet speed had increased twentyfold compared to 1993, and the number of users had reached 20,000. This rapid growth underscored the Internet's potential in Egypt.

President Mubarak's 1999 decision to further expand Internet access solidified Egypt's commitment to the digital revolution. This move aimed to establish Egypt as a regional Internet hub and a significant software exporter, highlighting the government's vision for a technology-driven future.

Government efforts diligently fostered Internet development in Egypt. By 2000, the country boasted roughly 100 competing ISPs. This competitive landscape and low communication costs significantly democratised online activity despite a national Internet penetration rate of only 3 per cent.

The Egyptian government launched a free Internet initiative in early 2002 to bridge the digital divide. This initiative aimed to improve Internet accessibility for residents by:

- **Enabling affordable personal computer purchases:** The program involved subsidies or discounts on computers, encouraging user adoption.
- **Free Internet access:** A unique feature allowed users to access the Internet through any ISP in the country, with phone call charges being the only cost. This service became available in 23 out of 26 districts by 2002.

Despite a national literacy rate of only 50 per cent, this initiative significantly increased the number of Internet users and fostered greater competition among ISPs. However, it is essential to note that concurrent with these developments, the government-initiated Internet monitoring practices in 2001, targeting "inappropriate or susceptible materials".

Limited public awareness and insufficient education levels posed significant barriers to Internet adoption in Egypt during the early 2000s. A 2003 UN survey on global e-governance readiness underscores this point. The survey assigned Egypt a human capital score of 0.62, indicating a relatively low level of preparedness compared to other Arab countries (scores ranged from 0.48 to 0.84). Only Morocco, Sudan, and Yemen scored lower.

Furthermore, the survey ranked Egypt 140th globally in e-governance readiness, surpassed by all but three Arab countries: Sudan, Yemen, and Libya. Interestingly, despite possessing nearly five times more personal computers, 50 times more landline telephones, and eight times more cell phones per capita than Libya, Egypt lagged significantly in Internet penetration (8.5 users per thousand compared to Libya's 109). This anomaly suggests Libya may have had a more educated population, as evidenced by its top ranking in human capital development among the 17 Arab countries surveyed.

Data from the early 2000s reveals interesting disparities in Internet adoption between Egypt and Syria. While both countries possessed similar numbers of personal computers and landline phones per capita, Egypt boasted a more than five times higher mobile phone penetration rate than Syria's. This suggests a potentially more mobile and tech-savvy population in Egypt.

Despite Syria's advantage in human capital development (as indicated by a higher human capital rate), Egypt's Internet usage rate surpassed Syria's by more than double. This could be attributed to several factors, including Egypt's greater government openness towards Internet accessibility.

However, it is essential to note that Egypt's e-commerce readiness lagged behind its Internet usage. An annual survey on online trade readiness placed Egypt at 53rd out of 65 countries in 2005, down from 51st in the previous year.

Egypt witnessed a significant surge in Internet users between 1999 and 2004. The number of users grew tenfold, reaching 4 million by 2004. Interestingly, estimates suggested an average of eight users per Internet account at the end of this period. Students aged 16-28 comprised a significant portion (over 40 per cent) of the user base.

Regarding Internet penetration, Egypt positioned itself as a regional leader within Africa. By 2004, it boasted a national penetration rate of 6 per cent, accounting for 17.6 per cent of all African Internet users. This placed Egypt well above the continental average of 2.7 per cent. Similarly, Egypt surpassed the Middle Eastern average of 8.6 per cent penetration.

Looking at a broader period (2000-2009), Egypt's Internet usage growth remained impressive. It experienced a staggering 2,693 per cent increase, significantly outpacing the growth rates observed in Africa (1,392 per cent) and the Middle East (1,648 per cent)('iilaf 2004b).

Data from ISPs in Egypt and a 2000 survey provided a snapshot of the average Internet user in 2000 (Abdulla 2005a):

- **Demographics**: Men comprised two-thirds of users, primarily utilising the Internet for social networking. Women, on the other hand, tended to focus on information gathering and dissemination. Households and small to medium-sized businesses collectively comprised half the user base.
- **Location**: A significant geographic disparity existed, with 80 per cent of users residing in Cairo and the remaining 20 per cent concentrated in Alexandria.
- **Usage Patterns**: Most Internet activity occurred during leisure hours, particularly before and after work schedules. Interestingly, half of all users engaged in interactive communication.

- **Internet Applications**: The Internet served various purposes, including entertainment, communication, software downloads, access to news, online shopping, education, and business.
- **Usage Duration:** A quarter of respondents reported using the Internet for less than 15 minutes daily.

The **Iranian** government has actively promoted the development of the country's technology and Internet sectors over the years. This commitment manifested in various initiatives:

- **Infrastructure Development:** Investments poured into improving telephony infrastructure and communication and information systems.
- **Governmental e-Services:** Launch of the first governmental e-payment (Islamic Republic News Agency (IRNA) 2005a) and e-trade (Islamic Republic News Agency (IRNA) 2005d) centres alongside official websites (Islamic Republic News Agency (IRNA) 2005c; 2005e) For state institutions and religious entities.
- **Promoting E-commerce:** Signing an e-commerce Memorandum of Understanding (MoU) and hosting the International Exhibition on Trade Electronic and Computer Electronic.
- **Leadership Involvement:** Statements and personal involvement of government leaders in speeches advocating for technological advancement and Internet access (Islamic Republic News Agency (IRNA) 2005g).
    - Examples included the president's advisor's report on implementing electronic money (Islamic Republic News Agency (IRNA) 2005h), the announcement of increased fixed phone lines (Islamic Republic News Agency (IRNA) 2005f), and investments in the IT sector (Islamic Republic News Agency (IRNA) 2004a).
    - The Foreign Minister opened an Internet Training Center (Islamic Republic News Agency (IRNA) 2004b), while the Majlis Speaker visited Internet website offices (Islamic Republic News Agency (IRNA) 2005b).

These initiatives demonstrate the Iranian government's dedication to fostering a robust technology and Internet landscape. Concurrently, Iranian leaders issued statements emphasising responsible Internet use and highlighting their commitment to promoting the nation's values and cultural heritage online (Islamic Republic News Agency (IRNA) 2004d; 2004c).

Given its solid foundation in information systems, Iran's potential to become a major Internet player in the Middle East was undeniable. The country benefited from a young, educated, and tech-savvy population that readily embraced the Internet in 1997.

Furthermore, significant investments were made in connecting cities with fibre-optic cables, leading to a dramatic surge in Internet usage. According to a report, the number of Internet users in Iran grew tenfold between 2000 (approximately 625,000 users) and President Khatami's second term ended.

This period also witnessed a rapid proliferation of Internet cafes, particularly in the latter half of the decade, further bolstering Internet accessibility (Rubin 2019).

A 2003 UN survey evaluating the e-governance readiness of 173 countries revealed that Iran ranked 107th. This placed Iran behind regional peers like the UAE (38th), Bahrain (46th), and Jordan (63rd).

This disparity is evident in several metrics. Iran possessed half the number of personal computers per capita compared to the UAE. Furthermore, its Internet user penetration rate stood at only 4 per cent (approximately 15,557 users per thousand people) compared to the UAE's significantly higher rate of 36.7 per cent (or 367,380 users per thousand people). Data from the early 2000s reveals a limited disparity in telephone lines per capita between Iran (199.5) and the UAE (341.8). Additionally, human capital levels appeared comparable in both countries (0.75 in Iran and 0.74 in the UAE). These factors suggest that limitations in technological infrastructure or user proficiency were unlikely to be the primary reasons behind Iran's lower Internet user base.

Iran's local communications industry rapidly developed in the early 2000s. The number of ISPs within the country surged to 683 by 2005. Telephone line penetration increased significantly, from 23.06 per cent in March 2004 to 27.13 per cent in July 2005.

However, despite these strides, Iran's performance in an annual survey assessing online trade readiness slipped slightly. The country ranked 59th out of sixty-five in 2005, down from 57th in the previous year.

Iran experienced impressive growth in Internet usage between 2000 and 2005. Its usage rate surged by 2,100 per cent, ranking second only to Syria (2,566.7 per cent) in the Middle East. This remarkable growth surpassed the regional average of 392.1 per cent by more than five times.

However, Iran's Internet penetration rate remained low despite this rapid increase. In 2005, it stood at just 8 per cent, significantly lagging regional leaders like the UAE (36.9 per cent), Kuwait (23.7 per cent), and Bahrain (21.6 per cent). It is worth noting that Iran's penetration rate did align with the overall Middle Eastern average of 8.6 per cent (ITP 2004).

Iran, a burgeoning Internet power in the MENA region, witnessed phenomenal growth in Internet usage between 2000 and 2009. Its usage rate skyrocketed by a staggering 12,780 per cent, far exceeding the regional average of 1,648 per cent. This remarkable achievement placed Iran at the forefront of Internet adoption within the MENA region.

This growth can be attributed, in part, to Iran's high human capital level. Additionally, the Internet became a vital communication tool for domestic and international actors. By the end of the first decade of the 21st century, Iran's Internet penetration rate had climbed to 34.9 per cent, solidifying its position as the third highest in the region, behind only Turkey and the UAE.

Despite a robust technological infrastructure and an educated population seeking information and global connection, these statistics highlight the ongoing

tension between Internet accessibility and government restrictions in Iran (The Open Research Network 1999).

Under Saddam Hussein's regime in **Iraq**, severe restrictions stifled personal freedoms, including freedom of expression and Internet access. The government closely monitored all Internet traffic, limiting usage primarily to government officials. Dial-up connections were the only method available for citizens to access the Internet.

However, the arrival of US forces in Iraq marked a significant shift. The US Department of Defense actively expanded Internet access by investing USD 165 million in establishing Internet cafes. This initiative significantly increased the number of cafes, from only 36 in 2004 to 170 by mid-2006 (OpenNet Initiative 2009b).

A mid-2005 report by an Iraqi blogger revealed that Internet cafes in the capital offered high-speed Internet access, various software programs specifically designed for Internet use, and even webcams. Notably, these cafes implemented privacy measures by installing partitions on the sides of computer screens.

The blogger further observed a significant rise in online activity among Iraqi Internet users during the period under review. This newfound access empowered users, particularly young women who exhibited high proficiency in using the Internet and maintaining email accounts.

The Internet emerged as a platform for Iraqis to document various aspects of life in their country. Internet users and bloggers actively uploaded content, including videos on YouTube, depicting the presence of American forces and the attacks they faced. It is important to note that a significant portion of this user-generated content originated from Islamic extremist groups. Their uploads primarily focused on showcasing attacks, ambushes, sniper fire, and mortar attacks targeting both foreign and local forces.

Despite a staggering 2,300 per cent growth rate in Internet connectivity by the end of 2009, Iraq's Internet penetration remained the lowest in the Middle East, with only 1 per cent of the population having access.

Jordan entered the Internet age in 1995, but initial access was limited to government and academic institutions. Recognising the potential for economic growth, the government transitioned the Internet to the public domain by 1996. Despite these early efforts, Jordan's Internet penetration rate remained low by 2009, reaching only 24 per cent. This placed Jordan at a similar level to Lebanon (23.5 per cent) but significantly lower than regional leaders like Iran (48.5 per cent) and the UAE (61 per cent). Notably, Jordan's Internet penetration rate experienced a growth rate of 1,078 per cent during this period (Internet World Stats, n.d.).

Jordan, despite boasting the highest literacy rate in the Arab world, faces challenges in achieving widespread Internet access. A primary constraint is affordability – the cost of Internet connectivity and computers remains out of reach for many citizens due to relative poverty.

Furthermore, the concentration of ISPs in the capital city limits the geographical distribution of Internet use and potentially empowers centralised government control. Outside the capital, access options were often limited to slow and expensive international dialling.

Despite these obstacles, Jordan exhibits unique potential for Internet development within the region. Like Arab countries, it actively promotes Internet use while enacting appropriate regulations and legislation to balance accessibility and mitigating potential risks associated with unrestricted online access.

Although Jordan implemented specific restrictions on Internet use, its popularity within the country remained undeniable. The widespread presence of Internet cafes was a strong indicator of this high demand. A November 2002 news report, citing the city of Irbid, claimed it held the Guinness World Record for »the most Internet cafes in a single kilometre.« This anecdote highlights Internet cafes' significant role in facilitating Internet access for Jordanians (Gomes 2002).

Further evidence of the Internet's popularity in Jordan came from the user demographics. Notably, women comprised nearly half (around 250,000) of the estimated 500,000 Internet users in Jordan by the end of 2002 (Arab Club for Media and Information Technologies 2002).

A 2003 UN survey evaluating e-governance readiness rated Jordan positively. The country ranked third among 17 assessed nations, demonstrating its strong foundation for using technology in government operations.

However, when examining communication infrastructure metrics, Jordan lagged some regional peers. This survey considered the number of personal computers, Internet users, telephone lines, mobile phones, and television sets per thousand people. While Jordan excelled in e-governance readiness, it fell short in its overall communication infrastructure development compared to most Gulf countries and some other Arab nations.

Jordan held the third position regarding human capital development, following Bahrain and Qatar. This indicates a well-educated population, a potential asset for further advancement in the technology sector.

Libya entered the Internet age in 1998, but initial access was restricted to a select group with close government ties. However, the government embarked on several initiatives to expand Internet accessibility. These efforts included lowering connection costs, permitting private sector investment in information systems, and offering information technology training programs.

Reports attributed a four hundred per cent increase in Libya's economy to these actions. However, it is essential to note that establishing a causal relationship between Internet access and economic growth is complex and requires further investigation (The Arabic Network for Human Rights Information, n.d.-b).

Following initial restrictions, Internet access in Libya became available to the public in 2000. By mid-2003, the country had an estimated 850,000 Internet users, a notable figure considering the country’s population of around six million.

The government actively fostered broader Internet access by establishing nearly 3,000 access points nationwide, including public Internet centres and private Internet cafes. Notably, by 2004, Libya boasted seven hundred Internet cafes, reportedly matching the combined total of Egypt and Kuwait.

In 2009, Libya's Internet penetration rate was 5 per cent, slightly lower than the African continent's average of 6.8 per cent. Libya witnessed a remarkable surge in Internet usage between 2000 and 2009. The country's Internet user base grew by a staggering 3,130 per cent, significantly outpacing the regional average of 1,648 per cent and surpassing the African average of 1,392 per cent (D. L. Wheeler 2004; Internet World Stats, n.d.).

A 2003 UN survey evaluating e-governance readiness worldwide revealed a paradox in Libya's approach to information technology. While the country had undertaken efforts to expand Internet access, its communication infrastructure remained underdeveloped.

The survey data presented a mixed picture. On the one hand, Libya ranked last among MENA countries in several key metrics, including Internet usage, total communication indicators, and the number of personal computers, telephones, and mobile phones per capita. Only Yemen, Sudan, Syria, and Algeria fared worse in some categories.

However, the UN survey also revealed a bright spot in Libya's Internet development. The country boasted the third-highest Internet user penetration rate per capita (measured as "persons online") within the MENA region, trailing only the UAE and Bahrain.

This impressive figure, exceeding Jordan's by a factor of three, Saudi Arabia's by four, and Egypt's by nearly thirteen times, highlights the potential impact of the government's initiatives. These initiatives, including cost reduction measures and training programs, contributed significantly to the rapid growth of Internet users.

Qatar's Internet journey began in 1996 when state-owned telecommunications company Q-Tel introduced the service. Initial uptake was slow, with fewer than 2,000 subscribers in the first year. However, the user base grew steadily, reaching 9,000 by 1999, 11,000 in 2001, and nearly 100,000 by May 2003. This growth trajectory continued, with Internet subscribers reaching 115,000 by 2004, representing a significant portion of Qatar's population of approximately 600,000.

The Qatari government's decision to allow private companies into the Internet service provider (ISP) market shortly after that proved instrumental in driving Internet penetration. This move spurred a steady rise in Internet users throughout the country. By 2005, Qatar boasted a robust Internet penetration rate of 21.5 per cent, significantly exceeding the regional average of 8.6 per cent.

Furthermore, Qatar's Internet usage growth rate between 2000 and 2005 was exceptional. It surged by an impressive 450 per cent, surpassing the Middle East region's average growth rate of 392.1 per cent. This remarkable achievement positioned Qatar as a regional Internet adoption leader (The Arabic Network for Human Rights Information, n.d.-d).

Qatar has emerged as a leader in information and communication technology (ICT) infrastructure. A UN survey evaluating e-governance readiness among seventeen regional countries placed Qatar within the top half for most assessment components. Notably, the country secured the top three spots regarding television receivers, telephone lines, and cell phone subscriptions per capita.

The UN survey further underscored Qatar's strong ICT foundation. The country possessed the highest number of personal computers per capita among all 17 Arab nations. While its Internet user penetration rate ranked fourth behind the UAE, Bahrain, and Libya, Qatar still achieved an impressive position.

Furthermore, the survey results indicated a well-educated population in Qatar, reflected in its fourth-highest human capital ranking. However, Bahrain, Libya,

and Lebanon held the top three positions in this category (Privacy International and the GreenNet Educational Trust 2003).

Saudi Arabia entered the Internet age in 1994, but initial access was restricted to government institutions, universities, medical facilities, research centres, and foreign businesses. For ordinary citizens, personal Internet access remained limited (Gardner 1998). While residents could purchase personal computers, connecting to the Internet proved challenging and expensive. They faced two options, neither ideal (Burkhart 1998; Human Rights Watch 1999b).

- **Dial-up access to ISPs in neighbouring countries:** This method incurred high international call charges.
- **Local networks like naseej.com.sa:** These offered email services, access to local databases, and chat rooms, but crucially, no direct Internet access.

In 1997, a significant shift occurred with the approval of public distribution of Top-Level Domains (TLDs) and public Internet access. However, implementation remained cautious. It was not until January 1999 that seventy-one selected local ISPs, primarily affiliated with the government, began offering Internet connections to the public. This marked the official launch of public Internet use in Saudi Arabia.

The delay in offering widespread Internet access stemmed from the government's desire to implement content filtering mechanisms. This aimed to restrict citizens' access to information deemed undesirable.

Recognising the Internet's potential to contribute to national development projects, Saudi Arabia has actively promoted Internet use. This policy shift came in response to the surging public demand for broader Internet access and associated services, particularly from the business sector. Consequently, the Kingdom embarked on several initiatives to develop its communication infrastructure and expand Internet deployment throughout the country.

In 1999, Saudi Arabia boasted an estimated 45,000 Internet subscribers, reflecting a surge in demand following the official launch of public Internet access. This

figure represented a threefold increase in users compared to the pre-public access period, highlighting the pent-up demand for Internet connectivity.

It is worth noting that even before official public access, tens of thousands of Saudis accessed the Internet through neighbouring countries like Kuwait, the UAE, and Bahrain. This underscores the pre-existing desire for Internet connectivity.

Following the launch of public access, Saudi Arabia's Internet penetration rate reached 27 per cent, aligning with the regional average of 28 per cent. However, the kingdom possessed the most significant absolute number of Internet users in the Arab world (representing 13 per cent of the population), trailing only Iran's significantly higher rate of 56 per cent.

Between 2000 and 2009, Internet use in Saudi Arabia witnessed a remarkable surge. User numbers grew by a staggering 3,750 per cent, significantly surpassing the regional average growth rate of 1,648 per cent.

However, despite government announcements in July 2002 of reduced Internet usage costs by 42-78 per cent, affordability remained a concern. The Internet connection cost appeared unchanged, ranging between USD 74 and 112 per month during this early period.

By 2004, the Saudi Arabian market absorbed a significant portion (40 per cent) of the total regional imports of software and equipment for the information systems industry. This robust demand fuelled a 15 per cent annual growth rate within the kingdom's information systems sector, solidifying its position as the leading consumer in the Arab world (OpenNet Initiative 2004b; Abdel Hameed 1999).

In 2003, Saudi Arabia possessed an estimated sixty-three personal computers per thousand people. While this figure represented nearly half the rates observed in Kuwait and the UAE, it nonetheless positioned the kingdom ahead of Oman (with roughly half the number) and significantly surpassed Morocco, Syria, and Egypt (where penetration rates were a quarter or even less).

A 2003 UN survey evaluating e-government readiness positioned Saudi Arabia in the middle rankings. The country ranked 105th globally and ninth among the 17 Arab countries assessed. Similarly, in a separate annual survey measuring readiness for online trade conducted in 2005, Saudi Arabia secured 46th out of sixty-five countries, demonstrating improvement from 48th place in 2004.

Despite being one of the later adopters of Internet access in the region, Saudi Arabia has exhibited promising strides in developing its digital infrastructure since its introduction.

Sudan initiated a communications liberalisation process in 1991. However, Internet access in the country remained unavailable until May 25, 1997, following a period of political liberalisation. This marked the arrival of the first Internet signal, as evidenced by the successful transmission of a ping command.

The development of Internet infrastructure was uneven across Sudan. While the capital, Khartoum, witnessed a rapid rollout, Internet access remained limited or absent in other regions (Network Startup Resource Center (NSRC), n.d.; El Bashir Mohamed 2005).

In 1996, the responsibility for managing the .sd TLD was assigned to a private company named Sudan On-Line. However, the domain remained inactive due to two fundamental limitations. Firstly, Internet service was not yet available in Sudan. Secondly, the TLD Company, established by a Sudanese citizen residing in the US, lacked direct engagement with the developing Sudanese Internet community (El Fatih El Tigani, n.d.). The growing interest in the Internet within Sudan spurred efforts to activate the country's .sd TLD. The newly established Sudan Internet Society (SIS), a non-profit organisation founded in December 2001, positioned itself as a critical player in this endeavour. As highlighted in a letter from the Sudanese Minister of Science and Technology to the Internet Corporation for Assigned Names and Numbers (IANA) president, the SIS actively advocated for assuming responsibility for managing the .sd domain (The Internet Corporation for Assigned Names and Numbers (IANA) 2002b). In January 2002, the Sudanese

authorities formally registered the Sudan Internet Society (SIS) as the official manager of the .sd TLD. IANA subsequently confirmed this authorisation by the end of 2002 (The Internet Corporation for Assigned Names and Numbers (IANA) 2002a). In January 2002, Sudanese authorities formally registered the Sudan Internet Society (SIS) as the official manager of the .sd TLD. IANA subsequently confirmed this authorisation by the end of 2002.

Despite government efforts to reduce taxes on personal computers in the early 2000s, Sudan remained the North African nation with the lowest per capita computer ownership rate. This excessive cost significantly restricted computer purchases, limiting access to a small population segment.

In 2000, Sudan registered approximately 2,000 Internet users. Government officials and various organisations comprised half of this initial user base, followed by business and commerce (30 per cent) and academia with research (20 per cent). Private individuals only accounted for a limited share (20 per cent).

However, Internet user numbers witnessed a significant expansion over the following years. By 2001, the total user base reached 15,000, with private individuals now representing 40 per cent. This trend continued, and by 2002, Sudan boasted an estimated 56,000 Internet users.

The most dramatic growth spurt occurred between 2002 and 2009. By the end of 2009, the number of Internet users in Sudan had exploded to a remarkable 4.2 million, representing a staggering 13,900 per cent increase. This surge signified a tenfold rise in Internet penetration, reaching 10 per cent of the population. However, it is essential to remember that this growth came from an extremely low baseline due to the earlier high cost of computers (Balancing Act, n.d.; The International Telecommunication Union (ITU), n.d.).

Numerous testimonies show that the early 2000s witnessed a proliferation of Internet cafes in the Sudanese capital, Khartoum. Usage costs ranged from USD 1 to 2 per hour, providing an affordable option for accessing the Internet.

However, these cafes faced significant challenges. Intense competition within the market and limitations in their technological infrastructure resulted in a high turnover rate.

Sudan's initial Internet expansion phase confronted significant infrastructure challenges. These challenges encompassed: (1) A robust and reliable electricity grid to ensure consistent power supply. (2) A dependable and high-quality communication network with nationwide coverage. (3) Educational programs to bridge the digital divide by familiarising the population with this entirely innovative technology.

A stark digital divide emerged between the capital, Khartoum, and the rest of Sudan. Internet penetration rates and the prevalence of Internet cafes were significantly lower in outlying regions. Limited infrastructure resulted in slower and unreliable Internet access, sometimes even complete absence. Consequently, hourly usage rates were considerably higher in these areas, discouraging the establishment of Internet cafes. Furthermore, the inconsistent stability of electricity and communication networks posed a significant barrier to consistent and affordable Internet use.

Given the existing deployment of Internet-connected computers, the potential for Internet usage within Sudanese academia could have been higher. However, this potential remained only partially realised due to inadequate training for faculty members and students, key stakeholders in the educational process.

Universities in Sudan did not offer students Internet access. Only Khartoum University and Ahfad University provided Internet connectivity exclusively for administrative purposes. Limited interest and demand for regular Internet use were observed among both students and academic staff. This can be attributed to dozens of untrained faculty members sharing a single Internet-connected computer, often with a restricted daily usage window of two hours.

The University of Sudan, however, presented a notable exception. By the end of 2000, all its faculties enjoyed 24/7 internet access through a local area network (LAN) connection (Balancing Act, n.d.).

On February 24, 1996, the **Syrian** Prime Minister's Office authorised the Syrian Telecommunications Establishment (STE) to spearhead internet integration. This mandate included connecting Syria to the internet and managing the.SY Top-Level Domain (TLD).

The initial phase focused on needs assessment, conducting pilot programs, and establishing the necessary infrastructure. To facilitate this process, the STE and the Syrian Computer Society (SCS), led by Bashar al-Assad, signed a cooperation agreement on March 11, 1996, to test Internet connectivity for government institutions.

The pilot program encompassed various aspects, including efficiency, cultural suitability, and potential security concerns. Following the pilot, researchers and experts presented a report to the STE and the Institute of Applied Sciences and Technology. This report highlighted the technical and administrative challenges of connecting Syria to the Internet.

However, the report concluded that swift Internet integration was necessary for Syria. The reasoning behind this conclusion was outlined in the report itself (Askhita 2000):

1. "The invaluable wealth of information and services it presents to students and researchers, as it has become a pillar of research worldwide due to the vast amount of information in online data banks.
2. The importance of the Internet for commercial advertisement and electronic commerce.
3. Syrian establishments can use the Internet to promote their products and publicise Syria's cultural, historical, archaeological, and tourist heritage.
4. Delivering the Syrian point of view in support of our stands and in defence of our rights to fill the wide gap and balance the misconceptions, lies, and deformed images of Syria presented by sites supported by international Zionism. In addition to the possibility of exposing the Israeli crimes and aggressions against Arabs via the Internet, which is becoming the most popular and influential media channel".

Following the report's recommendation for swift internet integration, Syria initiated plans for a pilot project. This project marked the first step in a series of initiatives to connect the country to the Internet and make it accessible to residents.

- **Pilot Project** – On November 17, 1997, Syria launched a pilot project to provide Internet access to 150 selected government entities. This initiative marked the country's first official Internet access program. It is worth noting that before this project, an estimated 65,000 Syrian residents already possessed Internet access through providers in neighbouring countries like Lebanon, Turkey, and Jordan. Additionally, some government entities in Egypt access the Internet via connections.

  The pilot project's initial phase encountered challenges due to high connection costs. These costs stemmed from a limited subscriber base, expensive equipment, and reliance on international Internet service providers. However, after seven months, improvements in hardware and communication infrastructure were made to address increased traffic demands.

  By the end of 1997, Syria possessed an estimated 35,000 personal computers, translating to a national penetration rate of two computers per thousand people. Nevertheless, many of these computers required upgrades to run modern applications (Alterman 1998).

The Syrian Telecommunications Establishment (STE) and the Syrian Computer Society (SCS) collaborated to design the architecture for the pilot project, which received approval from the Prime Minister. This architecture included essential hardware, notably a server for monitoring Internet activity, filtering content, and managing the network.

The project plan also outlined six key objectives, one of which focused on training local technical staff in monitoring, identifying, and blocking unwanted websites (Askhita 2000).

- **Public Access Project** – Building upon the pilot project's success and recommendations from the Syrian Computer Society (SCS), the Syrian Telecommu-

nications Establishment (STE) spearheaded the expansion of Internet access to the public in early 1999. This expansion project offered email services and basic Internet functionality like web browsing and file transfer within Syria.

The public access project launched in early 1999 offered two subscription tiers. Around 5,000 subscriptions were activated, with 3,000 users opting for the more comprehensive plan that included email and broader Internet access. By February 2000, the expanding access points resulted in an official user count of 6,000. However, this figure significantly underestimated actual usage.

Several factors contributed to the discrepancy. Institutions often employed a single server to connect multiple computers to a single phone line and subscription. Similarly, private users frequently shared accounts with friends and family. Considering these practices, estimates suggested a total user base of approximately 60,000, assuming an average of 10 users per subscription.

In October 2000, Internet access became officially authorised in Syria. However, full Internet access was initially limited to specific locations. These included two Internet cafes, the National Library, the Syrian Computer Society's Damascus offices, access points at Damascus airport, various private and public institutions (including commercial, industrial, and tourism agencies), one hundred schools, and select professionals such as doctors, engineers, and lawyers (Askhita 2000).

A 2003 UN survey found Syria lags behind most Arab countries in Internet usage and infrastructure preparedness. The survey ranked Syria near the bottom among 17 Arab nations, with only Sudan and Yemen scoring lower. Furthermore, Syria's Internet usage rate per capita was less than one per cent of that observed in the UAE.

Personal computer ownership in Syria also remained low. With 16.3 computers per thousand people, Syria possessed half the national penetration rate of Oman and Jordan, a quarter of Iran and Saudi Arabia, and less than a tenth of Bahrain and Qatar. Nevertheless, this figure was slightly higher than Egypt's and five times that of Libya.

A comparison of telecommunication infrastructure in Syria with other Arab countries in the early 2000s revealed a significant disparity. Syria ranked lowest in terms of both mobile phone and television penetration. With only twelve cell phones and 67 television receivers per thousand people, Syria lagged behind nations like the UAE (759 cell phones), Morocco (209 cell phones), and Egypt (67 television receivers). Iran (163 television receivers), Kuwait (486 television receivers), and Qatar (866 television receivers) also boasted higher ownership rates.

However, despite these limitations initially, Syria witnessed a steady rise in the penetration of wired and cellular communication technologies. This trend mirrored the country's increasing availability of personal computers and Internet access.

By 2004, Syria had experienced a remarkable surge in Internet usage, growing by 633 per cent. This impressive increase propelled Syria to the second-place position among Arab nations, trailing only Iran. The country reached an estimated total of 155,000 Internet users. The average home subscription-supported at least five users, and over five hundred Internet cafes provided additional access points.

These figures were particularly significant considering Syria's nascent state of Internet access. Public Internet access only started in 2002. Before this, many Syrian subscribers relied on providers in neighbouring countries to connect, a practice motivated by lower international communication costs. However, transitioning to local providers presented challenges due to limitations in the existing communication infrastructure. These limitations resulted in slow and expensive connections with extended wait times.

In response to these limitations, the authorities planned to expand the communication infrastructure to address these shortcomings and improve Internet quality.

By 2009, Syria comprised only 6 per cent of the total Middle East Internet users despite boasting an Internet penetration rate of 16 per cent. This figure starkly contrasted with the regional average of 28 per cent. This data revealed a signifi-

cant disparity in Internet usage between Syria and other MENA countries, exceeding the gap observed in other communication technologies and television.

Interestingly, Syria's education level remained comparable to that of the UAE and surpassed that of Egypt and Saudi Arabia. However, the country's low Internet penetration rate highlighted the prevalence of censorship and media control mechanisms. This suggested that the lower usage stemmed more from policy than technology or infrastructure.

Despite these access limitations, Syria witnessed a remarkable growth rate in Internet usage between 2000 and 2009. The country's user base surged by an impressive 11,783 per cent, ranking second only to Iran's 12,780 per cent increase. This growth significantly outpaced the regional average of 1,648 per cent.

Tunisia emerged as the North African leader in Internet development. The country implemented a series of initiatives to establish and expand Internet access, including reducing usage costs, lowering computer and equipment import taxes, upgrading telephony and Internet communication infrastructure, and encouraging the establishment of private and institutional ISPs.

Tunisia further bolstered its Internet presence by establishing a network of approximately three hundred institutional Internet cafes. Numerous government agencies actively maintained websites, fostering an online presence. Additionally, radio broadcasts and television programs were readily accessible via the Internet.

The government prioritised Internet access in education, equipping all universities, high schools, and scientific institutions with connectivity. Plans were in place to extend this access to elementary schools, further solidifying Tunisia's position as a North African Internet development leader (Human Rights Watch 2005a).

By 2009, Tunisia boasted an Internet penetration rate of 27 per cent, aligning with the regional average in the Middle East. This figure starkly contrasted with a significantly lower average of 7 per cent observed across Africa.

Tunisia's growth in Internet usage mirrored its leadership in development. Between 2000 and 2009, the country witnessed a surge of 2,700 per cent in its Internet user base. This impressive growth significantly outpaced the regional average of 1,648 per cent in the Middle East and surpassed the 1,392 per cent growth rate observed across Africa (Internet World Stats, n.d.).

The **UAE** launched Internet access services in 1995, initially targeting government entities, businesses, and educational institutions. Unlike many other countries, the UAE prioritised dedicated leased lines for Internet connectivity, bypassing the limitations of dial-up access.

Commercial interests, rather than political or educational institutions, played a dominant role in shaping the UAE's Internet history. Notably, Dubai and the UAE established free trade zones (Jebel Ali Free Zone and Dubai Multi Commodities Centre, etc.) that fostered the growth of the information technology (IT) sector. Companies within these zones significantly invested in modern technology and IT solutions to enhance their performance, efficiency, and service levels in this highly competitive environment.

Leading international IT providers recognised the UAE's potential and established branches in Dubai Internet City (DIC) to gain a foothold in the local market and expand their reach into the Middle East. This move resonated with the UAE's well-deserved reputation for embracing new technologies.

By 2004, the UAE's IT market exhibited signs of maturity. Reports indicated a shift, with investments in software and services surpassing hardware investments. Despite this trend, hardware still comprised 65 per cent of the total IT expenditure. However, the software and services sector witnessed the highest growth rate. This growth was driven by local small and medium-sized businesses (SMBs) implementing Enterprise Resource Planning (ERP) systems and expanding existing applications. Large companies, on the other hand, focus on IT solutions for customer relationship management (CRM), supply chain management (SCM), and business intelligence (BI).

In April 2002, a local UAE communications company significantly reduced its monthly Internet connection fee, making it the most affordable option in the Middle East. However, by the end of 2003, public concerns regarding high Internet costs resurfaced. This sentiment culminated in a user-led boycott campaign. The campaign gained traction and ultimately secured the support of the Minister of Culture and Information, who acknowledged that Internet connection prices exceeded global averages. This pressure from both users and the government ultimately reduced Internet costs (Emirates Internet and Multimedia 2002; The Arabic Network for Human Rights Information, n.d.-f).

In a 2003 UN global survey, the UAE emerged as the leader in e-governance preparedness among MENA countries. The survey assessed each nation's readiness for e-governance practices. The UAE secured 38th place globally and ranked first among 17 MENA countries in overall preparedness. This strong performance stemmed primarily from the country's success in two key index components: Web Measures and Communication infrastructure.

However, the UAE's dominance was not absolute. Notably, the country lagged behind Bahrain, Libya, Qatar, Jordan, and Iran in the human capital category, constituting one-third of the total readiness score. Despite boasting advanced technological and communication capabilities, the UAE's human capital scores, as measured by various indices (Human Development Index, Education Index, Adult Literacy Rate), mirrored those of other MENA countries. Moreover, these human capital indicators did not significantly improve, with some showing signs of decline.

While the UAE's human capital indicators showed a relative decline, the country maintained a robust telecommunications infrastructure. It boasted the highest landline and cellular communication network availability among all Arab countries. Additionally, the UAE ranked third in personal computer penetration, following only Qatar and Bahrain. These factors significantly contributed to the UAE's extensive Internet penetration rate, which surpassed those observed in other MENA countries by a considerable margin (Southwell 2004; Burkhart and Goodman 1998; Walters and Walters 2002).

Since the Internet's emergence in the Arab world, the Persian Gulf region has consistently demonstrated leadership in Internet usage rates. The UAE has consistently held the top spot for Internet penetration among Middle Eastern countries.

The UAE witnessed a remarkable surge in Internet users in its early development years. In mid-1997, the country had just 13,000 users. By 2001, this number had skyrocketed to an estimated 775,000, reflecting a subscriber base of approximately 240,000. This rapid growth continued, with EIM reporting a user base exceeding 995,000 by the end of 2002. Notably, the UAE surpassed Egypt in boasting the region's highest number of Internet accounts.

The UAE's impressive Internet infrastructure also garnered international recognition. In 2001, the International Telecommunication Union (ITU) acknowledged the country's position as the most networked Arab nation and one of the most connected globally.

The UAE's Internet penetration rate reached 61 per cent by 2009, a substantial achievement. However, the country's user base only comprised 5 per cent of the Middle East's total, ranking it third in the region behind more populous countries like Iran (56 per cent) and Saudi Arabia (13 per cent). Interestingly, the UAE's Internet usage growth rate from 2000 to 2009, at 298 per cent, paled compared to the regional average of 1,648 per cent.

The UAE witnessed a significant rise in personal computer penetration rates between 2005 and 2009, while landline phone penetration remained relatively stable, declining slightly from 291 to 275 phones per thousand people. This decline likely stemmed from market saturation with internet-enabled devices like personal computers and mobile phones.

Mobile phone use, in contrast, exhibited consistent growth, reaching a near one-to-one penetration rate (one phone per resident). This widespread mobile phone adoption likely contributed to the UAE's relatively modest growth of Internet users from 2000 to 2009. With the high Internet penetration, the potential for further significant user base expansion was limited.

The UAE offered a variety of locations for Internet access, including public spaces like shopping centres, restaurants, and Internet cafes. In the first half of 2002 alone, the number of Internet cafes increased by 98, bringing the total to 191. Notably, compared to other Arab countries, a much smaller percentage (only 6 per cent) of UAE Internet users relied solely on workplace access. A significant majority (56 per cent) enjoyed access at both work and home. By 2002, EIM reported that home Internet access had reached 39 per cent of users.

Mobile Phones

Introducing mobile phones in the MENA region has encountered challenges common to many developing countries. These included social conservatism, government centralisation, restrictions on free speech, and a weak technological infrastructure. As a result, data from the communications sector has positioned most MENA countries at the bottom of global rankings for information systems, communication methods, and technology penetration for many years.

However, a shift began in the early 2000s. Gulf countries, known for their rapid economic development, experienced a surge in mobile phone penetration and growth rates, mirroring trends in other technological areas. This success prompted policy changes and further economic growth across the MENA region, leading to a substantial overall increase in mobile phone use.

2005 marked a turning point for mobile phone penetration in the Middle East. A surge in new subscribers, totalling 20.6 million, pushed the region's total user base to approximately 63 million by year-end. This growth was particularly significant in Iraq and Algeria, where penetration rates skyrocketed by triple digits.

Established mobile markets like Syria and Egypt, which already boast the highest subscriber numbers, also witnessed impressive growth. Their penetration rates climbed by 84 per cent within a year, reaching 19 per cent. However, Jordan stood out with the most dramatic increase, with penetration nearly doubling from 28 per cent at the end of 2004 to 53 per cent by the end of 2005.

Several other countries, including Oman, Saudi Arabia, Tunisia, and Yemen, surpassed a 50 per cent penetration rate by the end of 2005. Regarding market liberalisation, Jordan and Bahrain emerged as leaders, offering relatively relaxed regulations. In contrast, countries like Lebanon, Libya, and Iran continued to grapple with high tariffs or entry barriers that limited mobile phone accessibility.

By the end of 2006, the Middle East had achieved a significant milestone, surpassing 130 million cellular connections. This accomplishment positioned the region as the second-fastest growing mobile phone market globally, with a growth rate of 30 per cent. Only Africa, at 45 per cent, boasted a higher rate of expansion.

Three countries – Turkey, Iran, and Saudi Arabia – were the primary drivers of this growth, contributing to 79 per cent of the region's total mobile activity. These leading nations also enjoyed a significantly higher cellular penetration rate of 67 per cent compared to the regional average of 50 per cent.

Iran emerged as the leader in mobile phone market growth within the Middle East. Turkey, a regional powerhouse in the cellular sector, and Saudi Arabia, which holds a 15 per cent share of the regional market, are closely behind. Interestingly, despite boasting penetration rates below the regional average, Iraq and Syria also witnessed significant growth in their cellular sectors. This suggests that these latter countries possess substantial untapped potential for mobile phone penetration.

A mid-2008 study in the MENA region revealed that Internet access, video calls, and third-generation (3G) technology were the primary applications driving mobile phone usage.

Mirroring a global trend, landline phone revenue in the MENA region experienced a consistent decline. A 2009 study surveying 46 cellular operators across 19 MENA countries identified Morocco and Lebanon as having the highest mobile usage costs, while Egypt and Yemen offered the most affordable options. These findings echoed an earlier October 2006 study. Lebanon and Mauritania emerged as

the most expensive among the 19 surveyed countries, with Yemen and the UAE boasting the lowest prices.

Driven by regional competition, most cellular operators in the MENA transitioned to billing based on seconds or fractions of a minute. However, a few operators continued to charge by whole minutes.

The evolution of the mobile industry has extended its reach beyond facilitating communication. Today, many mobile applications cater specifically to the needs of the Islamic community. These applications encompass various religious resources, including downloadable Islamic texts for reading on mobile devices, prayer time notifications, directional guidance towards Mecca (Qibla), charity calculators.

A 1998 study by Eric Arnum and Sergio Conti highlighted the promising potential for Internet penetration in Mediterranean countries. Their research argued that these nations constituted the second wave of Internet adoption, following the initial wave observed in North-western Europe. This conclusion was supported by data showing that the MENA region had the fastest annual growth rates in Internet usage at that time (Arnum and Conti 1998).

Early in the Internet era, the Middle East's contribution to the global information and communication industry lagged behind its population size. In 2000, estimates projected the region's share of technological production to be around USD 48 billion, a figure dwarfed by its large population. This was reflected in national statistics, with Egypt, Saudi Arabia, and Lebanon's contributions reaching only USD 418 million, USD 642 million, and USD 400 million, respectively (D. L. Wheeler 2004). However, defying predictions by Eric Arnum and Sergio Conti, the Middle East witnessed a remarkable surge in Internet usage between 2000 and 2005. The region experienced a growth rate of 312 per cent, nearly double the global average (Internet World Stats, n.d.).

Chapter 2 - Obstacles in the Internet Penetration to the MENA

Researchers have identified many factors influencing internet diffusion, including economic conditions, socioeconomic indicators, and geopolitical interventions by international organisations.

In 1997, Bazar and Boalch identified four critical stages in a nation's internet distribution process (Bazar and Boalch 1997):

- **Research**: In many countries, research institutes and universities spearheaded the initial introduction of the Internet, primarily driven by research goals.
- **Education**: Educational institutions, particularly universities, often played a critical role in implementing the Internet. University students further accelerated its spread through their early adoption and enthusiastic use.
- **Commercialization**: While research and education-initiated internet access, commercial forces significantly accelerated development. Investments in infrastructure fuelled this by competing for ISPs, ultimately leading to lower costs for end users.
- **Usage**: The widespread adoption of the Internet by individuals and local communities ultimately brought it to the public.

The study identified several vital actors critical to a nation's internet diffusion:

- **Government and infrastructure providers**: determining the regulations and costs of communication services.
- **Financing entities**: These entities enable financial resources to be invested in infrastructure.
- **ISPs**: provide the Internet technology and the required services.
- **Professional organisations in information systems** are required to implement the technology.

In conclusion, the study examined the factors influencing a country's internet penetration rate.

- **Infrastructure**: Greater infrastructure availability made the introduction of the Internet more accessible, with lower initial capital requirements and fostered higher Internet usage rates. Moreover, ongoing infrastructure development has historically led to cost reductions as communication infrastructure and technology adapt to meet evolving needs.
- **Government policy**: Countries with more liberal government policies on communication and internet services fostered increased market competition. Conversely, regulations restricting information flow and imposing censorship emerged as significant barriers to internet diffusion.
- **Economic development**: The study revealed a strong correlation between a country's economic development level, the nature of its infrastructure, and demand for internet services.
- **Culture**: Cultural norms significantly influenced internet applications and usage patterns. This encompassed personal beliefs, values, and attitudes regarding information sharing.
- **Language**: Language presents a significant barrier to internet access for non-English-speaking countries. To overcome this hurdle and achieve actual Internet adoption, these countries require Internet applications to be available in their local languages.
- **Penetration of information systems**: A high penetration rate of information systems within a country has historically been correlated with increased internet penetration and usage.

A 2004 study by Mauro F. Guillen and Sandra L. Suarez investigated the relationship between a country's Internet usage and its various characteristics. Analysing data from 118 countries between 1997 and 2001, the researchers identified potential links between a nation's level of Internet use and the following attributes (Guillén and Suárez 2005):

- **Economic factors:** This category included a country's income level and the affordability of Internet access. Lower costs and higher national income were associated with increased Internet use.

- **Regulatory environment:** We examined the level of competition in the communication sector and the extent of privatisation. More competition and privatisation could potentially foster Internet adoption.
- **Political factors:** The study considered restrictions on Internet access. Democracies emphasising openness tended to experience faster Internet penetration than countries with centralised control over economic development and income.
- **Sociological factors:** The analysis revealed a correlation between a nation's level of Internet use and its social characteristics. More cosmopolitan societies, characterised by greater openness to diverse cultures and ideas, demonstrated more Internet utilisation over time.

The MENA region's low Internet adoption, penetration, and usage rates can be attributed to several fundamental issues (The Estimate 1998).

Politics

The MENA region has grappled with a persistent 'digital divide' and encountered challenges in implementing reforms. While regional leaders acknowledge the need for such reforms, some may hesitate due to potential consequences for their rule. These concerns might involve fears of destabilisation, a perceived disconnect between citizens and their traditions, or a possible loss of respect for established authorities.

However, the proliferation of information technology and the Internet in MENA countries has the potential to drive a shift towards a more diverse and democratic communication landscape. This evolution could ultimately lead to a more open and decentralised political system.

The Internet challenges faced by the MENA region stem from a complex interplay of technical, structural, political, and cultural issues. Considering these diverse factors and the region's heterogeneity in infrastructure and political landscapes, Henner Kirchner (2001) proposes categorising MENA countries into three distinct development areas (Kirchner 2001):

- **The Maghreb (North African Countries)**: This category encompasses countries in North Africa.
- **The Mashreq (Core Middle Eastern Countries)**: This category refers to countries in the central Middle East.
- **The Gulf Countries**: This category includes countries bordering the Persian Gulf.

Research has consistently highlighted the critical role of government policy in the diffusion of new technologies. Theories examining the relationship between Internet penetration and political structures posit that political systems prioritise technological applications differently. These theories suggest that centralised governments may be less inclined to prioritise the development of interpersonal communication methods, such as telephones and the Internet.

Government policy significantly impacts a country's Internet penetration rate. This influence stems from the government's control over various aspects that shape a nation's digital landscape, including infrastructure, economic development, culture, language, and the existing information systems. Besides direct restrictions on its use, government policy indirectly affects the Internet's circulation by controlling the telecommunications market's competitiveness and openness. A competitive market fosters innovation and investment, ultimately leading to better communication services and lower access and usage costs for citizens.

This approach suggests a positive correlation between free competition in the communication sector and a country's Internet distribution. In other words, countries with a more open and competitive telecommunications market are likely to experience a wider spread of Internet access compared to those with a concentrated industry.

Indeed, MENA countries exhibited significant variations in government policies regarding Internet use. Syria and Iraq imposed the most restrictive measures, effectively barring the public from Internet access. Tunisia maintained tight state control, potentially limiting potential users. Countries like Bahrain, the UAE, and Saudi Arabia employed dedicated filtering systems, enabling them to block specif-

ic websites and monitor email activity. Egypt and Jordan pursued a less stringent approach, focusing on regulating other forms of expression through existing laws.

In contrast, Lebanon, Morocco, and the Palestinian Authority adopted a more relaxed stance. These countries implemented minimal Internet monitoring and restrictions, allowing for greater user freedom (Rinnawi, n.d.).

Society

A 1999 study by Eszter Hargittai examined why some OECD countries had more internet users than others. Her research identified education, particularly universities, as a critical factor. Based on prior studies, Hargittai argued that universities often lead the way in Internet adoption by establishing the first Internet connections within a country. Additionally, she linked higher education levels to increased university enrolment. Her findings in MENA countries supported these points, revealing that most university students utilised the Internet. The study identified education and age as the two most significant factors influencing Internet usage.

Research by Caroline Tolbert, Karen Mossberger, and Ramona McNeal suggests a correlation between higher education and income levels and more robust support for digital democracy (Tolbert, Mossberger, and Mcneal 2002).

MENA countries exhibit a strong positive correlation between education level and Internet usage. A 1999 study found that 70 per cent of Internet users fell within the age group of 21 to 35, with more than half having at least a high school education. Furthermore, a link exists between education and income levels, influencing the adoption of information technology. This connection is particularly evident in political engagement and government interaction, including online voting, petitions, and e-governance.

Language – The dominance of English significantly impacted early Internet usage in the MENA region, the primary language of the Internet in its early years. While

local language websites existed, most information originated from foreign sources in English, creating a significant barrier for many users. Companies like Microsoft eventually addressed this by developing software for the Arabic language. However, initial solutions relied on graphics instead of fonts, leading to slower Internet speeds ("The Current Status of the Internet in the Arab World," n.d.).

Eszter Hargittai's research highlights education and English proficiency as crucial human capital factors influencing a country's Internet penetration rate (Hargittai 1999).

Illiteracy – High illiteracy rates challenge Internet adoption in the Middle East. Shai-lee Spigelman's study found a literacy rate of 65.5 per cent in Muslim countries. However, her research also revealed a weak correlation (0.3) between literacy and Internet penetration in Islamic nations. This suggests that other factors may play a more significant role in explaining Internet usage patterns in the region (Spigelman, n.d.).

Westernisation and Government Anxieties – Arab regimes have historically displayed a range of anxieties regarding the intellectual elite. These intellectuals, particularly those educated in the West, are sometimes viewed with suspicion due to perceived Western influences in their ideas. Consequently, governments may restrict the intellectual elite's individual and collective activities. This apprehension towards the potential for unfettered communication and the spread of ideas online has sometimes led to government hesitation in adopting new Western technologies, including the Internet.

Rasha A. Abdulla argues that the typical Internet user in the Arab world will likely be well-educated, possess strong language skills, and have exposure to Western culture, potentially facilitating cross-cultural dialogue (Abdulla 2005a). Additionally, a high-ranking Bahraini information ministry official observed the rapid proliferation of Internet cafes, comparing it to the sudden appearance of mushrooms after rain. This phenomenon can be seen as a direct consequence of globalisation (Bahrain Tribune, 19 December 2005).

Gender – The MENA region struggles with a gender gap in the labour market and Internet usage. While women comprise a significant portion of students (63 per cent), their representation in the workforce remains low (32 per cent). This disparity is even more pronounced in the technology sector, with women making up less than 12 per cent of the workforce in the UAE. Data from 2000 highlights a similar gap in Internet usage, with women accounting for only 4 per cent of all Internet users in MENA countries (UNESCO 2000). Khalil Rinnawi points out that men constitute 76 per cent of Internet users in the UAE (Rinnawi, n.d.).

A study by Michael Dahan revealed a significant gender gap in Internet use within the MENA region. While women globally comprised 20-40 per cent of Internet users, only 6 per cent of MENA women had Internet access. Despite having the lowest Internet penetration rate worldwide, Dahan concluded that the MENA region also held the most significant potential for future growth (Dahan, n.d.).

In 2003, Nikhilesh Dholakia, Ruby Roy Dholakia, and Nir Kshetri investigated the relationship between gender and Internet penetration. Their study examined global Internet use patterns through a gender lens, revealing a lower global GDP per capita for women than men. This disparity, they noted, varied significantly across countries. Consequently, the study proposed that gender income inequality contributed to differences observed in Internet adoption and usage across nations (Dholakia, Dholakia, and Kshetri 2003). Additionally, the research identified a correlation between the proportion of female Internet users and the maturity of a country's Internet infrastructure. In the MENA region specifically, the study found an exemplified gender gap, with a ratio of 94 male users to 6 female users.

The researchers projected a gradual narrowing of this gender gap, acknowledging that the pace of change would vary by country. They linked this variation to the types of Internet activities prevalent in each region, their frequency of use, and the age demographics of Internet users.

Religion and Internet Use – Spigelman argued that a higher percentage of Muslims in a country correlated with a lower Internet penetration rate. This suggest-

ed a potential negative correlation between Islam and Internet proliferation (Spigelman, n.d.).

However, it is essential to consider the specific challenges the Internet presented for some governments. The Internet's ability to facilitate accessible communication, public discourse, and the anonymous expression of diverse viewpoints could be perceived as a threat to established political and religious authorities in various countries.

A growing body of research has examined the impact of the Internet on society and the Muslim world, specifically its uses and potential benefits. These studies have identified three distinct stages in the evolution of the Muslim online presence (J. Anderson 1997):

1. **The Early Stage (1980s): Digitization and Discourse**: In the early 1980s, Muslim students working or studying in high-tech fields pioneered the Muslim online presence. They digitised religious texts, uploading them to the Internet for the first time. These students also established online discussion groups to debate various Islamic issues.
2. **The Rise of Online Activism**: The following stage witnessed the involvement of radical activists in online spaces. Their activities and presence on the Internet require further exploration.
3. **Expanding Voices**: The Rise of the Muslim Middle Class: As Internet usage expanded, the middle class emerged as a significant force in expressing diverse Islamic viewpoints online. Despite their smaller numbers than the established religious elite, their online presence held considerable weight.

Economic

Economic Development – low income emerged as a significant factor impeding the proliferation of the Internet in the MENA region (Privacy International and the GreenNet Educational Trust 2003).

Research by Eszter Hargittai identified low income as a significant barrier to Internet proliferation within the MENA region. Her study examined the impact of various factors on Internet access, including economic indicators (GDP), income inequality (measured by the Gini index), human capital (education and English language proficiency), legal and regulatory frameworks (specifically communication industry regulations and Internet access costs), and the existing technological infrastructure. Hargittai's research concluded that a country's economic well-being and communication policies were the most influential factors determining the level of Internet connectivity (Hargittai 1999).

Katsuyoshi Okui investigated the relationship between political and economic freedom, ultimately challenging the assumption of a direct causal link between the two. His research suggested that an authoritarian government could expand its citizens' economic opportunities to restrict their political freedoms (Okui 2005).

Purchasing power – Studies highlighted the significant financial barriers to Internet access in the MENA region. After considering all costs, Alterman estimated that a potential user would require a minimum of USD 3,000 to gain Internet access. This high cost effectively excluded many of the MENA population from Internet use. Conversely, Wheeler argued for the surprising affordability and efficiency of communication and Internet services in Jordan and Egypt compared to Europe and North America. He claimed that costs in these Western regions could be two to three times higher than in the MENA, and the time required to obtain Internet access could be similarly extended (D. L. Wheeler 2004).

In a 1998 study, Eric Arnum and Sergio Conti actively investigated the relationship between Internet penetration and economic prosperity across 100 countries. Their analysis revealed that economic prosperity directly facilitated the acquisition of hardware, software, and communication resources – all essential elements for Internet connectivity (Arnum and Conti 1998).

Infrastructure – Arnum and Conti (1998) further identified a potential correlation between infrastructure development and Internet usage. Their study suggested

that countries with higher transportation, energy, and communication distribution rates typically exhibited higher Internet usage rates and broader Internet access. Interestingly, the MENA region in their analysis, which included countries like Kuwait, Bahrain, the UAE, Lebanon, Turkey, Oman, Egypt, Morocco, Saudi Arabia, Iran, and Algeria, fell within the lower range of Internet usage (Arnum and Conti 1998).

Communication Infrastructure Challenges – In 1995, communication infrastructure in MENA countries presented a significant hurdle to Internet adoption. The average telephone line density was a mere 4 per 100 inhabitants, only one-tenth of the level observed in most industrialised nations. This limited infrastructure, coupled with bandwidth constraints like those experienced in Western countries, hampered Internet development in the region. Limited bandwidth led to significant connection speed and data transmission challenges as Internet users grew. Recognising this bottleneck, many MENA countries, with the UAE leading, embarked on initiatives to upgrade their communication infrastructure. These efforts were a direct response to the increasing Internet penetration in the region ("The Current Status of the Internet in the Arab World," n.d.).

The personal computer market in MENA countries experienced a significant boom by the end of the 1990s. The region witnessed an annual growth rate of 20 per cent, with some countries like Lebanon, Egypt, and Saudi Arabia exhibiting even more dramatic increases, reaching annual growth rates of 50-60 per cent. This surge in computer ownership coincided with a substantial rise in Internet users. Between 2000 and 2001, eight MENA countries saw a remarkable 47 per cent increase in Internet user base. Furthermore, bandwidth capacity also underwent significant improvement during this period. From August 2001 to January 2002, a substantial increase of 154 per cent was recorded in bandwidth availability (Alterman 1998; Rinnawi, n.d.).

Costs – Internet usage in the MENA region was characterised by a paradox: low Internet access rates and high connection costs. These high costs deterred poten-

tial users from subscribing. However, the emergence of new competitors in the communication market triggered a price war, leading to significant cost reductions. This, in turn, increased Internet accessibility and drove a rise in Internet accounts. Peled identified a vicious cycle hindering Internet adoption in the region. Weak communication infrastructure and high connection costs resulted in low demand for Internet connectivity. Conversely, this low demand failed to generate sufficient public pressure to force improvements in infrastructure or reductions in connection costs. Peled warned that this cycle could leave MENA countries lagging in the global Internet revolution (Peled 2000).

Information Technology – Rafal Rohozonski argued that the MENA region fell behind most of the world in crucial Information Technology (IT) metrics, surpassed only by Sub-Saharan Africa and South Asia. This digital lag persisted despite solid growth in home Internet access, suggesting limited integration of information systems and the Internet into daily life. Rohozonski emphasised that building a robust IT sector solely through exports was unsustainable. He urged MENA governments to prioritise integrating the Internet and IT into all aspects of daily life, including education, business operations, domestic uses, and government services. This lack of integration was evident in the widespread reliance on Internet cafes and communication centres instead of private Internet subscriptions. Consequently, two distinct patterns of Internet usage emerged in the region (Rohozinski, n.d.):

- **Internet Cafes** – In regions with low private Internet subscriptions, public access points like Internet cafes played a crucial role. Deborah L. Wheeler (2004) highlighted their significance in the early stages of Internet adoption in the MENA region. She noted, "Most of the general public in the region obtains access via an Internet café or community centre, rather than through an individual ISP account" (D. L. Wheeler 2004). In a 2004 study, Wheeler presented compelling statistics on the prevalence of Internet cafes in several MENA countries:

Country	Number of cafés
Algeria	3,000
Morocco	2,150
Libya	700
Syria	600
Jordan	500
Egypt	400
Tunisia	300
Kuwait	300

- **Shared Accounts** – **In 2002, the average number of users per account in MENA countries was a notable characteristic of Internet usage**. Data indicated an average of three users per Internet subscription.

Old Media – The MENA region historically exhibited a challenging environment for media freedom, with journalists facing government supervision and restrictions. This lack of penetration of traditional media ("old media") potentially influenced the region's unique path towards new media adoption. Compared to a staggering 100.6 average penetration rate for "old media" in the USA, MENA countries averaged a mere 12.9. Researchers observed a potential correlation: increased Internet usage might coincide with greater market liberalisation, competition in the telecommunications sector, and democratisation efforts. However, they acknowledged that regulatory hurdles, political factors, and social dynamics also significantly shaped the digital divide. It is important to remember that this research, conducted between 1997 and 2001, captured the early stages of Internet development in the MENA region, lagging considerably behind the Western world.

Research has emphasised that a single factor does not drive Internet penetration and usage. Instead, a complex interplay of various parameters is at work. Eszter Hargittai (1999) underscored this complexity, demonstrating that many factors influence a country's Internet penetration level. While economic prosperity undeniably plays a critical role in enabling Internet connectivity, Hargittai argued that

economic factors alone cannot fully explain the picture. Therefore, she advocated for considering additional data points such as a country's human capital (e.g., education levels) and information regarding its media policies (Hargittai 1999).

The research identified several key factors influencing Internet usage in a country. While complete English language fluency was not essential, a good command was beneficial for productive Internet use. Furthermore, the study revealed a significant negative impact on Internet connectivity in countries with a communication market monopoly. Additionally, Internet usage costs emerged as a substantial factor influencing national connectivity levels. Finally, the research highlighted the direct impact of communication policy on Internet use. Policy measures that regulate access prices, technology choices, and communication infrastructure directly affect the extent of Internet adoption within a country.

Chapter 3 - Government Usage of the Internet

Historically, MENA governments have pursued a two-pronged approach towards technology, particularly the Internet. They actively develop their technology sectors to improve government operations while maintaining tight control over internet activity. They crack down on ISPs, websites, users, and owners deemed to have violated government restrictions.

E-Government Initiatives

Several MENA countries, including Lebanon, Egypt, the UAE, Bahrain, and Kuwait, launched e-government services offering various functionalities to citizens, businesses, and tourists. These websites provided a wealth of information and allowed users to make payments, settle fines, submit online forms, register for universities, book transportation, conduct customs operations, and access various informative resources.

A 2010 UN survey positioned Bahrain as a regional leader in e-governance. The country secured an impressive 13th-place ranking, marking a significant leap from its 42nd position in 2008 (United Nations 2010).

Local governments in the region actively embraced social media platforms while maintaining websites for individual government ministries and a unified national portal. This comprehensive e-governance program offered citizens a variety of online communication channels with government officials, including blogs, forums, surveys, and live chat functionalities. Notably, this multi-faceted approach yielded impressive results, with a user satisfaction rate reaching 85 per cent.

The 2010 UN survey revealed a close cluster of several Gulf countries in the global e-governance rankings: the UAE (49th), Kuwait (50th), Saudi Arabia (58th), and Qatar (62nd). Interestingly, most of these countries experienced a decline in their rankings compared to previous years, further emphasising Bahrain's exceptional progress. Bahrain distinguished itself by offering various e-governance servic-

es, including a pioneering e-visa project that streamlined visa applications for international visitors (Bahrain Tribune 2005a). The Bahraini Ministry of Health also took a groundbreaking initiative among Gulf countries by publishing a list of approximately 3,000 available medicines on its website. Furthermore, Batelco, a local telecommunications company, spearheaded an e-governance program that allowed citizens to conveniently pay traffic fines, renew vehicle and driver's licenses, and settle water and electricity bills online.

Underscoring its strong foundation for e-governance initiatives, Bahrain secured an impressive second place ranking behind the UAE in all communication indicators within a 2003 UN readiness assessment. This achievement placed both countries among the global leaders, with Bahrain at 35th and the UAE at 29th out of 191 nations assessed.

In 2002, Egypt announced progress on its "electronic government" project, aiming to provide citizens with various phone and Internet-based services. Project manager Ahmed Darwish outlined an ambitious vision: delivering all government services online and eliminating the need for in-person visits. This, Darwish argued, would not only reduce government expenses but also facilitate Egypt's integration into the global economy. However, a 2005 report revealed a significant gap between ambition and reality. While citizens could download forms and access service information online, only a third of government services offered online completion of processes ('iilaf 2004a).

The MENA region witnessed a surge in e-commerce activity alongside the rise of e-government initiatives. A diverse range of websites emerged, catering to various e-commerce segments. Cobone.com, souq.ae, arabtradezone.com, sooqelarab.com, and others offered general merchandise, while platforms like simplyislam.com, iqrashop.com, and Islamicimpressions.co.uk specialised in Islamic products. These platforms facilitated business-to-consumer (B2C) transactions and served as a marketplace for business-to-business (B2B) interactions, as exemplified by businessdubai.com and alwen.com (Stensgaard 2005). Credit card

Company Visa data revealed a significant rise in online spending across the Persian Gulf countries. During the first quarter of 2005, online transactions reached a staggering USD 20 million, reflecting a remarkable 600 per cent increase compared to the previous year. The report further indicated the UAE' dominance, accounting for 85 per cent of the total online spending. The UAE also witnessed a dramatic rise in the number of transactions, with a fivefold increase. These figures point to the growing penetration of e-commerce in the UAE and users' increasing comfort and willingness to conduct online transactions, likely facilitated by supportive government policies. By 2010, online purchases had become more commonplace across the MENA region, with 32 per cent of Internet users engaging in e-commerce activities. This figure rose to 43 per cent in the Gulf countries, a trend likely fuelled by the steady rise in Internet penetration rates across the region.

Several initiatives emerged to facilitate online transactions, particularly in the leading e-commerce sectors of tourism and gaming, such as One Card (onecard.net). Launched in 2004, this electronic payment method was operated by a Saudi company.

As early as 2002, the Director of the Social Development Office in Egypt's Ministry of Communications strongly recommended implementing electronic commerce. This call to action emphasised the potential for businesses that failed to adapt to the Internet to face bankruptcy. The study further underscored the importance of developing a strategic plan to integrate e-commerce to bolster the national economy.

As early as 2002, the Director of the Social Development Office in Egypt's Ministry of Communications strongly recommended implementing electronic commerce. This call to action emphasised the potential for businesses that failed to adapt to the Internet to face bankruptcy. The study further underscored the importance of developing a strategic plan to integrate e-commerce to bolster the national economy.

Technology Park

Several countries in the Middle East, particularly those bordering the Persian Gulf, strategically utilised the Internet to achieve economic growth and enhance their regional standing. Skype's decision to establish its first Middle Eastern branch in Bahrain in June 2010 exemplified this focus on digital development. Similarly, Dubai Internet City (DIC), a technology park founded in Dubai in 2000, emerged as a hub for numerous communication and technology corporations. These companies benefited from DIC's comprehensive one-stop-shop services, including giants like Microsoft, Cisco Systems, IBM, HP, Dell, Siemens, Sun Microsystems, and Computer Associates. This streamlined approach offered support for business establishment and ongoing management, encompassing everything from immigration assistance to advanced communication infrastructure.

Critics, however, raised concerns about DIC potentially enabling local authorities to exert tighter control over foreign technology operations within the park. This included imposing technical restrictions on communication and setting significantly higher pricing structures – 5 to 10 times more expensive than those found in Western countries. Additionally, authorities blocked access to online social services and implemented content regulations for numerous websites.

In contrast, another emirate within the UAE, Ras Al Khaimah, established a competing technology park – Ras Al Khaimah IT Park. This park became part of the UAE's broader network of free trade zones, catering to diverse sectors like communication, media, healthcare, and finance.

Head of States' Websites

In addition to other initiatives promoting Internet use, many MENA heads of state actively cultivated an online presence through personal or institutional websites. These websites served several purposes: legitimising the Internet as a communication tool, encouraging responsible use, and promoting the leader's activities in the digital sphere. By analysing these websites in 2009 research, the author

explored the potential of this online presence to shed light on leadership styles and political structures within the MENA region. The study focused on websites from 15 MENA countries, with varying degrees of freedom and Internet penetration potentially influencing the content and presentation:

Algeria – the website of the presidency (no longer active) ("President de La Republique," n.d.).

Bahrain –the website of King Bu Salman (no longer active) ("Buslman," n.d.)

Dubai – the site of the ruler of Dubai, Sheikh Muhammad Ibn Rashed Al Maktoum (no longer active) ("His Highness Sheikh Mohammed Bin Rashid Al Maktoum," n.d.), as well as that of his consort (from 2004 to 2019), Princess Haya Bint Al Hussein ("Her Royal Highness Princess Haya Bint Al Hussein," n.d.)

Egypt – the website of the presidency (inactive) ("The Egyptian Presidency," n.d.)

Iran – the websites of the president of Iran, Mahmoud Ahmadinejad ("Official Website of the President of the Islamic Republic of Iran," n.d.), his speeches ("Presidency of The Islamic Republic of Iran," n.d.), the private website Ahmadinejad ("Yaaddaasht Haaye Shakhsi Ahmadi Nejhaad (Persian)," n.d.) (both are no longer active) and the website of the Supreme Leader Ali Khamenei ("The Office of the Supreme Leader," n.d.)

Iraq - the website of the presidency (no longer active) ("Iraqi Presidency," n.d.)

Jordan – the websites of King Abdullah ("Almawqie Alrasmiu Lijalalat Almalik Eabdallah Althaani Aibn Alhusayn (Arabic)," n.d.) and his wife, Queen Rania Al Abdullah, and that of His father, King Hussein ("The Office of King Hussein I of Jordan," n.d.)

Kuwait – the website of Emir Sheikh Zabah al-Ahmad al-Jaber al-Zabah (no longer active) ("Al Diwan Al Amiri," n.d.)

Lebanon – the website of the President of Lebanon (no longer active) ("Presidency of the Republic of Lebanon," n.d.)

Libya – the website of Muammar al-Gaddafi (no longer active) ("AlGathafi Speaks," n.d.)

Qatar – the website of Emir Sheikh Hamad bin Khalifa Al Thani ("Amiri Diwan, Doha, Qatar," n.d.), as well as that of his wife, Sheikha Mozah bint Nasser al-Missned ("Her Highness," n.d.) (Both are no longer active).

Saudi Arabia - the website of King Abdullah ibn Abdel-Aziz Al Saud ("King Abdullah, Saudi Arabia," n.d.), that of the late King Fahd bin Abdul Aziz ("King Fahd Bin Abdul Aziz," n.d.), and the site of Prince Fitzal Ibn Sultan Ibn Muhammad ibn Abdel Aziz ("Prince Faisal," n.d.) (The last two websites are no longer active)

Syria – President Bashar al-Assad does not have an official website on behalf of the state; on the Syrian News Agency website, there is an area dedicated to the president. There is also a private website in honour of the president and his father ("Syrian Arab News Agency (SANA)," n.d.), at two different addresses and several inactive official addresses - basharassad.org, basharassad.com, and assad.org (all are inactive).

Tunisia – the website of the elections of President Zine al-Abdin Ben Ali ("Mawqie Alhamlat al'iintikhabiat Lilrayiys Zayn Aleabidin Bin Eali (Arabic)," n.d.) (no longer active) and the website of the presidency ("Riasat Aljumhuriat Altuwnisia (Arabic)," n.d.)

Yemen – the website of President Ali Abdullah Saleh ("President Ali Abdullah Saleh - Yemen," n.d.)

Several exciting conclusions can be found:

Lack of Official websites -

Syria, Egypt and Saudi Arabia – Intriguingly, research revealed an absence of official and active websites for the heads of state in some of the most influential MENA countries, including Syria, Egypt, and Saudi Arabia. This finding is particularly noteworthy given that these countries are known for imposing some of the

most stringent Internet restrictions, including Syria, Egypt, and Saudi Arabia. Reporters Without Borders has even classified them as "enemies of the Internet" alongside 12 other nations. For instance, the Syrian News Agency website featured a section dedicated to the president, but it did not function as an official presidential website. Similarly, the official presidential website in Egypt remained inactive and under construction for a significant period. Saudi Arabia presented a similar picture, with only a dedicated section within a more extensive website for the reigning king.

Palestinian Authorities – The research also yielded no results in identifying official websites for the leaders of the Palestinian Authorities, which encompass both the West Bank Authority and Hamas in the Gaza Strip. While three Facebook profiles emerged under the name Ismail Haniya, their authenticity could not be conclusively verified, and they did not function as official platforms.

Leader Representation Online –

Centralised States – In countries with centralised governments, leader websites often prioritise showcasing the leader's image and activities, potentially overshadowing the institution itself. These websites focused on the leader, evident in the extensive coverage of speeches, visits, photographs, interviews, and press conferences.

Monarchical Systems – Royal websites often highlight the rulers' familial and dynastic heritage. They featured detailed accounts of the royal lineage and their historical significance. Connections to websites of family members and consorts are also presented, particularly in Jordan, Qatar, and Dubai. English emerged as the dominant language on these websites.

Ideological Regimes – Websites of leaders in ideological regimes, such as those in Iran and Libya, primarily functioned as platforms for promoting their ideologies. These websites offered content in a broader range of languages, with the Libyan leader's website translated into eight languages and the website of Iran's spiritual

leader available in ten. English was often used as the default language, exemplified by the Iranian president's blog.

Language – Arabic emerged as the dominant language for most leader websites, with some offering the option to switch to other languages. However, a few exceptions existed, such as the Bahraini ruler's website, which remained exclusively available in Arabic.

President and Presidency –

Multi-Party System – In countries with multi-party systems, like Lebanon and Algeria, a clear distinction was made between the president as an individual and the presidency as an institution. These countries' official websites typically displayed a modest-sized image of the president, often in a formal suit.

Centralised States – In contrast, presidents in centralised states like Iran were frequently pictured more symbolically. For instance, the Iranian president's image might offer blessings against a backdrop of sky and clouds, potentially symbolising divine endorsement. Similarly, the Tunisian president's website offered contrasting portrayals: a more casual image on his campaign website and a more formal one on the official presidency website, where he presided over a government meeting with attendees seemingly showing deference.

Monarchical Systems – Royal websites predominantly depicted rulers with a smile, cultivating an image of approachability. King Abdullah of Jordan's website exemplified this strategy, featuring two prominent profile pictures showcasing his warm smile. The Emir of Dubai, despite a potentially stern appearance in photographs, was often referred to by his first name ("Muhammad" or "Sheikh Muhammad"), further fostering a sense of familiarity.

Ideological Regimes – An outlier was the Libyan leader's website, which presented a more domineering portrayal. His image spanned the entire width of the website, superimposed on a world map (coloured green, of course) – his presence dwarfing even the map itself.

Graphics and colours –

Multi-Party System – Websites of presidents from multi-party governments, such as Algeria and Lebanon, displayed a distinct visual approach compared to those in more centralised states. These websites emphasised the separation between the presidency as an institution and the individual holding office. This distinction was reflected in a modest photograph of the president and a larger presidential palace image. Additionally, these websites favoured a colour palette of similar cream tones, often associated with naturalness, diligence, seriousness, and efficiency.

Monarchical Systems – Royal websites, particularly those from the Gulf countries and Jordan, exhibited a distinct design aesthetic. These websites prioritised meticulous design and striking visuals, often incorporating shades of blue. As a versatile colour, blue symbolised prestige, nobility, wisdom, faith, and tranquillity. This colour preference was evident on the websites of the Jordanian king and the emirs of Dubai, Kuwait, and Qatar.

Interestingly, even the websites of the Iranian president and supreme leader utilised blue hues, albeit in a more nuanced way. The former employed lighter tones, while the latter favoured darker shades, distinct from the "royal blue" prominent on other websites. Some royal websites, such as those of the Kuwaiti emir, King Abdullah (with added gold tones), and the Emir of Dubai, incorporated brown alongside blue, potentially symbolising the unity of water, sky, and earth under the leader's domain.

Royal websites also employed other symbolic colours. For instance, the websites of King Hussein and the wife of the Qatari emir used various shades of purple traditionally associated with spirituality. The website of the Tunisian president offered a unique contrast, featuring a combination of red (representing the physical realm) and blue (representing the mental realm). This combination was likely intended to convey stability, consistency, and an ambitious vision.

This analysis of MENA leader websites yielded several key findings and prompted further exploration:

- **Limited Correlation with Internet Freedom**: The study did not reveal a direct correlation between leader websites and a country's Internet penetration rate or level of Internet freedom.
- **Internet as a Propaganda Tool**: The widespread adoption of leader websites across the region suggests the Internet's growing importance for shaping public perception. These websites are often used to promote the leader's image, achievements, heritage, and lineage, even in countries with limited Internet access or restrictions on free speech.
- **Ideology and Website Activity**: A correlation emerged between a regime's ideological foundation and the website's activity level. Websites of leaders in more ideologically driven regimes tended to be more active, disseminating the leader's teachings, writings, and speeches in a broader range of languages.
- **Similarities across Systems**: Interestingly, the research identified notable similarities in website structure and content between leaders from multi-party states and those from monarchies.
- **Insights and Limitations**: While analysing leader websites provided valuable insights, limitations exist. The sheer number of existing websites, alongside the absence of websites for some key leaders, highlights potential gaps in data collection. Additionally, the inaccessibility of websites for former leaders complicates efforts to track historical changes in online representation.

PART B – DISILLUSIONMENT: THE CHALLENGES

Chapter 4 - The Internet as a National Challenge in the MENA

Like global trends, the Internet emerged as a powerful tool for marginalised groups in the MENA region. This included minorities, human rights organisations, and religious and political opposition groups. These actors, often silenced by state media due to social or religious restrictions, leveraged the Internet to amplify their messages, regardless of their location within or outside the country. The Internet's ability to influence domestic affairs on multiple levels presented a significant challenge for MENA governments (Kalathil and Boas 2001; Peled 2000).

The Arabic Network for Human Rights Information (ANHRI), an Arab human rights organisation, identified three primary taboos in the Arab world: religion, sex, and politics. In Egypt, corruption joined this list. Their research demonstrated government oversight of media engagement with all four topics, including online content. This phenomenon reflects a core tension in the region. Arab countries simultaneously desire technological advancement and the economic benefits of the Internet yet also aim to restrict its use to safeguard religious, cultural, and moral values, as well as political, governmental, and economic norms (Human Rights Watch 2005a).

Politics

The democratisation process in some MENA countries fostered the development of a society receptive to technological innovation. A liberal approach to information access and exchanging ideas underpinned this development. However, policies in MENA countries contradicted the principles of free discourse, which are essential for the Internet to flourish.

Governmental restrictions on information access significantly hampered the MENA region's participation in the information revolution, regardless of invest-

ments in communication networks. The Internet emerged as an alternative platform for diverse organisations to voice dissent, often using covert methods. Public access to information technology was viewed as a tool for receiving and disseminating information. Compared to traditional communication methods, the Internet offered a readily available and swift way to mobilise public opinion against established regimes, challenging their legitimacy and dominance. This power stemmed from the Internet's ability to spread information and ideas and engage international audiences with relative speed, ease, and security.

Thomas Friedman, a prominent author, argued that modern technologies, including the Internet, could create a more transparent, democratic, distributed, and global society. He saw the Internet as a new channel for the unrestricted flow of information, bypassing the control of centralised regimes. In his view, the Internet was poised to disrupt and potentially weaken centralised governments in the MENA region (Friedman 1999).

Opposition – Periods of political unrest particularly highlighted the need for internet control measures. For instance, during elections in Iran, authorities shut down reformist websites and internet cafes. These actions aimed to stifle online activity that could undermine the government's legitimacy. This strategy mirrored tactics used in other countries, such as direct censorship to silence dissent (seen in Egypt and Syria) or indirect control to maintain traditional values (employed in Saudi Arabia and the UAE). Fears of online dissent and activism were the primary factors that delayed the adoption of advanced interpersonal communication technologies in MENA countries. The government's inability to monitor these communications gave opposition groups a significant advantage over state forces, including the police, intelligence agencies, and the military. The opposition exploited this new medium domestically and internationally, engaging with citizens abroad to influence domestic affairs. They gained new communication capabilities and access to an independent information source the government could not control.

Press freedom restrictions in Iran propelled the Internet to become a vital resource. The government heavily scrutinised and often shut down printed press and other media outlets. The Internet, however, offered a liberated platform for newspapers banned from printing and served as a political catalyst for reformist parties facing government suppression of their publications. The first decade of the 21st century witnessed numerous events across the MENA region where the Internet was pivotal in their inception and global reporting.

The Iranian online sphere may serve as an example: "The popularity of the president of the Islamic Republic, as peddled by the official media, is all on the surface. Criticism by Iranians floods the Internet even if the authorities block most methods of getting around censorship available on the network" (Reporters Without Borders, n.d.-b).

Iran's conflict between conservatives and reformists spilled over into the online sphere, with each faction establishing its news websites. To illustrate this digital divide, authorities blocked the reformist-affiliated website emrooz.ws in February 2003. This action prompted the scathing observation: "In fact, it is now easier to access pornographic sites than reformist ones." (Reporters Without Borders 2004a)

All four candidates in Iran's June 2009 presidential election campaign and their supporters actively utilised the Internet, particularly various social networks. This surge in online activity stemmed from recognising the growing importance of social media and Iran's high Internet penetration rate. Candidates leveraged various tools, focusing heavily on platforms like Flickr, Friendfeed, Facebook, Twitter, YouTube, Delicious, and Google Calendar. These platforms empowered candidates and their supporters to report on the campaign, recruit bloggers, upload photos and videos, and even outline upcoming events. Mir Hossein Mousavi, a reformist candidate, emerged as a leader in online engagement. His focus on Facebook, where he amassed 36,000 supporters, ultimately temporarily led Iranian authorities to block the service in late May. Mousavi's supporters and many bloggers also established a dedicated website for him. Over a thousand support-

ers publicly declared their backing on this platform, even providing their names and website addresses.

Following the announcement of the election results, mass protests erupted in the streets of the capital and other cities. Incumbent president Mahmoud Ahmadinejad's victory was met with outrage by supporters of his rival, Mir Hossein Mousavi, who viewed it as a stolen election. Domestically and internationally, the demonstrations were framed as a fight for freedom against a dictatorship. Mousavi's supporters, leveraging the power of the Internet, rallied others to their cause and documented their clashes with security forces. They used their mobile phones to live-tweet these incidents directly to their Twitter accounts, instantly broadcasting their experiences to a global audience.

Field reports streamed onto Twitter, while YouTube witnessed an almost instantaneous upload of hundreds of protest videos from city streets, capturing the events and attracting a global audience. Mousavi's supporters flooded their Flickr account with over 1,500 photos, primarily from the recent demonstrations, creating a daily showcase of the unfolding events on Iran's streets. This rapid flow of information on the Internet powerfully demonstrated its potential in countries with limited freedom of expression, becoming a mirror reflecting the aspirations of the Iranian people.

The chaotic aftermath of Iran's June 2009 presidential election dramatically illustrated the power of the Internet and mobile phones in challenging centralised regimes like those in the MENA region. These technologies empowered protestors to communicate, document clashes with security forces, and rapidly disseminate information – text and visuals – from the streets of Iran to a global audience. A powerful example emerged with the video capturing the last moments of Neda Agha-Soltan, a young woman shot by security forces. Uploaded and circulated rapidly online, this video transformed Neda into a posthumous symbol of Iran's reform movement. Beyond Iran, mobile phones became a ubiquitous reporting tool for bloggers and human rights activists facing detention. These individuals frequently used their phones to tweet about their arrests, documenting the event

and providing public "insurance" for their safety. This often-triggered significant public outcry and expedited their release.

Separatists – Sean McLaughlin investigated how non-state dissidents, also known as separatist elements within the MENA region, actively used the Internet to influence political activity against the state. This analysis considered the limitations imposed by state restrictions on Internet usage (S. W. McLaughlin 2003).

McLaughlin dissected state-imposed restrictions on Internet access, categorising them into infrastructure limitations and censorship. These limitations aimed to hinder separatist movements by restricting their online activity. In response, the author developed a dynamic model of Internet-facilitated separatism. This model considered the goals of both the state (curtailing separatist efforts) and the separatists (leveraging the Internet to gain an advantage). The model also factored in how separatists would adapt their tactics in response to state restrictions.

The author argued that states primarily sought to limit the effectiveness of separatists through Internet controls. These controls included restricting infrastructure access and imposing censorship to weaken online resistance. Conversely, separatist factions actively sought to overcome these limitations. They viewed the Internet as a tool that could potentially tip the power balance in their favour. Given the absence of formal political avenues in these regimes, separatists resorted to extra-legal means like online dissent to undermine state authority.

McLaughlin's model analyses three significant components of Internet-facilitated separatism:

1. **Separatist Strategies**: This section of the study examined the goals of separatist groups in the MENA region, the political actions they undertook to achieve them, and the role of the Internet in facilitating these activities. Three distinct tactics were identified:
   - Mobilisation – The research found that separatists primarily used Arabic messaging with religious and political themes to attract a broad domestic

audience. These religious appeals transcended national borders, fostering a broader support base.

- Internationalisation – The Internet gave separatists unprecedented access to a global audience. They communicated their message in English, often referencing universally recognised principles like human rights.
- Undermining Legitimacy – The study observed that efforts to garner support for the separatists' positions aimed to deprive the state of legitimacy. Consequently, the messages associated with their political activities were predominantly negative. They portrayed the regime as un-Islamic to domestic audiences while emphasising international norms such as human rights to foreign audiences.

2. **State Countermeasures**: The study further evaluated the objectives of various countries in the MENA region and explored how they could curtail the impact of Internet-facilitated separatist activities. It found that successful Internet utilisation by separatists necessitated unrestricted access for both users and their target audience. Therefore, states employed two primary strategies to undermine the effectiveness of these political activities:
   - Infrastructure Control – Limiting Internet access by controlling the underlying infrastructure.
   - Legal Constraints – Enforcing legal restrictions on user behaviour and content.

The study acknowledged that combining these approaches was also a common tactic.

3. **Separatist Adaptation**: The study scrutinised how separatists adapted to state efforts to curtail Internet-based political activities. Three primary strategies emerged:
   - **Message Adjustment** – This involved altering the content of political declarations in response to government censorship. While a short-term victory for the state, it allowed separatists to maintain communication with their power base, disseminate non-political information, and develop more sophisticated countermeasures.

- **Technological adaptation** – This refers to the separatists' use of technology to circumvent technical barriers imposed by the state. Examples included message encryption, alternative email services, and websites facilitating anonymous Internet usage.
- **Organisational adaptation** – involved transitioning to a more networked organisational structure, which provided an advantage over the state's hierarchical structure.

The author applied this model to the Muslim Brotherhood in Jordan and Egypt, and the Movement for Islamic Reform (MIRA) in Saudi Arabia. Each organisation was analysed across the three components and within the context of the three types of political activities (mobilisation, internationalisation, and support for drift).

The study concluded that separatist factions in the MENA region primarily targeted domestic audiences through Arabic language and Islamic motifs, with limited international outreach (except for MIRA). Additionally, the author highlighted the governmental restrictions imposed on these organisations' websites and the countermeasures they employed.

The McLaughlin model, however, suffers from several limitations:

1. **Limited time frame:** The study failed to specify when the information was collected. This lack of temporal context makes it difficult to assess the findings' applicability to the present day.
2. **Narrow Scope:** The model focused on just three countries, examining government restrictions solely on the websites of a single organisation within each. Notably, the organisations in Jordan and Egypt were branches of the same entity. The research did not delve into a broader analysis of governmental Internet restrictions as a general phenomenon within these countries.
3. **Superficial Data Analysis:** The model addressed technological restrictions and website censorship in a rather general way. It simply questioned whether official restrictions existed and, if so, their nature. It did not consider other aspects of government control over Internet infrastructure and usage.

4. **Absence of Comparative Analysis:** The study lacked quantitative data analysis. It did not present metrics that would allow for a comparative ranking of the three countries based on the extent of their Internet restrictions. This hinders our ability to draw clear conclusions about the relative severity of Internet control across these nations.

Terrorism

The Internet, a powerful tool with broad reach and accessibility, revolutionised information exchange and public opinion gathering. It provided a platform for diverse voices. However, its inherent characteristics also opened doors for various subversive activities.

Terrorist organisations exploited the Internet for several purposes:

- **Recruitment**: They used the Internet to recruit operatives.
  - **Ideological Foundation**: The Internet provided a platform to spread their ideology and justify their actions.
  - **Operational Guidance**: Terrorist groups offered guidance to operatives through the Internet.
  - **Educational Materials**: They disseminated educational materials on bomb-making and other violent tactics.
  - **Fundraising Infrastructure**: The Internet facilitated the creation of fundraising infrastructure to support terrorist organisations.

Over time, terrorists devised various methods to extract funds from Internet users. The effectiveness of these methods depended on the user's awareness that their contributions financially supported terrorism.

Beyond facilitating legitimate commerce, the Internet emerged as a platform for terrorist financing, employing direct, indirect, and intermediary methods.

Early Online Fundraising: In their initial foray into the online world, some MENA terrorist organisations openly solicited donations on their websites. These ap-

peals included bank account details, check mailing addresses and online donation forms. Early Hezbollah websites, like Al Manar TV, explicitly requested donations for the organisation or the "Islamic Resistance." However, these direct appeals became less common over time.

Shifting Tactics: Terrorist groups swiftly adapted their online fundraising tactics. Initially, they openly solicited donations on websites, offering bank details, mailing addresses, and online forms. Early examples include Hezbollah websites like Al Manar TV, which explicitly requested funds for the organisation.

However, terrorist groups later transitioned to more veiled approaches. Websites focusing on innocuous topics like welfare or social issues sometimes masked their true affiliations. For example, a website launched a campaign to free a political figure while funnelling donations for the cause ("Campaign to Free Ahmad Sa'adat," n.d.). Another example involved a Hamas magazine offering paid subscriptions ("Majalat Filastin Almuslima (Arabic)," n.d.). Additionally, an organisation affiliated with Hezbollah ("Al-Shahid") invited website visitors to donate but did not explicitly mention the group's name, only providing contact details ("Mawqie Muasasat Alshahid (Arabic)," n.d.)

In subsequent stages, terrorist organisations exploited established Islamic charities and welfare organisations in the West. These organisations appeared legitimate, raising funds for social causes and aiding the needy in the Arab and Muslim world. This tactic represented a more indirect method of financing terrorism. These charities functioned as fronts, redirecting donations intended for welfare and relief efforts to support terrorist networks. Over time, these groups established various philanthropic entities with websites designed to raise funds. However, these funds were diverted from the social goals advertised and channelled towards the organisations' subversive activities. Unsurprisingly, the activities of some of these organisations were eventually outlawed in various Western countries.

Between 1994 and 1997, two Dallas-based Islamic charities, the Holy Land Foundation (HLF) and the Islamic Association for Palestine (IAP), faced allegations of

providing significant financial support to Hamas (Middle East Quarterly 1997; "Islamic Association for Palestine," n.d.). This activity intensified after the U.S. designated Hamas a terrorist organisation in 1995, forcing the group to move its fundraising activities underground.

The HLF, then considered the leading Islamic charity in the U.S., collaborated with the IAP to raise funds online. They claimed these funds were for humanitarian aid and to benefit Palestinians in need. However, the U.S. government contended that the HLF funnelled over USD 12 million to Hamas-controlled social organisations. The U.S. further accused the HLF of facilitating Hamas activities by disseminating its ideology and recruiting supporters (Department of Justice 2002).

The HLF and the IAP maintained close ties. They shared a web hosting provider, INFOCOM (InfoCom Corporation, n.d.), which hosted websites for roughly 500 other organisations, primarily Arab or Muslim (The Guardian 2001). However, the connection between these three entities went more profound than just location. A senior Hamas official, Musa Abu Marzouk, played a crucial role in founding both the HLF and IAP, as well as INFOCOM. Furthermore, Abu Marzouk's wife was related to the Elashi brothers, who held leadership positions in both organisations. Hassan Elashi, for instance, served as INFOCOM's vice president and the HLF's chairman.

A joint task force raided the offices of an Internet company in September 2001. Muslim sources alleged this action stemmed from a Wall Street article calling for the closure of the company's website and that of another organisation. This raid led to the freezing of assets belonging to both the HLF and the Global Relief Foundation (GRF), an organisation suspected of being an Al Qaeda front. The organisations were ultimately forced to close in December 2001 due to claims that Hamas received a significant portion of its funding from the United States (Fighel 2006). However, a month later, KindHearts, a charity organisation, was established in the USA with the same objective. It encouraged website visitors to donate to establish clinics and aid for those in need in the West Bank and Gaza Strip. Nevertheless, various documents revealed a close relationship between the organ-

isation and Hamas, as well as its support for Hezbollah and in February 2006, the US government froze the organisation's assets due to its ties to Hamas. In December 2002, the US Department of Justice charged Abu Marzouk and the five Elashi brothers with conspiracy to violate state laws prohibiting terrorist financing (Department of Justice 2002).

In August 2007, the Bush administration released a list of 22 charitable organisations, predominantly Islamic, accused of affiliations with terrorist organisations and activities. Several of these organisations, including the HLF, the IAP, Interpal (which primarily raised funds for Hamas from Britain), and the Human Relief Foundation, were implicated in connections with Hamas. Over time, intricate connections were unearthed between these organisations and other Islamic organisations in the US (The Investigative Project on Terrorism 2008). In November 2008, the HLF and its associates were convicted.

A shift in online terrorist financing tactics emerged several years ago. Allegations surfaced that criminal and terrorist networks in the MENA were exploiting online transactions to generate funds. This marked a distinct change from the past, where direct online donations to terrorist organisations were more prevalent.

The new methods involved revenue streams from spam emails and the sale of counterfeit goods. These goods allegedly included medications (Pitts 2006; News-Medical.Net 2009). Additionally, reports suggested that the sale of counterfeit archaeological items also contributed to terrorist financing (Daily Mail 2006).

Society

Numerous MENA regional groups leveraged the Internet to challenge prevailing social, cultural, religious, and political norms that traditionally silenced them. This online space empowered women, particularly those living under restrictions, to share their experiences and advocate for greater equality. Their activism manifested in various initiatives, including dozens of MENA-based organisations promoting women's rights and maintaining a robust online presence.

Women actively used the Internet to address issues ranging from broader societal challenges to specific concerns, such as divorce laws in Saudi Arabia. Additionally, a women-established radio station in Egypt expanded its reach by maintaining an online presence.

Human rights organisations in the MENA extensively leveraged the Internet to document and report human rights violations swiftly and freely. These organisations orchestrated online campaigns advocating for the release of detainees.

Additionally, bloggers and regime critics used the Internet to critique government policies and expose injustices. They also chronicled their activities online, creating a widely disseminated record to protect against potential arrest or disappearance by authorities.

Facebook's most significant social impact in the MENA became evident during the "Facebook Riots" in Egypt in April 2008. Young people actively used the platform to support a planned workers' strike on April 6th. They created groups advocating for a nationwide strike, attracting tens of thousands of members. This online mobilisation spurred a broader movement – a substantial portion of the Egyptian opposition endorsed the strike, and news spread rapidly across the country.

In contrast, pro-government groups on Facebook struggled to gain traction, attracting significantly fewer members. The online activity culminated in street protests and clashes with security forces. Extensive social media reporting on these events further solidified the power of the Internet. It served as a recruitment and mobilisation tool and a vital and sometimes exclusive source of real-time reporting. Notably, the Egyptian case marked one of the first instances where a direct link was established between online activity and physical events – an online protest the government demonstrably translated into real-world street demonstrations.

On April 11, 2009, Egyptian human rights activist and blogger Wael Abbas was arrested by police. Demonstrating the growing power of social media for real-time activism, Abbas used his mobile phone to tweet updates about his arrest directly

to his 2,500 Twitter followers. His tweets garnered significant attention and were closely monitored until his release.

Similarly, American student James Buck from Berkeley, California, leveraged Twitter during his arrest in Egypt on April 10, 2008. Buck, who had documented a demonstration the previous day, sent a single, powerful tweet – "Arrested" – to his global network of followers (Buck 2008). This single tweet rapidly spread the news of his arrest, even reaching his university. Buck, like Abbas, was released the following day.

A vast body of research explores the factors influencing Internet use patterns alongside its societal impact, explicitly focusing on the Arab world.

Paul DiMaggio, Eszter Hargittai, W. Russell Neuman, and John P. Robinson examined the effects of the Internet in five key domains (Dimaggio et al. 2001):

1. Inequality and the Digital Divide
2. Community and Social Capital
3. Political Participation
4. Organizations and Other Economic Institutions
5. Participation and Cultural Diversity

Their research revealed that the Internet generally integrates with existing media and user behaviours rather than replacing them entirely. This integration occurs through three primary mechanisms: the adoption of established media templates, the introduction of specific modifications to existing practices, and the amplification of certain types of social change. Notably, this integration process presented a significant challenge to autocratic regimes within the MENA.

The authors argued that the Internet's social impact in various areas hinges on external factors like economic, legal, and policy decisions that shape its structure. They further suggested that the social effects of Internet use, particularly regarding inequality, are contingent upon the existing societal structures that influence how people use it.

The study highlighted a crucial shift in political discourse driven by the Internet: the emergence of an "engaged public" that actively responds to online information. This replaces the traditional model of a passive "informed public." The research explored how Internet users engage with information through discussion groups and sharing articles with peers.

However, the study also acknowledged potential drawbacks. Concerns arose about the Internet fostering political polarisation, potentially fracturing the cultural unity established by traditional media. Additionally, the anonymity provided online could embolden extremists and facilitate the spread of hate speech.

From a political perspective, the study raised concerns about the Internet's potential to destabilise centralised regimes. The proliferation of online discourse could challenge the legitimacy and stability of such systems.

The Internet's impact on cultural values in the MENA region was multifaceted. On the one hand, it provided a platform for strengthening cultural identity by uniting individuals with shared religious beliefs and facilitating engagement with new members. Online communities fostered a sense of belonging and connection.

On the other hand, the Internet also exposed users to a broader range of information and cultures, particularly Western culture. This access triggered concerns in MENA countries about the potential erosion of traditional values. Religious leaders often viewed the Internet with suspicion, fearing its influence on young people and perceiving it as threatening religious traditions. Consequently, governments implemented website-blocking policies targeting pornography, gambling, and even some health-related sites deemed culturally inappropriate.

A high-ranking Bahraini official highlighted the Internet's potential as a valuable educational and communication tool and emphasised the need for responsible use. He urged authorities to develop strategies to address concerns about Internet misuse. Specifically, the official expressed worries about the potential negative influence of chat rooms and web cameras on young people, whom he

perceived as particularly vulnerable. He warned that such misuse could harm Bahrain's social and cultural fabric (Bahrain Tribune 2005d).

In 1997, Jon Anderson argued that the Internet's significance in the Middle East is "Not a Technological Revolution ... But a Social One" (J. Anderson 1997).

The Internet's vast repository of diverse global information fundamentally challenged state control over information dissemination. The Internet undermined the state's monopoly on news and narratives by enabling access to information outside government-controlled channels. For instance, a 2004 survey in Iran revealed a significant level of trust among Iranians on the Internet compared to other media forms (Committee to Protect Journalists 2005).

Blogs – During times of crisis and change, these websites emerged as a central and essential platform for Iranian residents to share news amongst themselves. Notably, as early as 2002, a vibrant online community of Iranian women writers flourished on various blogs, enabling them to "talk freely about taboo subjects such as sex and boyfriends" (BBC News 2002b). For example, "The Diary of a former prostitute is one of the hottest Web sites in Iran, a strict Islamic society where the Internet is coveted for the access it gives users to a forbidden world".

In the lead-up to the February 2004 elections, the Iranian government's sensitivity to independent online voices was evident. Authorities pressured local media in the preceding weeks, blocking a popular independent website in early January. This crackdown extended to approximately 50 blogs engaged in election discussions and disseminating information about reformist candidates. Iran boasted a vibrant blogosphere with an estimated twenty thousand active blogs.

Rasha A. Abdulla asserted that the Internet's emergence presented vast opportunities for the Arab world across all facets of life, encompassing politics, society, economics, and culture. It emphasised the critical need to unlock the potential for political and media reforms. The argument centred on the notion that the free flow of information would compel Arab leaders to loosen restrictions on individu-

al freedoms within their countries. This, in turn, would erode censorship, cultivate more engaged public audiences, and influence government decision-making processes. Consequently, the underlying assumption was that Internet access could pave the way for more accessible and multifaceted communication, fostering a more democratic, open, and decentralised political system (Abdulla 2005b).

The emergence of the Internet significantly facilitated communication between diverse segments of Middle Eastern society:

- Demography – David J. Atkin, Leo W. Jeffres, and Kimberly A. Neuendorf investigated the compatibility between Internet distribution and demographic factors. It began with the assumption that Internet users differed demographically from non-users, typically younger, more cosmopolitan, and possessing higher education levels, income, interest in innovative technologies, and distinct communication needs. However, the research argued that demographics were insufficient to explain Internet reception. The study contended that other investigations highlighted user needs and media use patterns as more substantial factors influencing how people received new media, including the Internet (Atkin, Jeffres, and Neuendorf 1998).

- Gender – The Internet empowered previously marginalised groups and individuals, particularly women, to circumvent restrictions imposed by mainstream media in traditionally conservative societies. This technology provided unprecedented tools for disseminating their views. Across the Middle East, women actively engaged online, expressing themselves in Arabic, Persian, Turkish, and English. They shared personal stories, discussed societal issues, and leveraged the Internet's anonymity. Some women embraced public platforms, sharing their thoughts through Twitter blogs and feeds. Conversely, others, particularly those in regions with stricter social norms like Saudi Arabia, prioritised anonymity and carefully curated their online audience.

  Their Internet activity encompassed public and private matters, often employing frank, even critical language typically absent from traditional societal

discourse. This phenomenon, particularly online dialogue between the sexes, held profound significance in societies where communication outside the family structure was previously restricted (D. Wheeler 2001).

Saudi Arabia served as a prime example of this phenomenon. Several Saudi women actively leveraged the Internet to advocate for improved women's rights within the kingdom. For instance, Saudi journalist Rim al-Salah emerged as a prominent voice, championing broader societal reforms alongside advancements for women. She particularly criticised the ease with which men could obtain a divorce, highlighting instances where notifications were delivered via fax, potentially without the wife's knowledge. Al-Salah raised concerns about the potential for even swifter divorce methods through SMS or email (’iilaf 2008). Equally noteworthy were the efforts of Saudi journalist Hifa Khalid. In advocating for equitable divorce rights for women, she established an Arabic-language website titled "The Saudi Divorce." This platform documents her organisation's activities and provides a repository of informative materials, including articles and interviews (Khaldu, n.d.). Another prominent figure was Eman al-Nafjan, an English lecturer at a Riyadh health sciences university and mother of three. She actively maintained a year-and-a-half-old blog written in English, which addressed women's issues within the kingdom. Al-Nafjan also published various articles on similar themes ("Saudiwoman's Weblog," n.d.). Zaynab Ghasab, in her writings, explored the motivations of Arab, mainly Saudi, female terrorists, arguing that their actions stemmed primarily from a lack of education or understanding (Ghasiba 2008). Hatun Ajwad al-Fasi, a leading Saudi intellectual, boldly addressed gender inequality during prayers at the Grand Mosque in Mecca (’ajwad alfasi 2008). Writing from abroad, liberal Saudi writer Wajiha al-Haydar took an even more critical stance, advocating for secularism as a potential solution to many of Saudi society's problems (Alhuidar 2008).

Around the region, female commentators treat a variety of subjects. The Palestinian journalist Maryam al-Dahar has attacked the forgiving approach towards Islamist terrorism adopted by Arab satellite television news programs and

called on the Arab public to forthrightly condemn terrorism (Aldaahir 2007). In a recent critique, Syrian intellectual Marah al-Baka, living in exile, levelled her criticism of Arab society. She had explicitly condemned the prevalence of ignorance and closed-mindedness, arguing that these traits contrasted with the intellectual openness she had encountered in Western societies (Albiqaeiu 2007). In a similar vein, Syrian American psychiatrist Wafa Sultan lashed out against the absence of freedom of expression in the Arab world during a controversial Al-Jazeera TV interview. This interview coincided with the uproar surrounding the Danish cartoons of the Prophet Muhammad (itayzil 2006). In Kuwait, the writer Ibtihal Abd al-Aziz al-Khatib condemned the absence of an Arab equivalent to Israel's Winograd Commission, which investigated the government's and army's conduct in the 2006 Lebanon War, emphasising the lack of accountability of Arab leaders (Eabd Aleaziz Alkhutayb 2008).

In pursuing gender equality, Egyptian women strategically employed the Internet. One prominent example is the "We Are All Layla" website. For the past three years, this platform has emerged as a powerful voice against everyday injustices faced by women. The organisation's affiliated Twitter account further amplifies this message by providing resources on regional women's issues 'Kuluna Laylaa (Arabic)', n.d.). The esteemed physician and feminist icon Nawal al-Sa'dawi has a long-standing campaign against female circumcision. In recent years, she, along with other activists on this issue, has harnessed the Internet's power to disseminate her message further. Activist Fatma Na'ot (Naeuti 2008) and human rights campaigner and blogger Dalia Zaida both vehemently condemned the lack of religious tolerance shown towards Egypt's Coptic minority ("Dalia Ziada Blog," n.d.)

One prominent Iranian blog, "Change for Equality" ("Change for Equality," n.d.), emerged as a vital platform addressing the status of women. Their activism garnered recognition, earning them an award from Reporters Without Borders. Notably, the blog spearheaded an initiative to collect one million signatures for a petition demanding reform of discriminatory laws against wom-

en. This effort reflects the significant price many Iranian female activists have paid in their fight for women's rights, facing arrests and imprisonment for their cause (Reporters Without Borders 2008b).

Organisations like the "Iranian and Kurdish Women's Rights Organization" and the "Revolutionary Association of the Women of Afghanistan" (RAWA), among numerous others, leveraged the Internet to champion minority and women's rights and advocate for greater social justice.

The Internet has amplified the impact of diverse women-led local initiatives. Notably, it facilitated a boycott by Saudi women of lingerie stores staffed exclusively by men (Middle East Online 2009). It also empowered Egyptian women to launch and operate a radio station dedicated to their needs and interests. Similarly, online platforms enabled criticism of Saudi religious pronouncements, seeking to exclude women from the media (Ghashmary 2009). The Internet has become a multifaceted space for social interaction. While it facilitates connections between men and women ("Arab Lounge," n.d.) and shares details from women's daily life "under headscarf" ("Love in a Headscarf," n.d.). It plays an even more crucial role for LGBTQ+ communities across the region. Online platforms provide them with essential social support and opportunities for personal connections, fostering a sense of community that may be difficult to establish offline due to social restrictions ("Alwaan - Arab Lesbian Women & Allies Network," n.d.)

The Internet undeniably served as a platform for amplifying diverse women's voices and perspectives. While gender does not inherently define online expression, the proliferation of "women's spaces" online has undeniably broadened the discourse on social change in the region. These online platforms have challenged the status quo and advocated for shattering the glass ceiling that restricts women's fundamental rights (Tucker 2009).

- Virtual Communities – The Internet emerged as a powerful tool for fostering greater understanding and connection within the Arab world. Websites and

virtual communities dedicated to Islam, Muslims, and pan-Arab discussions blossomed online. These platforms often functioned as alternative media, facilitating communication between diverse groups and disseminating information to the public. This democratisation of information exchange has fuelled the potential for a more active and engaged Arab society, even sparking discussions about the possibility of a "virtual Pan-Arabism" (Alterman 1998; Abdulla 2005a; J. W. Anderson 1997).

Virtual worlds have evolved significantly, blurring the lines between the digital and physical realms. These increasingly complex platforms allow users to construct 3D environments, embodying themselves through avatars and incorporating real-world elements. A prime example is Second Life (SL), launched in 2003, where user-created content is copyrighted. This system fostered a thriving virtual economy, where real-world money could be exchanged for virtual goods, effectively intertwining the two economies. Notably, Second Life witnessed a surge in user engagement, with usage hours increasing by 33 per cent and the virtual economy growing by 94 per cent in the second quarter of 2009 compared to the previous year.

These virtual worlds extended their influence on the MENA region, impacting various aspects of life. One prominent example was Muslim Pal (pal.muxlim.com), launched as the "first Muslim virtual world" offering a family-oriented online social space. This platform strictly prohibited drugs, alcohol, and inappropriate behaviour, aiming to create a safe environment. Muslim Pal fostered communication and understanding between Western and Eastern cultures, aiming to unite Muslim communities globally, particularly those in the West. Reflecting this goal, the platform welcomed Muslims and non-Muslims (Hamidoui 2009).

Second Life offered a remarkably diverse range of activities within the MENA region. Notably, it featured dedicated virtual islands for Saudi Arabia and the Middle East, attracting roughly 25,000 users each, alongside 34 additional

Arab islands. These virtual spaces functioned as hubs for social interaction, cultural exchange, and even business ventures, facilitating communication and gatherings that might be difficult to achieve in the physical world. Religious activities flourished online, with virtual pilgrimages to Mecca, mosque tours across the Arab world, lectures by religious scholars, and discussions on religious topics. Beyond religious activities, these virtual spaces served as platforms for demonstrations concerning the Israeli-Palestinian conflict, fundraising initiatives for Palestinians in Gaza, and even Iranian protests mirroring real-world events following their presidential election.

A 2007 survey revealed a regional hierarchy of Second Life users, with Turkey and Israel leading the way. Egypt, the UAE, and Saudi Arabia followed that order. Notably, Iran, a regional Internet powerhouse, surprisingly ranked eighth among the twelve countries surveyed. This discrepancy likely stemmed from the Iranian government's strict Internet restrictions, including bandwidth limitations. However, limitations exceeded policy; using Second Life required specific technological capabilities. Installing and running the software necessitated a modern operating system (XP or higher), robust graphics processing, and a high-speed Internet connection (broadband only). These technical hurdles undoubtedly contributed to the lower user base in Iran.

The 2007 survey revealed a stark disparity between regional Internet penetration and Second Life usage. While the Middle East boasted Internet users, they only constituted a meagre one per cent of Second Life's global user base – half the regional Internet user proportion. This discrepancy extended to engagement, with actual usage measured in hours even lower. Two primary factors contributed to this: limited broadband penetration and government restrictions. The region's broadband penetration rate hovered around 2.55 per cent during that period. This stemmed from inadequate communication infrastructure in some cases and, in others, deliberate decisions by authorities. These limitations on high-speed Internet access undoubtedly hampered the widespread adoption and use of virtual worlds like Second Life in the Middle East.

- Tradition – Respect for tribal and religious codes traditionally fostered deference towards ruling leaders in the region. This social norm often translated into government censorship practices. Websites deemed critical of the government, the ruling family, or Islam – or offering alternative interpretations of Islam – were particularly vulnerable to blocking (Singh 2000).

- Diaspora – The Internet emerged as a powerful tool for connecting and empowering Arab diaspora communities in the Arab world. In 1997, the Middle Eastern presence online was primarily comprised of these diaspora groups – immigrants, expatriates, migrant workers, and students. The Internet provided them with a platform to connect with others worldwide, fostering the creation of online discourse communities that transcended traditional political and religious boundaries (J. W. Anderson 1996). Migration is accompanied by a change in 'intellectual technologies' that challenge accepted religious and social views, the frameworks of thought, and the social foundation. Migration often entails a shift in "intellectual technologies," challenging established religious and social views and thought frameworks. The Internet, typically used in English by these communities, was a crucial tool for maintaining connections to their home countries and each other. This was achieved through sharing expatriate experiences, cultural event updates, discussions about home-country issues, and discourse on religion, politics, and society – topics that might have been more restricted in their countries of origin. This online activity led to their portrayal in some home countries as "new barbarians," seen as bypassing existing restrictions by creating new, intellectually and practically legitimate frameworks for community and communication. Consequently, Muslim communities in the West felt a lessened sense of minority status while experiencing a significant increase in the frequency and range of their international connections. The Internet thus played a crucial role in boosting their self-confidence and solidifying their Muslim identity (Sedgwick 1998).

- Religious interpretation – The Internet revolutionised access to religious information and interpretation. Online platforms offered a multitude of viewpoints and variations within Islam, which some governments viewed as a potential

threat to stability. Additionally, the Internet challenged traditional methods of acquiring religious knowledge. It facilitated exploring diverse and contemporary Islamic studies programs, offering alternatives to established learning methods and degrees (Sedgwick 1998).

- LGBTQ+ – The Internet made it possible for the LGBTQ+ community to "declare their existence" since "Homosexuals might be the only social group in the Arab World that was completely unable to declare its existence publicly until the appearance of the Internet. To declare yourself leftist, Islamist, Shiite or Nasserist means to expose yourself to some security, cultural or religious problems; to declare yourself homosexual means exposing yourself to every single one of these problems" (The Arabic Network for Human Rights Information, n.d.-c).

  The limitations on Internet freedom in the Arab world, particularly for the LGBTQ+ community, are exemplified by the safety guidelines offered on a Saudi Arabian LGBTQ+ website. These preventive measures highlight the dangers users face from authorities while browsing online:

  1- "Many do not tell the truth.
  2- Do not use your real name.
  3- Use a private and confidential email address.
  4- If someone wants to meet you, it is less cool than you might think.
  5- Do not give your address to anyone.
  6- Do not give the phone number to anyone.
  7- Your name must be fake.
  8- The Internet can be great fun, but be careful.
  9- If someone hurts you, tell the one you trust" ("Almithliiyn Alearab (Arabic)," n.d.)

- Porn – Similar to users in other cultures, Arab Internet users sought to fulfil sexual needs online. Due to the region's conservative, traditional, and religious nature, social and religious barriers often limit communication between genders. The Internet, however, offered unprecedented access to information, including a vast amount of sexual content. This ranged from online interactions

for social connection and getting to know each other to passive consumption of pornography and even active participation in online sex. The Internet undoubtedly served as a significant outlet for these user needs, with evidence suggesting a considerable volume of such activity.

The Internet's unrestricted access to content, unavailable through traditional channels, extended to pornography. The quote, "The cultural controls imposed on people living in the Arab world make them hungrier to explore the world of dot-com sexual thrills", suggests that the cultural restrictions imposed on Arab societies fuelled a heightened interest in exploring online pornography. A 2001 claim, though likely inflated, highlighted the potential scale of this phenomenon, suggesting that 80 per cent of Internet traffic in the Arab world may have been directed towards adult websites. Therefore, "The United Arab Emirates, like many other countries in the Arab world, block users from accessing such content" (Kettmann 2001a).

A 2004 report by a journalist visiting an Internet cafe in Damascus revealed a significant youth presence, with 90 per cent of users identified as young. The cafe owner attributed his livelihood to these young patrons, suggesting their primary online activity was accessing pornography.

This demand for pornography among Middle Eastern Internet users manifested in two primary categories: general and Western websites and content specific to Arab society. Unique to the region, the latter category became more intriguing due to its unexpected nature.

For this purpose, you can find a site with sex videos which will be distinguished as being active in Arabic as well and claims that all the videos are in Arabic and were filmed with the participation of hundreds of women from around the Arab world ("Arabic Sex Movies. Arab Girls - Arab Sex Models - Arabicsex," n.d.) Different websites, in a variety of languages, of pornographic videos and photos of women from the Arab world ("Arab Sex," n.d.; "Free Arab Sex Movies | Arabsex Pictures | Arabic Porn Videos," n.d.; "Bnat-Zone," n.d.; "Arab-Slut," n.d.) All of them are inactive nowadays.

A notable trend emerged in which women were photographed engaged in sexual acts while adorned in traditional clothing, including headwear. This seemingly paradoxical practice served two purposes, as some scholars have argued. Firstly, it presented a facade of authenticity, implying that the films depicted genuine sexual practices within the Arab world. Secondly, it emphasised the "forbidden fruit" aspect, potentially appealing to viewers due to the juxtaposition of traditional attire and sexual content.

Consequently, governments in the Middle East have consistently expressed concern over pornography and online sex. These anxieties stem from historical events and the perceived threat to societal, cultural, and religious values.

Non-sexually explicit web content – In a 2002 field study, Jonathan Zittrain and Benjamin Edelman of Harvard Law School's Berkman Center for Internet & Society investigated the prevalence of filtering and censorship on Saudi Arabian Internet sites (Zittrain and Edelman 2002). Their research involved connecting to the Internet through servers in Saudi Arabia and attempting to access approximately 60,000 web pages. This process aimed to determine the extent of Internet filtering the kingdom employs. The researchers identified roughly 2,000 blocked pages, encompassing content related to religion, health, education, humour, and entertainment. The study's conclusions were: The Saudi government implemented a system to filter non-sexually explicit web content for users within the country. This filtering rendered a significant portion of this content inaccessible to most Saudi residents. Interestingly, much of the filtered content originated from websites experiencing a surge in global popularity.

However, this experiment has several drawbacks:

1. **The duration of the experiment** – The study's limitation was its brief duration. The researchers only modelled the state of the Internet filter in Saudi Arabia over two weeks.
2. **The location of the experiment** – conducting field experiments on users' computers, isolated from the filtering body's infrastructure, offers more ex-

cellent reliability than collaborating directly with the Internet Service Unit (ISU), the entity responsible for Internet filtering in Saudi Arabia. This argument is supported by the following quote "With the permission and cooperation of ISU staff, we obtained access to the ISU's proxy servers from 14 May to 27 May 2002."

3. **The scope of the experiment** – An examination of the study's description suggests it analysed approximately 60,000 web pages, not entire websites. Websites can encompass numerous web pages, potentially impacting the comprehensiveness of the findings. Including a broader range of websites, rather than focusing on many pages from a limited set of websites, would likely yield a more reliable and representative picture of Internet filtering practices.

An early 2004 experiment by the OpenNet Initiative in Saudi Arabia investigated website filtering practices. Researchers used the Google search engine to identify websites returned when searching for "Gay" ("Bulletin 002" 2004). They then employed Google's SafeSearch feature, designed to filter out websites with explicit sexual content, to verify the results. Subsequently, five separate computers in Saudi Arabia verified each identified website address.

Also, this experiment has several drawbacks:

- **The experiment** – This experiment functioned as a one-time assessment of website accessibility within Saudi Arabia. It focused on determining the accessibility of selected websites at a specific point in time. Consequently, the study did not examine how accessibility might fluctuate over time.
- **The location** – Another limitation is the experiment's geographic scope, which is limited solely to Saudi Arabia. This and the study's brief duration restrict the findings' generalizability.
- **The scope –** While the experiment analysed many websites (913), it focused solely on a single thematic category: the LGBTQ+ community. Additionally, researchers exclusively employed Google as the search engine for website discovery.

Economic

To bolster its legitimacy and popularity, the state actively invests in Internet development, including establishing high-tech industry zones. This strategy hinges on the belief that economic growth and modernisation will increase public support for the regime. However, such growth can inadvertently empower new social forces. A burgeoning business elite and a strengthening middle class may eventually challenge the regime's absolute control by demanding greater political participation. These empowered groups can further leverage the Internet's unique characteristic – its non-perishable nature – to facilitate collaboration and information sharing across borders. This potential for regional cooperation, even within individual states, suggests that the future of Middle Eastern economies may lie in information-based structures.

- Inter-Arab trade – The Internet has emerged as a powerful communication facilitator between businesses across the Middle East. Notably, it empowers Arab companies, particularly those within the Internet sector, to connect directly with regional customers. This eliminates geographical barriers, allowing products to reach consumers in other countries instantaneously and often at a significantly lower cost than traditional methods employed by local governments. Furthermore, the Internet fosters the creation of e-commerce opportunities, enabling seamless cross-border transactions (Alterman 1998).

  Unlike the Western world, where academics spearheaded the Internet's development, the Arab world witnessed a unique trajectory. Here, commercial users emerged as the primary drivers of Internet growth. Fueled by their traditional business understanding and capacity for ambitious investments, these commercial entities and enterprises outpaced the efforts of government research institutions and universities, which often lacked the resources or vision to keep up. Consequently, the Internet in the Arab world became synonymous with fostering communication, commerce, and information exchange (J. Anderson 1997).

The Internet's potential to empower diverse groups in the Middle East and its capacity to provide a platform for expressing dissent previously suppressed by authorities presented a significant challenge for regional governments. In response, these governments implemented measures to restrict Internet access and limit online activity within their borders. The history of Internet adoption in Middle Eastern countries can be broadly divided into three distinct stages (The Arabic Network for Human Rights Information, n.d.-c):

1. **Initial Promotion**: Governments initially encouraged Internet adoption by promoting its use within government bodies and facilitating computer acquisition for residents.
2. **Unforeseen Consequences:** This initial enthusiasm was tempered by the realisation that the Internet provided unfettered access to information beyond government control, including content from opposition parties, human rights groups, and diverse fringe groups.
3. **The Shift Towards Control:** In response to these concerns, governments transitioned towards a more restrictive approach. This involved implementing measures to regulate Internet use and potentially limit access, ostensibly safeguarding religious, cultural, and political values.

Chapter 5 – Cyber Threats in the MENA

Examining cyber threats in the MENA region reveals two key dimensions: the **motivations** behind the attacks and the **attackers' identities**.

- Technically – an analysis of website attacks worldwide during the 2005-2007 period revealed that, in many cases, hackers were primarily motivated by a desire to showcase their technical prowess and expose vulnerabilities in website security. This often involved leaving a warning message on the compromised website, highlighting its weak defences. Sometimes, hackers even offer services to improve the site's information security. These findings support the notion that personal prestige, enjoyment of the challenge, and the thrill of accomplishment were the dominant motivations behind website attacks; for social and ideological reasons, while present, appeared to be less prevalent (Almeida, n.d.).
- Between countries – online attacks on a country's websites allegedly carried out by another country with which it is in conflict. Such attacks were relatively rare in the Middle East during the period in question.
- Political – governmental and opposition organisations within the same country engaged in online mutual attacks.
- Nationalists – residents or supporters from another country launched online attacks against websites belonging to or associated with a specific country. These attacks, primarily driven by ideology rather than government direction, were carried out independently.
- Religious – carrying out online attacks for religious reasons both against the West and Israel and in internal Islamic struggles.
- Economic – Unlike most attacks in our region, economic motives primarily drove online attacks fueled by political, nationalistic, or religious agendas.

Analysis of online attacks revealed a clear division between government and user targets and between attacker types at each level.

	Government	**Individual**
Attackers	Governmental Cyber agencies	Script Kiddies, Hacktivists, cyber terrorists, Cybercriminals
Targets	Specific high-profile institutional and individual targets	Various websites without any distinction. Some may be with high visibility.
Cause	Intelligence and information gathering, Sabotage and Destruction	Ego, entertainment, protest, money

The Attackers - information warfare in the Middle East is often carried out by experts, individually or in groups, who contribute their expertise to creating an online layer for physical conflicts. This activity exists in several circles and towards several arenas.

- The west
- Rival parties in the Arab and Islamic world
- Israel

The West

The rise of Arab and Muslim hackers targeting Western websites in the early 2000s stemmed from ideological, nationalistic, religious, and personal motivations centred on enhancing their technical reputations. As the decade began, various Western sources expressed apprehension about the threat of online attacks and website defacements by extremist Islamic groups, particularly against banking, commerce, and financial sites. As early as 2002, experts cautioned that Al Qaeda's warnings of cyber-attacks on economic targets in the West should be taken seriously. This concern arose from the presence of technically skilled youth within these communities who had acquired advanced education and proficiency in hacking techniques, asserting that "There are millions of Muslims around the world involved in hacking the Pentagon and Israeli government sites" (News.lt 2002).

In December 2006, a United States government expert issued a warning about the potential for Al Qaeda to launch cyber-attacks against financial websites. This

caution followed the appearance of a message on a jihadi forum frequented by young hackers, which called for such attacks as retaliation for the detainees held at the Guantanamo Bay detention camp. The expert's advisory underscored the credible threat posed by the convergence of extremist ideology and technical capabilities within this online community. "In a matter of time, you will see attacks on the stock market" and "I would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies". Alongside fear of cyber-attacks against critical infrastructure, "Cyberwarfare attacks against our critical infrastructure systems will become an increasingly viable option for terrorists as they become more familiar with these targets and the technologies required to attack them". The expert tried to downplay the importance of the matter and claimed that Al Qaeda hackers are less sophisticated than their Russian counterparts (D. Kaplan 2006).

Ideological motivations and a desire to enhance their reputations as skilled hackers drove a series of cyber-attacks against Western websites. Operating within this context, the Turkish hacking group NetDevilz successfully breached the Internet Corporation for Assigned Names and Numbers (ICANN) and the Assigned Numbers Authority (IANA) websites in June 2008. These two international organisations serve the critical function of regulating the unique identification systems that underpin the Internet's infrastructure. The group's ability to compromise these pivotal entities demonstrated their technical prowess while aligning with broader ideological agendas advocating anti-Western sentiments through disruptive online operations (Almeida and Fernandez Kevin (Siegfr) 2008).

The technical capabilities and ideological motivations of hackers in the Middle East found tangible manifestation in March 2003, coinciding with the commencement of the U.S.-led coalition's military intervention in Iraq. During this period, thousands of Distributed Denial of Service (DDoS) attacks targeted servers in the United States, the United Kingdom, and the Arab world. These coordinated cyber-attacks served as a compelling demonstration of the region's hacking proficiency, which was harnessed to advance broader ideological objectives and ex-

press opposition to the ongoing conflict (Rantanen 2007). In the lead-up to the attack, hackers defaced an average of 350 websites daily. This number spiked to 2,500 websites per day following the attack, with an additional surge to 1,000 on weekends (Lemos and Fried 2003).

The publication of 12 cartoons depicting the Prophet Muhammad in the Danish newspaper Jyllands Posten on September 30, 2005, triggered a wave of online attacks several months later. In early February 2006, attackers targeted Danish servers, launching over 600 attacks. European and Israeli servers also came under fire, with more than 400 additional attacks registered (Ynet 2006). In most instances, the attackers defaced the websites and left condemnatory messages towards Denmark, with some even including threats of suicide attacks.

Even several years after the controversy surrounding the Prophet Muhammad cartoons, Danish and foreign websites that displayed messages condemning the event remained vulnerable to attacks. In July 2009, hackers launched a coordinated assault on hundreds of such websites. These attacks involved defacing the sites and replacing content with messages critical of Denmark, such as defacing the Danish flag with a symbolic image (e.g., a foot) and the inscription "AnTi Europa and America and Israel" (Abohamza Almohajir 2009).

In response to Israel's Operation Cast Lead in Gaza (January 2009), Turkish hacker group Agd_Scorp launched a cyber-attack campaign. The group, responsible for hundreds of previous defacements, targeted the websites of the US Army and NATO Parliament. Breaching these websites, Agd_Scorp defaced them with messages in Turkish and English condemning Israel's military actions (R. Preatoni 2009; Agd_Scorp, n.d.)

In a display of nationalist fervour, Turkish hackers targeted Western websites in August 2008. One such instance involved the defacement of Olympic swimmer Michael Phelps' website. The hackers replaced website content with patriotic and nationalist messages, including a link to a Turkish-language website featuring national motifs. Security experts attributed the attack to teenagers seeking to

showcase their technical skills and express nationalist sentiment by targeting a high-profile website (D. Kaplan 2008).

Arab and Islamic world

The online arena has emerged as another battleground for struggles within the Arab and Islamic worlds. Like other contested spaces, this phenomenon is driven by a multitude of factors and plays out at both the state and individual user levels.

Technically – In some instances, website defacements serve as a public display of technical prowess for attackers. Hackers exploit security vulnerabilities to gain access to websites and leave messages highlighting the breach. This tactic is a form of self-promotion, showcasing their capabilities and technological skills. A well-known example of this approach is the activity of Muslim hacker "altbta," who targeted various websites and left messages claiming the attacks were solely technical warnings (ALTBT, n.d.):

"Hacked By ALTBTA
First Warning That is Bug From Your Servers
Next Time You Must Be Careful And Fixed Your Site Before
Coming Another Hacker And Hacked You Again
Sorry Admin And Don't Worry Just I changed Index."

Similarly, Saudi hackers operating under the aliases S4UDI-ZO0M and S4U-DI-J0K3R infiltrated a Saudi government website related to the education system. The hackers defaced the website with a message, "ooops...!! There is a vulnerability," seemingly to raise awareness of the security breach. They further provided a link to a forum, potentially offering a solution to the exposed vulnerability.

Politically – Between 2007 and 2009, government actors in Tunisia, Libya, and Mauritania targeted opposition organisations online. Hackers affiliated with these governments launched attacks that defaced and sometimes even destroyed over 20 opposition websites (Ben Gharbia 2009).

- Tunisia – Between 2007 and 2008, seventeen websites critical of the Tunisian government were hacked. This included seven website defacements and three complete website deletions in 2007 alone. The targeted websites primarily consisted of blogs, news outlets, opposition organisations, and protest groups advocating for increased freedoms and reporting on the human rights situation in Tunisia. The extensive nature of these attacks, impacting nearly all opposition and independent online platforms, led opposition groups and human rights activists to suspect government involvement (Ben Gharbia 2008b; Rjiba 2008).
- Libya – Six opposition websites were hacked in January 2009. The websites were defaced, and content from a private website presenting Gaddafi's activities and vision was placed on them. Four of the six sites did not resume operation.
- Mauritania – Hackers targeted two news websites whose editors had previously published accusations against the current military regime. The attack also disrupted the websites of several national and external organisations.

In response, some users engaged in online activism by launching cyber-attacks against government websites.

- Morocco – On July 18, 2009, a Moroccan hacking group called !TeAm RaBaT-SaLe! breached the website of the Arab Water Council (an inter-Arab organisation headquartered in Cairo). This attack was launched in protest of the Council's activities. The hackers defaced the website and posted content in Arabic condemning governments that sell Arab water resources to foreign entities (!TeAm RaBaT-SaLe!, n.d.-b). In a broader cyber-offensive, the group also hacked into dozens of other websites, regardless of affiliation. These compromised websites displayed content and images critical of Israel, Denmark, and the USA (!TeAm RaBaT-SaLe!, n.d.-a).
- Iran – Following the violent protests that erupted in Tehran's streets after the June 12, 2009, presidential election, supporters of Mir Hossein Mousavi and the Iranian administration engaged in a series of website attacks against each other. The conflict spilled over to the global web, with various Iranian govern-

ment websites and international platforms being hacked (DATA ir Security Group, n.d.) In this context, a hacking group called Freedom. IRAN emerged in the latter half of July 2009. They targeted dozens of websites, primarily Russian (including a government site), and defaced them with messages condemning Iran and Russia's support for the regime. These messages, written in English on a green background (symbolic of Mousavi's campaign colour), were accompanied by photos from the Tehran demonstrations (Freedom.IRAN, n.d.).

- Palestinian Authority – A report surfaced on the Fatah movement forum (alqudsinfo.com/vb) in April 2008, detailing the hacking and takeover of an organisation's website by members affiliated with Hamas. The organisation's Internet radio station reportedly began broadcasting a sudden influx of Hamas songs (Abu Omar 2005). A similar event was recorded at the beginning of July 2009 when the Gaza Hacker Team hacked the same forum (Gaza Hacker Team, n.d.-a). On the vandalised website was placed a picture of Ismail Haniya and a message in Arabic attacking the US and the Palestinian Authority government, which they say will lead the Palestinians to further division. The announcement was signed with "Your brothers: the pirates of Gaza."
- Nationalist – In January 2008, Moroccan hackers launched cyber-attacks against Spanish and Algerian websites in protest of border closures imposed by Morocco's neighbours. The Spanish border closure targeted refugees from Morocco, while the Algerian closure stemmed from the Western Sahara issue (Shabakat alfaysal nit 2008). Additionally, they hacked into the website of the Africa Cup of Nations competition hosted in Ghana that same month. They posted messages of support for the Moroccan team following their defeat to the host nation (Mahmoud 2008).

  During the conflict between Armenia and Azerbaijan, hackers affiliated with both countries targeted each other's websites. Azeri hackers vandalised Armenian websites, placing messages condemning Armenia. Turkish hackers also participated in these online attacks. Similarly, a separate online conflict emerged between India and Pakistan, where hackers from both sides launched attacks against each other's websites (Barak 2008).

In protest of the Chinese authorities' treatment of the Uyghur Muslim minority and support of their demonstrations, a wave of cyber-attacks targeted Chinese websites, primarily launched by Turkish hackers (1923Turk, n.d.). A prominent Turkish hacker known as "Swan" spearheaded these attacks, compromising hundreds of websites and defacing them with a consistent message: "Stop the genocide of the Uyghurs." "Swan" taunted the targeted sites with messages like "Security - 0, my experience - 1" and "revenge time." However, in June 2009, "Swan" shifted focus, launching similar large-scale attacks on websites worldwide. These attacks included messages condemning Israel alongside expressions of support for the Ottoman Empire.

Notably, Turkish hackers appear most frequently among these attackers. Furthermore, their actions often exhibit more nationalistic influence than other groups. This is evident in their choice of hacker aliases ("1923 Turk" and "Ottoman-empire" (ottoman-empire, n.d.)) and the content they place on defaced websites.

Iranian hackers also exhibit nationalist motivations in their online attacks. The activity of the "Persian Boys Hacking Team" exemplifies this trend. Documented activity from this group dates to October 2007, when they defaced a website with the following message (PowerDream, n.d.);

"We Are Descent Of Great King Cyrus"
Over the past few days, the design of the corrupt pages has changed. The following message was posted;
"Islamic Republic Of Iran Is Successful And Powerful In All Of The Subjects".

- Religious - Two primary fault lines have emerged in online religious conflict within our region: one targeting Christianity and the West, and another focused on the Sunni-Shia divide within Islam.
  - **Islam-Christianity** – In response to Pope Benedict XVI's speech at the University of Regensburg on September 12, 2006, which addressed the complexities of Christian-Islamic relations, a two-week wave of cyber-attacks emerged. These attacks targeted approximately 5,000 Christian and other

websites, defacing or destroying them. The motivations behind the attacks were primarily religious and nationalistic, with a strong emphasis on Islamic protest (R. (SyS64738) Preatoni 2006b).

Following the website defacements, attackers posted messages condemning Christianity, Israel, and the Iraq War. These messages often included links to various websites, some containing information about Islam. The messages varied in length and detail but most directly targeted the Pope. For instance, H4ck3rsBr's attacks on Italian sites and the Turkish group AYYLDIZ VIP TEAM both issued direct appeals to the Pope, urging him to cancel a visit (presumably to a specific country).

In a separate incident in July 2009, a Turkish hacker known as "King_Wolf" defaced a website for apparent Islamic missionary purposes. A lengthy document was uploaded onto the compromised page, with the opening section providing clues about its content (King_Wolf, n.d.):

"INVITING CHRISTIANS TO DIVINE GUIDANCE AND TRUE SALVATION

(This brochure has been prepared to briefly describe the Islamic belief in Allah and the status of Jesus (may the peace and blessings of Allah be upon him (PBUH)) as well as to invite Christians to the path of righteousness and redemption)."

- **Sunna-Shia** – In October 2008, amid ongoing tensions between Sunnis and Shias, the Al-Arabiya news website and its associated websites were targeted in a cyber-attack. The perpetrators, believed to be Shia hackers, defaced the websites and posted a warning message. The message threatened that if attacks on Shia websites continued, retaliation would come in the form of hacks against Sunni websites (Aleuayjan 2008). To bolster their claims, the attackers appended a list of over one hundred Sunni websites they asserted had been compromised. According to the hackers, this action responded to accusations of bias in Al-Arabiya's reporting. News outlets also reported that a screenshot of the defaced website circulated online alongside a message urging Muslim unity against a common enemy and downplaying the attack as a mere warning (Alhamdan 2008). Al-Arabiya, on the other hand, coun-

tered that the attack was part of a more significant cyber conflict between Sunni and Shia hackers who routinely target each other's websites. They pointed to instances where websites of religious scholars from both sects had been compromised. One article affiliated with the station even argued that "destroying a website or hacking into it to disable it are acts equivalent to killing or burning," highlighting the strong emotions fuelling these online battles. This is an activity that eliminates the other"; these are "acts of virtual destruction and killing through an attack on websites belonging to religious people, politicians or the media" (Zaman alwasl 2008).

Online attacks with religious motivations extend beyond targeting rival sects. Some incidents aim to undermine religious institutions, interpretations, or moral codes. For example, hackers compromised a forum (alhak.org/vb containing cultural and religious discussion rooms, where they posted messages reviling the prophet and his wives (3abdelbasset 2007). In another incident, the owner of "The Arab Story" website, hacked in November 2008, condemned the attackers for distorting Islam and using it as a justification for cyber-attacks. He argued that the Internet can be a powerful tool for promoting positive values, tolerance, and interfaith dialogue. Additionally, he emphasised its potential for disseminating Islamic culture and language. The owner reassured users of the website's restoration and thanked his supporters (admin 2008).

Religious justifications are also cited in some website defacements. For instance, the "Gaza Hacker Team" (Gaza Hacker Team, n.d.-b) targeted an Arab forum (9n5.net/vb), defacing it with messages condemning the site for allegedly hosting pornographic content.

- Economic – Ransom-motivated cyber-attacks, while not a prevalent trend, have emerged. In a 2006 first for Pakistan, attackers compromised the Center for Development and Peace Initiative (CDPI) website. The intrusion involved changing passwords, effectively blocking access to the website's data. The attackers then demanded a ransom payment to restore standard functionality (Chickowski 2006).

Israel

Arab and Muslim hackers frequently target Israel in the online sphere. This readily accessible and influential platform serves as a tool for their conflict, leading to routine attacks on both Israeli and international websites. Website defacement often functions as a means of disseminating messages critical of Israel. Notably, these attacks extend beyond Israeli websites, encompassing unrelated sites around the world. Hackers frequently deface these non-Israeli websites with messages condemning both Israel and the West. During the period under review, they witnessed a surge in website defacements targeting Israeli sites, with a significant escalation during wars and military operations.

- **Turkey**
  - The Ayyıldız Tim – A prominent hacking group, has been linked to over a thousand attacks since May 2005. According to a report by the Israeli Arab newspaper Panorama, the group actively targeted Israeli websites during the Second Lebanon War. Notably, the National Road Safety Authority's website was among those compromised (Zarqawi 2008).
  - dr.militan-53! – A Turkish hacker emerged in late 2008 and has since been linked to the defacement of hundreds of websites, including those in Israel. These attacks typically involved replacing website content with Dr.militan-53!'s email addresses and a self-designation as a "Turkish Defacer," but lacked any additional messages.
- **Morocco**
  - Team-evil – A hacking group believed to have originated around 2004, first gained notoriety for targeting Israeli and Jewish websites, as well as government websites globally. However, their most extensive documented activity began on June 28, 2006, coinciding with Israel's "Operation Summer Rains" in the Gaza Strip. On the first day of the operation alone, the group compromised and defaced over 750 Israeli websites. This attack marked a significant escalation in both the scale and sophistication of their targets, encompassing websites from banking institutions, hospitals, and various

companies. Additionally, the defaced websites displayed messages with Islamic themes, composed in improved English compared to previous attacks. Technical reviews of the group's attacks conducted in July 2006 and subsequent analyses provide evidence of their activity (Damari, Chayun, and Evron 2006; Mor and Kinan 2006).

- M0µ34d – A Moroccan hacker has incorporated anti-Israel and anti-Western content into compromised pages, targeting various websites.

- **Algeria**
  - The Moorish – The hacker's attacks primarily targeted Israeli websites, including the English-language website of the Bank of Israel. These attacks occurred in two major waves: the first coinciding with the conclusion of Israel's "Operation Warm Winter" in February 2008, and the second near the end of "Operation Cast Lead" in January 2009.
  - Dz-Boys Team – A hacking group targeted several Western websites in July 2009, defacing them with messages critical of Israel (Dz-Boys Team, n.d.);

    … From The River To Sea, Palestine Will Be Free

    Don't Tell Me To Stop..

    you kill kids, and we kill your servers.

- **Saudi Arabia**
  - aB0 m0h4mM3d – Ideologically motivated, this attacker launched a series of website defacements targeting hundreds of sites primarily in the Netherlands, Denmark, and Israel, extending to other countries from September 2008 onwards. Each wave of attacks compromised dozens of websites, which were then defaced with extensive anti-Israel, anti-Danish (in the case of Danish targets), and potentially broader anti-Western content in text, image, and video formats. When targeting Danish websites, the attacker specifically called for protests Israel and the Danish government's support for it. In other instances, the messages issued a more general call to action against Israeli activities (aB0 m0h4mM3d, n.d.)

    The attacker also targeted Iranian websites, which he defaced with anti-Shia content. Additionally, some website defacements were motivat-

ed solely by the challenge of hacking itself. Beyond these instances, the overall pattern of website selection suggests an ideological purpose, potentially reflecting a broader Islamic protest in the political climate in the Middle East.

- **Iraq**
  - GHOST OF IRAQ – Over several months, this group targeted hundreds of websites worldwide, including those in Israel. While the primary motivation appears to be the thrill of hacking and subsequent bragging, there were instances where the defacements also included messages critical of Israel's actions in Gaza and its relationship with Denmark. These messages often incorporate text, images, and videos (Islamic Ghosts Team, n.d.)
- **The Palestinian Authority**
  - Gaza Hacker Team – Emerging in mid-2008, a hacking group primarily targeted Israeli websites, defacing dozens over a sustained period. These defacements typically included messages condemning Israel, often featuring the English statement: "We Are Not A T3RR0RISTs We are A Freedom Fighters" (Gaza Hacker Team, n.d.-c).

    The group also breached Arab websites, seemingly motivated by concerns over morality and internal Palestinian politics. Additionally, they compromised various websites, possibly to boast about their hacking capabilities.

Guidance

Online calls for attacks against Western and Israeli websites have been documented for over a decade. As early as 2005, an Arab forum post reportedly discussed a Lebanese girl who hacked Lebanese, American, and Israeli websites. The forum user who wrote the message expressed praise and gratitude for the young woman's actions (Naeimi99 2004).

Religious Guidance – However, besides words of encouragement, there are spiritual qualifications for performing these actions. In August 2008, it was announced that Egypt's Al-Azhar Institute's fatwa committee issued a fatwa allow-

ing the hacking of American and Israeli websites that harm Islam and Muslims as part of "electronic jihad" (The Middle East Media Research Institute (MEMRI) 2008). In addition, in January 2009, several Moroccan halachic scholars spoke out and stated that these actions of the Moroccan hackers are included in what is known as "electronic jihad". According to them, these are acceptable actions as part of the duty of every Muslim to do everything in his power to face the aggression in front of them. Therefore, according to them, war through the Internet is one of the 12 types of Jihads "by Allah's will."

During Israel's Operation Cast Lead in January 2009, the Az ad-Din Al-Qassam Brigades, Hamas' military wing, issued a warning on their forum. The message targeted websites masquerading as Islamic content providers. The author, according to the forum post, accused these websites of harbouring anti-Islamic material disseminated by Jews and Christians. The message urged users to cease patronising these deceptive websites and to further disseminate the call to action (Albikri 2009b).

Technical guidance – A network of Arabic-language websites and individual messages readily provided instructions, technical assistance, and even tools for conducting cyber-attacks. The Arabic Mirror website (Arabic-m.com) offered a platform for accessing hacking methods and resources, including a ranking system for prominent attackers. Similarly, the "Muslim Hacker Group" website (mslamh.jeeran.com) facilitated participation in online attacks. Users gained access to real-time information and dedicated pages for launching attacks by joining their mailing lists. Notably, targets were explicitly detailed. Websites deemed offensive to Islam, particularly those promoting "moral corruption," homosexuality, and pornography, were prioritised. This included Danish Jewish websites, especially those with political affiliations, and any website critical of Islamic content. Another platform, al-jinan.org, once offered detailed information, attack manuals, and simple cyber-attack software. However, this website is no longer operational (R. (SyS64738) Preatoni 2006a).

The online environment provided a wealth of technical resources to facilitate cyber-attacks. Detailed instructions and manuals were readily available. Notably, a prominent figure known as Br0keN-Pr0xy compiled a comprehensive 33-page guide in Arabic. This step-by-step manual offered instructions on hacking wireless networks (api-3801794 2008).

During the final days of Israel's Operation Cast Lead in January 2009, the web forum of Hamas' military wing, the Az ad-Din Al-Qassam Brigades, published detailed technical instructions. These instructions specifically guided users on how to carry out cyber-attacks against Israeli websites (Albikri 2009a; 2009c).

Beyond dedicated websites and forums, the online environment offered more resources for aspiring attackers. Numerous books and publications provided varying levels of technical instruction on website hacking (Scambray, Shema, and Sima 2006; Beaver 2006). Additionally, many defaced websites (websites altered by hackers) served as advertisements, referencing the hackers' websites. These referenced sites exhibited inconsistent activity levels, with some remaining operational and others defunct (e.g., dz-boys.com, attackerz.com, turkhackteam.org, imhatimi.org, turkdevils.org, kanunordusu.com, spysecurity.org).

This proliferation of resources extended beyond mere technical knowledge. Notably, in November 2006, an Islamic website launched the first issue of "Technical Mujahid Magazine" (Al-Mujahid Al-Taqni), demonstrating the integration of technical hacking skills with ideological motivations. The journal dealt with various technical topics with the aim of "preventing acts of online aggression against Muslims and assisting the Mujahideen in their efforts". In the introduction, it is explained that "the Internet provides a golden opportunity... for the mujahideen to break the siege placed upon them by the media of the Crusaders and their followers in the Muslim countries, and to use [the Internet] for [the sake of] jihad and the victory of the faith" (The Middle East Media Research Institute (MEMRI) 2006).

The second issue of "Technical Mujahid Magazine" (Al-Mujahid Al-Taqni), published in March 2007, further underscored the convergence of technical skills and ideological messaging. The issue featured articles on a variety of topics, including:

- Information encryption using images
- Techniques for establishing a jihadi website
- Information on types of surface-to-air missiles (a potentially concerning inclusion)
- A video question-and-answer segment
- Subtitles for jihad films (potentially for wider dissemination)
- A review of "Asrar Al-Mujahidin" encryption software (Bakier 2007).

Extremist Islamic organisations actively exploited the internet to transmit messages securely. In this context, a group known as the Global Islamic Media Front released a new version of their encryption tool, "Asrar Al-Mujahidin," in early 2008. This software supported encrypted communication across chat platforms, forums, and instant messaging (IM) applications. The updated version boasted improved capabilities, including a more robust 256-bit encryption standard. While various programs like PGP exist for general Internet communication encryption, "Asrar Al-Mujahidin" held a unique distinction: its development by and for militant Islamic groups (Tung 2008).

Conclusions

- The Rise of Online Warfare in the Middle East – Mirroring a global trend, the Internet emerged as an additional battleground in the Middle East. Online warfare became prominent in various conflicts involving diverse actors and objectives.
- Website Defacement: A Propaganda Weapon – In this context, Website defacement emerged as the primary tool for online warfare. Hackers exploited this technique for its effectiveness as a propaganda tool. Defacement allowed them to alter website content and deliver messages directly to the target audience without completely shutting down the site. This approach starkly con-

trasted with Distributed Denial-of-Service (DDoS) attacks, which aimed to overwhelm a website with traffic, rendering it inaccessible and causing significant disruption for the website owner and its users.

- Motivations for Online Warfare in the Middle East – Unlike online attacks observed elsewhere, financial motivations such as information or identity theft were relatively absent in the Middle East. Additionally, the use of online warfare as a tool by terrorist organisations or governments against each other was not a prominent feature. Instead, online attacks primarily stemmed from ideological, political, religious, and technical motivations. The content of defaced websites overwhelmingly reflected the Israeli-Palestinian conflict. Spiritual messages unrelated to this conflict, such as missionary activity, were rarely encountered.
- The Actors: Hacktivists Take Centre Stage – Unlike some regions where governments dominated online warfare, the Middle East primarily witnessed activity by individual hackers and groups, often called hacktivists. While a few instances of state-sponsored attacks emerged in North Africa and Iran, these targeted domestic opposition parties and news websites, not neighbouring countries. However, these incidents did highlight the potential for governments in the Middle East to escalate conflicts by deploying online attacks against enemy states.
- Hotbeds of Hacktivism: Freedom and Expression – Analysis of online attacks revealed a concentration of activity in countries with greater Internet freedom and freedom of speech than other regional actors. Turkey, Morocco, and Algeria emerged as prominent hubs for these hacktivist groups and individuals.
- Targets: Beyond Borders - Hacktivist activity in the Middle East extended beyond their region. They targeted specific countries, primarily Israel and Denmark, likely due to perceived political and religious grievances. Additionally, they defaced a more comprehensive range of websites globally, using them as platforms to disseminate their messages.
- Targets of Opportunity: Focus on Mass Defacement – Unlike targeted attacks on specific websites, hacktivists in the Middle East often focused on mass defacement campaigns. They exploited readily available vulnerabilities in servers

to deface many websites simultaneously. The targets themselves varied in importance and security complexity. State-owned websites and those deemed critical infrastructure presented a more significant challenge due to their heightened security measures and the potential consequences of a successful attack.

- Evolution of Defacement Techniques: Beyond Text – The content of defaced websites in the Middle East underwent a significant transformation over time. Early attacks typically involved inserting short text messages. This approach has evolved, with contemporary defacements frequently incorporating extensive text, images, audio, video files, and elaborate graphic elements.

Like the region's broader Internet adoption, online attacks in the Middle East appeared to be in a developmental stage during the period under review. This phenomenon's full potential and dangers were likely not fully realised or identified. The perpetrators were diverse, often driven by a desire to voice dissent or gain personal recognition for their technical skills. Notably, the involvement of governments, criminal organisations, and terrorist groups was relatively limited in this timeframe.

PART C – RESTRICTION: THE MEASURES

Chapter 6 – Methods of Internet Restrictions

The intersection of the Internet and freedom of expression in the Middle East raises several critical questions:

- **Privacy and Freedom:** Do Arab users enjoy online privacy and freedom of expression in a comparable way to other regions?
- **Circumventing Restrictions:** Does the Internet offer these users greater freedom than traditional media outlets, often subject to government control?
- **Legal Ambiguity:** Under which legal frameworks are Internet-related offences prosecuted in the Middle East?(The Arabic Network for Human Rights Information, n.d.-c)

The inherent structure and characteristics of the Internet create opportunities for governments to employ various monitoring, blocking, and filtering techniques. Centralised control allows for a multi-layered approach, categorised into two main strategies: **preventing** and **controlling existing access**. At the highest level, the state can prevent access to the Internet through **technological**, **regulatory**, and **economic** means:

Technology

There are four levels of government censorship to blocking the Internet and filtering its content (Parry et al. 2003):

1. **Independent Filtering:** ISPs offered users optional filtering services; government involvement in this model was minimal.
2. **Government-Guided Filtering:** Governments actively defined inappropriate content and encouraged ISPs to offer filtering services. However, ISP participation remained voluntary.

3. **Mandatory Filtering:** Governments mandated ISPs to provide filtering software to users, blocking access to unwanted content. Legislation defined the scope of restricted content, while ISPs and users were obligated to comply.
4. **National Filtering:** Governments implemented filtering programs directly at the Internet backbone level, bypassing ISPs and user control. The government defined and updated the list of restricted content, with no option for users or ISPs to opt-out.

Alexander Gruhler's research explored various approaches to regulating Internet access and identified five levels of restriction (Kirchner 2001):

1. **Voluntary Measures:** This level emphasises self-regulation and user control over Internet content.
2. **Legal Enforcement:** This approach involves law enforcement and judicial bodies intervening to address illegal online activity.
3. **Website Indexing:** This level focuses on cataloguing specific websites for potential monitoring or restriction.
4. **Content Filtering:** Filtering systems selectively block access to predefined categories of online content.
5. **Internet Access Restriction:** This most restrictive level involves limiting or even entirely severing Internet access within a specific region or for certain user groups.

In his research, Gruhler identified restriction levels 3-5 (website indexing, content filtering, Internet access limitations) as prevalent in Arab countries. However, the current analysis highlights a limitation in Gruhler's model: its exclusive focus on administrative restrictions and their consequences. This framework overlooks the potential impact of economic factors, such as poverty, infrastructure deficiencies, and high Internet connectivity costs, which can significantly restrict user access in the region.

While seeking to control online content, authoritarian regimes in the Middle East also recognised the Internet's potential as a tool to serve their agendas. They adopted a "proactive" approach, utilising the Internet for several purposes:

- **Propaganda Dissemination:** Regimes exploited the Internet to disseminate propaganda and promote their narratives to domestic and international audiences.
- **Closed Networks:** Some governments developed state-controlled intranets, offering a curated online experience as a substitute for the broader Internet.
- **E-Government Services:** Regimes implemented e-government services to enhance efficiency and improve citizen satisfaction with government performance.
- **Information Warfare:** Certain governments engaged in international information warfare, targeting websites critical of their regimes and potentially deploying malicious software.

Authoritarian regimes in the Middle East navigate the Internet through reactive and proactive policies. Reactive policies address immediate challenges and threats posed by Internet use. In contrast, proactive policies aim to cultivate an Internet environment that aligns with the state's interests. This two-pronged approach allows these regimes to manage the potential dangers of the Internet while simultaneously leveraging it to bolster their authority and promote national development (Kalathil and Boas 2001).

Methods of Internet Restrictions

Authoritarian regimes in the Middle East employ various techniques to restrict access to online information. These methods fall under two main categories: filtering and blocking.

- **Filtering** involves selectively blocking specific types of content across various websites. This allows the government to control the flow of information without entirely shutting down websites. Examples of filtered content might include gambling sites, political dissident websites, or religiously offensive content (Greenfield 2001; "Documenting Internet Content Filtering Worldwide" 2004).
- **Blocking** takes a more drastic approach, restricting access to entire websites or Internet services. This can be achieved by manipulating server configurations or implementing more comprehensive measures limiting Internet access

within a specific region or for certain user groups. In extreme cases, governments may restrict access entirely, allowing only a predefined list of approved websites ("Fact Sheet on Internet Filters" 2003).

The vast and readily available information on the Internet, surpassing any other media source, has prompted efforts by various actors to restrict online access and content. These restrictions aim to prevent diverse populations, particularly vulnerable groups like children, from accessing potentially harmful content such as violence, pornography, or gambling websites.

However, the scope of restrictions can extend beyond protecting specific audiences. In some countries, governments have implemented measures to restrict access to culturally or religiously inappropriate content, even if such content is freely available elsewhere. These restrictions may encompass various topics, including religious materials, health information, social commentary, and political activism, potentially limiting access to music, cultural expression, and other forms of creative content.

In response to concerns about children's exposure to inappropriate content online, the US Congress passed the Communications Decency Act (CDA) in 1996. This law aimed to prohibit the presentation of such materials to minors. However, the CDA faced immediate legal challenges. Critics argued that it violated the First Amendment's guarantee of free speech. Some proposed parental filtering software as an alternative to government censorship, suggesting it could empower parents to restrict access to specific websites without state intervention. Opponents of this approach countered that while parental controls could mitigate the need for government censorship, they effectively transferred the power of censorship to private companies.

Initial Internet filters relied on content ratings assigned by publishers or third parties, categorising websites based on suitability for different audiences. However, the Internet's rapid growth and dynamic nature rendered this method increasingly ineffective. Filter companies struggled to keep pace with the sheer volume

of websites and their constantly evolving content. This led to the development of "mechanical blocking" techniques using pre-determined keywords or phrases to identify and block target websites. This automated approach resulted in over-blocking (inadvertently blocking legitimate content) and under-blocking (failing to block inappropriate content). Filter companies countered these criticisms, claiming extensive manual review processes to refine their filtering criteria. Critics remained sceptical, arguing that such practices were resource-intensive and beyond the capacity of these companies.

Beyond concerns about overreach, many opposed censorships based on political or ideological content. Free speech advocates strongly objected to Internet service providers or legislation imposing mandatory filtering without allowing users to turn off the filter. These arguments were sometimes bolstered by personal accounts of activists challenging government censorship efforts (Wallace 1998).

Authoritarian regimes in the Middle East utilise various software and hardware solutions to filter and block access to specific websites. These solutions can be categorised into four primary approaches:

- **Client-Based Filtering Software:** This software is installed directly on user devices, allowing individuals or organisations to control access to specific content.
- **Server-Based Web Filtering Software:** This approach deploys filtering software on Internet servers, enabling administrators to manage content access for a broader user base.
- **Turnkey Filtering Servers:** Combining hardware and software, turnkey filtering servers offer a pre-configured content filtering and blocking solution.
- **Dedicated Filtering Appliances:** These standalone hardware devices perform filtering and blocking functions independently of additional software installations ("Web Filtering Appliances Heat Up the Hardware vs. Software Debate" 2005; "Internet Filtering Alternatives," n.d.)

Types:

- **Inclusion Filtering (Whitelist):** This method only grants access to a pre-approved website list (whitelist). While offering a high degree of control, it is rarely used due to the significant effort required to compile and maintain an exhaustive whitelist. In contrast, most website blocking techniques employ a blacklist approach, restricting access to specific websites deemed undesirable.
- **Exclusion Filtering (Blacklist):** This more common approach blocks access to a predefined list of websites (blacklist). While offering greater flexibility (specific pages, websites, or IP addresses can be targeted), blacklists are prone to errors:
  - **Under-blocking:** Filtering technology based on content analysis may fail to capture all targeted content, sometimes allowing unintended access.
  - **Over-blocking:** Due to the nature of these lists (often a combination of manual and automated creation), filters may unintentionally block legitimate content. This can empower blocking parties (private companies or authorities) to control access and limit transparency, especially when collaborating with undemocratic regimes. For instance, content containing the word "breast" (even in a medical context, like "breast cancer") or words like "Sussex" and "Essex" might be inadvertently blocked.

An examination of websites censored by filtering software revealed a critical flaw: these programs **over-block** legitimate content they should not restrict (e.g., medical websites containing "breast cancer") and **under-block** websites they intend to restrict (e.g., bypassing filters with minimal effort). This highlights the limitations of blacklist-based filtering and the potential for unintended consequences (Heins and Cho 2001; Akdeniz 1998; Edelman 2003; Sims 1998).

The limitations of blacklist filtering are evident in its tendency to **over-block** legitimate content. For instance, these programs may block websites related to the LGBTQ+ community, even those containing purely informational content unrelated to sexuality (C. S. Kaplan 1997; "Access Denied Version 2.0: The

Continuing Threat Against Internet Access and Privacy and Its Impact on the Lesbian, Gay, Bisexual and Transgender Community" 1999). A 2005 experiment in Tunisia further demonstrates this phenomenon, where filtering software employing blacklists inadvertently blocked non-sexual websites associated with the LGBTQ+ community (Human Rights Watch 2005a).

The challenge for governments in the Middle East lies in crafting effective website-blocking policies. This involves choosing between two primary approaches:

- **Limited Filtering:** This strategy prioritises minimising false positives (over-blocking) by restricting blocks to a carefully curated list of websites deemed genuinely objectionable. However, this approach may leave some undesirable content accessible.
- **Comprehensive Filtering:** This method blocks a broad range of potentially harmful content. However, it carries a significant risk of over-blocking legitimate websites, inadvertently restricting access to information and potentially infringing on free speech principles.

The issue of website blocking in the Middle East can be illustrated by examining contrasting policies within the Persian Gulf region. Bahrain exemplifies a limited filtering approach. ISPs in Bahrain restricted access only to a specific list of predefined websites deemed objectionable by the government.

The UAE implements a contrasting strategy. The UAE employs broader content filtering mechanisms to block a more comprehensive range of potentially problematic content. However, this approach risks inadvertently blocking legitimate websites based on content analysis. This can have a chilling effect on free speech and restrict access to information (Palfrey 2005).

Methods: Countries wishing to block access to certain websites can do so in several ways:

DNS Filtering – DNS filtering, a method where ISPs configure their servers to prevent requests to specific websites, presents several limitations:

- **Ease of Circumvention:** Users can bypass DNS filtering by entering a website's IP address directly or utilising alternative DNS servers (l0gic 2005).
- **Over-blocking:** Blocking an entire domain through DNS filtering also restricts access to all its subdomains, even if they contain legitimate content. This "over-blocking" can significantly hinder user experience (Zittrain and Palfrey, n.d.).
- **Logistical Challenges:** AOL's experience in Pennsylvania exemplifies the logistical hurdles associated with DNS filtering. Implementing the filter across its vast network of DNS servers proved impractical ("Why Block by IP Address?" 2005).

IP Filtering – is a standard method for website blocking employed by governments, particularly those new to Internet content control. This method involves identifying the IP address associated with a specific URL (Uniform Resource Locator) and configuring routing equipment to block all traffic directed to that address.

While appealing for its simplicity and speed of implementation, IP filtering suffers from several limitations:

- **Limited Effectiveness:** Websites can easily change IP addresses, rendering the block obsolete.
- **Collateral Damage:** Blocking an entire IP address can inadvertently restrict access to other legitimate websites hosted on the same server.
- **High Maintenance:** Monitoring and updating blocked IP addresses can be resource-intensive.

Although a cost-effective initial approach, IP filtering's limitations necessitate exploring alternative methods for robust content control strategies.

Even countries with sophisticated Internet infrastructure, such as South Korea and China, often prioritise IP-based website blocking over more targeted URL or content filtering methods. This approach prioritises blocking entire websites associated with a specific IP address, even if it results in the unintended conse-

quence of over-blocking legitimate content hosted on the same server. While this strategy aligns with the content control objectives of these governments, it sacrifices user access to potentially valuable information.

URL Filtering – offers a more precise approach to website blocking than IP filtering. This method involves examining the requested URL (website address) against a blacklist and blocking access if a match is found. However, URL filtering presents significant challenges:

- **Technical Infrastructure:** Implementing URL filtering necessitates additional equipment or complex router reconfigurations for ISPs. The sheer volume of hardware required can be cost-prohibitive, potentially leading to performance degradation.
- **Scalability:** The effectiveness of URL filtering diminishes as the number of users and targeted websites increases. Maintaining an accurate and up-to-date blacklist becomes a significant technical hurdle.
- **Government Control:** Effective URL filtering relies on ISP cooperation or government control over these entities. This approach can raise concerns about censorship and Internet access limitations (Palfrey 2005).

A study cited the inefficiency of IP blocking, highlighting a case where over 3,000 websites were blocked to restrict access to only 31. However, as exemplified by Saudi Arabia's delayed public Internet access due to filter implementation challenges, URL filtering presents its complexities.

Content Filtering – extends beyond website blocking by analysing the nature of information on web pages. This approach employs various techniques.

- **File-Type Filtering:** This method scans requested pages for pre-defined file types, such as audio or video, to restrict access based on file format rather than content.
- **Keyword Filtering:** Content analysis can involve searching for specific keywords within a webpage. While basic, this technique offers some level of control compared to blocking entire websites.

- **Advanced Content Analysis:** More sophisticated content filtering goes beyond simple keyword matching. These techniques attempt to analyse a webpage's content's overall meaning and context.
- **Link Analysis:** This method examines the links on a requested page, assuming thematic relevance to the content it hosts. This allows for potential filtering based on the broader website ecosystem.
- **Image Analysis:** Technological advancements enable the analysis of images' content, potentially restricting access based on visual elements.
- **Profile-Based Filtering:** This technique analyses web pages based on pre-defined characteristics associated with specific page types. This allows for targeted filtering within categories like social media or news websites.

Content filtering offers greater precision than website blocking, but it also presents challenges:

- **Accuracy:** The effectiveness of content filtering hinges on the accuracy and sophistication of the analysis techniques. False positives (inadvertently blocking legitimate content) and false negatives (missing intended targets) remain a concern.
- **Complexity:** Implementing advanced content filtering requires significant technical resources and expertise.
- **Subjectivity:** Defining appropriate filtering criteria can be subjective and raise concerns about censorship.

Overall, content filtering offers a nuanced approach to content control but requires careful implementation to balance user access with filtering objectives.

Content filtering products offer governments a range of tools to monitor and control Internet activity:

- **User Identification:** These systems can identify users by associating their IP addresses with usernames or personal data.
- **Traffic Monitoring:** Governments can leverage content filtering products to monitor Internet traffic through ISPs. This may involve intercepting communi-

cations (phone calls, emails, web traffic) to track user activity, including websites visited, pages accessed, and files downloaded.

- **Content Blocking:** The core function of content filtering products is to restrict access to specific websites, groups of websites, or online activity deemed undesirable by the government.
- **Data Collection and Analysis:** These systems can collect and store data on user activity, including websites visited, browsing history, and time spent on specific sites. This data can generate reports and inform further content control measures.
- **User Tracking and Regulation:** By monitoring and analysing online activity, governments can potentially identify and target users for arrest, legal action, or other restrictions on their Internet use. Additionally, pressure may be exerted on ISPs and Internet cafes to enforce government-mandated monitoring practices.

Acknowledging the potential downsides of such comprehensive monitoring and control is essential. These practices raise concerns about user privacy and freedom of expression. The ability to anonymously access and share information online is fundamental to a free and open Internet. Content filtering products can threaten these core principles when deployed without proper oversight and safeguards.

Website blocking efforts are often met with countervailing measures. Users may attempt to circumvent restrictions through various methods:

- **Anonymized Services:** These services allow users to mask their IP addresses, potentially bypassing filters based on geographical location.
- **Proxy Servers:** Proxy servers act as intermediaries between users and websites, potentially enabling access to blocked content.
- **Virtual Private Networks (VPNs):** VPNs encrypt internet traffic and route it through a remote server, offering another method for bypassing content restrictions.

The effectiveness of website blocking strategies is often debated. While such measures can achieve some level of control, the availability of circumvention tools highlights the ongoing struggle between content control and user access to information.

Location: Website blocking and content filtering can be implemented at various levels:

- **End-User (Local):** Software installed on individual devices (home computers, work computers, or public terminals in Internet cafes) can restrict access to specific content. Users may have some control over blocking parameters, such as blacklists and whitelists, depending on the software configuration. This approach is often used to limit access to pornography or other sensitive content. Some countries mandate the installation of such filtering software in Internet cafes.
    - **Organizational (Corporate):** Organizations (workplaces, schools, or Internet service providers) can deploy content filtering and blocking mechanisms within their networks. This typically involves utilising routers, firewalls, or proxy servers. Proxy servers act as intermediaries between users and websites, allowing easier control and filtering of user requests. Routers and firewalls can be configured to block access to specific websites or IP addresses, further restricting potential workarounds (Radding 2004).
    - **National:** Governments can implement content filtering and website blocking nationally. This approach often involves packet filtering, which inspects data packets for source and destination IP addresses. By controlling the flow of data based on IP addresses, governments can block specific websites or even monitor network traffic for pre-defined keywords. This national-level filtering raises significant concerns about user privacy and freedom of expression.

Regulations

Governments employ various methods to regulate and control online content, with website blocking and filtering being prominent strategies. Here are two fundamental mechanisms**:**

- **State Control of ISPs:** In many countries with widespread Internet use, governments leverage their influence or direct control over ISPs and telecommunication companies to implement content control measures. This control can persist even after privatisation, as government regulations and laws can mandate specific actions from ISPs regarding Internet access. This approach is efficient in regions where governments control traditional media, as existing infrastructure and regulatory power can readily apply to ISPs. Furthermore, even in partial privatisation, state oversight of international network access points often remains (Human Rights Watch 1999d; C. S. Kaplan 1997).
- **Regulatory Blockage:** Governments can restrict Internet access through legislative and licensing measures. This may involve limitations on obtaining the necessary equipment or infrastructure to connect to the Internet or enacting laws restricting online activity.

Government control over online content raises complex questions regarding the balance between national security, public morality, and freedom of expression. While governments have a legitimate interest in regulating harmful or illegal content, overly broad restrictions can hinder access to information and innovation.

The MENA region has a long history of government attempts to control media content. This is evident in the early efforts to regulate new communication technologies. For instance, the government imposed strict restrictions upon introducing fax machines (facsimile devices) in Syria. Owning a fax machine or even registering a personal computer required approval from military and security authorities. Syrian citizens initially could not possess fax machines at all. This policy shifted only when the government acquired technology to intercept fax communications without disrupting transmissions. Furthermore, authorities could disconnect the

phone lines of individuals found using fax machines without authorisation (The Arabic Network for Human Rights Information, n.d.-e).

Many governments worldwide use legal and regulatory frameworks to control Internet access and content. These regulations often encompass various areas of law, including media, communication, national security, and Internet use. The aim is to restrict citizens' ability to access or publish certain online content.

A particularly stringent approach involves licensing ISPs. Governments can exert significant influence over the online environment by controlling who can offer Internet access. This approach is exemplified by several countries, including Burma, Cuba, and North Korea, where the government severely restricts Internet access. In extreme cases, like Burma, citizens face legal repercussions (up to 15 years in prison) for owning a computer without government registration (C. S. Kaplan 1997).

Arrests and Harassment – In some countries, governments may use intimidation tactics to discourage citizens from freely using the Internet. This can include arresting or harassing Internet users to create a climate of fear and self-censorship. While such methods may seem more practical than legal restrictions on online activity, they raise significant concerns (Human Rights Watch 1999d).

- **Chilling Effect:** The threat of arrest or harassment can have a chilling effect on free expression. Users may be more cautious about expressing themselves online, fearing government reprisal. This self-censorship can stifle online discourse and limit the free flow of information.
- **Human Rights Concerns:** Government practices of intimidation and harassment violate fundamental human rights, including freedom of expression and privacy. These tactics can create fear and distrust, hindering open communication and civic engagement.

Acknowledging that governments have legitimate interests in regulating certain online content is essential. However, alternative approaches, such as robust legal

frameworks and content filtering mechanisms, can be more effective in achieving these goals without resorting to intimidation tactics.

Economic

Several economic factors limit widespread Internet access in MENA countries (Kirchner 2001).

- **High Equipment Costs:** The hardware required for Internet access, often imported, can be expensive due to import duties or classification as luxury goods. This puts ownership of computers and mobile devices out of reach for many citizens.
- **Software Costs and Legality:** Essential software for Internet use can also be costly and not readily available through legal channels. This discourages users who cannot afford licensed software and creates ethical dilemmas for those considering piracy.
- **Expensive Internet Connections:** The cost of Internet access, including subscriptions and fees, can significantly burden many people in MENA countries. This applies even to public Internet cafes, often considered more affordable. These high costs limit the affordability of Internet access for a large segment of the population.
- **Socioeconomic Disparity:** The pricing structures employed by ISPs and media organisations can exacerbate existing socioeconomic inequalities. Tiered pricing plans and limited access for lower-income groups can create a digital divide where certain socioeconomic strata have preferential access to the Internet. This approach has been described as an “acceptable model” for limiting overall Internet access within a population.

Addressing these economic barriers is crucial for expanding Internet access in MENA countries. Affordable equipment, software, and Internet connection fees are essential for bridging the digital divide and ensuring equitable access to information and communication technologies.

Religious

Religious institutions and authorities can play a role in limiting Internet access in some societies. This approach can take several forms:

- **Clerical Pronouncements:** One of the ways that the government in a traditional society can limit access to the Internet is through religious restrictions. Whether through religious orders or calls and warnings from clerics. Some religious communities view pornography with concern due to its potential spiritual consequences. An illustrative example is a website called "Hunting al-Fua'd" (Arabic for "Hunting the Heart"), which discourages pornography use by warning viewers that such actions will be recorded as harmful deeds in the afterlife and could lead to shame if death occurs while accessing the content. According to a user testimonial, encountering such warnings on "Hunting al-Fua'd" motivated them to stop visiting pornography websites (Sayd Alfawayid, n.d.).
- **Religious Teachings on Online Conduct:** Religious authorities may offer guidance on appropriate online behaviour regarding topics like sexuality and gender relations. This guidance can range from rulings against pornography to extreme measures like advocating for complete Internet disconnection to strengthen one's faith and resist temptation.
- **Gender-Based Restrictions:** Religious interpretations can also influence access based on gender. The example provided mentions a potential ban on women using the Internet without a chaperone who could "monitor their activities." This approach reflects specific cultural norms and gender roles within a particular religious framework.

A study of various religious websites revealed a range of user queries concerning Internet use and religious obligations:

- **Pornography:** Users sought guidance on navigating pornography websites, particularly for young people (Islam Online 2003b).

- **Internet Cafes:** The appropriateness of operating Internet cafes was questioned, with concerns raised about their potential for "negative purposes" exceeding positive uses (Islam Online 2005b).
- **ISPs and Content Filtering:** Users debated the responsibility of ISPs regarding content filtering. One viewpoint argued against censorship, placing the onus on users to avoid "immoral websites."
- **Gender Representation in Media:** The permissibility of publishing magazines that portray women negatively was another topic of inquiry.
- **Marital Issues and Online Behaviour:** Users sought guidance on navigating online behaviour within marriage, specifically regarding online chat and pornography use by spouses.
- **Overall Attitudes Towards the Internet:** The broader question of the Internet's influence was raised, prompting users to consider whether it represents freedom or a form of restriction (Islam Online 2004)

A review of online resources revealed several queries regarding online communication and relationships between men and women:

- **Online Chat:** The permissibility of online chat between genders was a topic of discussion (Islam Online 2005a).
- **Muslim Guidelines for Chat Rooms:** Specific guidance was sought for Muslims navigating online chat rooms. Tips for Muslims when communicating in chat rooms (Islam Online 2003a).
- **Online Dating and Marriage:** Women could register on dating websites and specify desired qualities in a spouse (Islam Online 2008).
- **Restrictions on Online Matchmaking:** Users inquired about potential limitations associated with online searches for spouses
- **Online Communication within Marriage:** The permissibility of using webcams for intimate conversations between spouses was explored, mainly when they are geographically separated.

Two key questions emerged regarding children's education and Internet safety:

- **Balancing Children's Awareness and Protection:** Users grappled with staying informed about online content while shielding their parents from potentially harmful material. The question highlighted the difficulty of balancing children's knowledge and Internet safety for younger generations.
- **Protecting Children from Online Risks:** Another concern focused on safeguarding children from exploitation on the Internet, particularly in the context of the proliferation of pornographic websites. This question underscores the broader issue of online safety for children and the need for parental vigilance in specific online spaces.

In September 2004, Saudi Arabia's Grand Mufti issued a religious edict against exchanging messages on cell phones between young men and women. This prohibition was reportedly motivated by concerns about potential immorality and social problems arising from such communication. The Mufti reportedly cited an incident where girls were photographed without their consent, leading to what he termed "grave moral harm" to their modesty and dignity. He urged young women to avoid this "abyss". He called for a complete ban on such communication, arguing that it was the most effective way to prevent "moral humiliation," which he perceived as the goal of many young men ("International Islamic News Agency (IINA) Bulletin" 2004).

The widespread adoption of the Internet in the Middle East presents significant challenges to established social and political structures. These concerns can be broadly categorised as follows:

- **Moral and Cultural Impact:** Some in the region are anxious about the potential for online content to undermine traditional morality, cultural values, and religious beliefs. This concern stems from the perception that the Internet can expose users to ideas and behaviours contradicting established norms.

- **Political Change and Legitimacy:** Some see the Internet's ability to facilitate communication and information sharing as a threat to the existing political order. Governments may fear the Internet could empower dissident voices and challenge their legitimacy.
- **Social Fabric and Change:** Another concern is the Internet's potential to disrupt traditional social structures and norms. Some worry that increased online interaction could weaken established social bonds and community values.

Due to the historically conservative social norms in many Middle Eastern countries, issues related to sexuality are susceptible. This translates into a heightened focus on regulating online content, particularly pornography and websites depicting sexual activity. Governments often implement website blocking measures in response to concerns about the potential corrupting influence of such content on public morality.

It is essential to acknowledge alternative perspectives on these concerns. Some argue that government restrictions on online content amplify its appeal by creating a "forbidden fruit" dynamic. They say that open access to information and diverse viewpoints could be crucial for promoting social progress and responsible online behaviour.

Press, Personal and Internet Freedom in the MENA –

Researchers have developed various indices to assess press freedom, media freedom, and overall levels of freedom in MENA countries. These indices quantify and compare Internet connectivity and government restrictions on Internet access across different nations. Some of these indices face limitations due to their reliance on a limited set of parameters. These parameters may focus on specific aspects of Internet freedom rather than providing a more comprehensive picture. For instance:

Freedom House –

Methodology:

The annual "Freedom of the World" index by Freedom House categorises countries and territories as "Free," "Partly Free," or "Not Free" in terms of overall freedom. While relevant, this broad categorisation may not capture each country's nuanced variations in Internet freedom. Additionally, the cited appendices (A1 and A2) focus on a specific timeframe (2000-2009) and may not reflect the current state of Internet freedom in the MENA region.

Conclusions:

1. **Limited Freedom:** An analysis of Internet freedom in 21 Middle Eastern countries revealed that none achieved the "Free" designation between 2000 and 2009. Instead, all countries fell into the categories of "Not Free" (68 per cent average) or "Partly Free" (27 per cent average).
2. **Israel as an Outlier:** Israel was the sole exception within the region, consistently classified as "Free" throughout the period.
3. **Limited Movement:** Overall, changes in Internet freedom rankings were relatively minor. Three countries experienced fluctuations between "Not Free" and "Partly Free" statuses.
4. **Stagnation and Decline:** A significant majority (62 per cent) of countries remained classified as "Not Free" for ten years. Similarly, 19 per cent remained "Partly Free" throughout.
5. **Lebanon's Improvement:** Lebanon is the only country with consistent progress. Its ranking improved from "Not Free" (2000-2004) to "Partly Free" (2005-2009).
6. **Regression in Bahrain and Yemen:** Both Bahrain and Yemen initially showed improvement by transitioning from "Not Free" to "Partly Free" in 2002 and 2004, respectively. However, both countries regressed to "Not Free" by 2009.

Reporters Without Borders: World Press Freedom Index – Data on press freedom in 21 MENA countries was collected from the annual "World Press Freedom" index published by Reporters Without Borders, which began in 2002.

Methodology:

1. **Data Collection:** Data points for the 21 MENA countries were extracted from the annual Reporters Without Borders reports and compiled in Appendix B1.
2. **Data Presentation:** To facilitate analysis, trends and changes in press freedom for these countries have been visualised in three separate charts within the appendices:
   a. **Appendix B2**: This chart presents data for Algeria, Bahrain, Egypt, Iran, Iraq, Israel, and the Israeli-Occupied Territories.
   b. **Appendix B3**: This chart focuses on Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, and Qatar.
   c. **Appendix B4**: This chart displays data for Saudi Arabia, Sudan, Syria, Tunisia, Turkey, the UAE, and Yemen.

Conclusions:

The "World Press Freedom" index by Reporters Without Borders corroborates the findings of the "Freedom of the World" index regarding the limited press freedom in MENA countries. However, the Reporters Without Borders data offers a more nuanced understanding by examining specific trends within each country from 2002 to 2009.

1. **Press Freedom Decline in MENA** – The analysis reveals a negative trend across most MENA countries, with nearly all surveyed nations experiencing a decline in their press freedom ranking between 2002 and 2009.
2. **Limited Improvement** – Only a few exceptions emerged, with Kuwait, Qatar, and the UAE demonstrating some improvement in their press freedom rankings during the analysed period.

Centre for Systemic Peace (CSP) –

The Center for Systemic Peace (CSP) "Polity5 Project" provides data on the level of autocracy or democracy for countries worldwide from 1800 to 2018. The project employs a scoring system where +10 indicates a strongly democratic regime and -10 signifies a strongly autocratic one (Marshall and Gurr 2020).

Methodology:

1. **Data Collection:** Data points for the 21 MENA countries were extracted from the CSP "Polity5 Project" and compiled in Appendix C1.
2. **Data Presentation:** To facilitate analysis, trends and changes in democratic characteristics for these countries have been visualised in three separate charts within the appendices:
   a. **Appendix C2**: This chart presents data for Algeria, Bahrain, Egypt, Iran, Iraq, Israel, and the Israeli-Occupied Territories.
   b. **Appendix C3**: This chart focuses on Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, and Qatar.
   c. **Appendix C4**: This chart displays data for Saudi Arabia, Sudan, Syria, Tunisia, Turkey, the UAE, and Yemen.

Conclusions:

An analysis of data from the Center for Systemic Peace (CSP) reveals a predominance of autocratic regimes in the MENA region.

- **Autocracy Prevails:** From 2000 to 2009, 76 per cent (16 out of 21) of MENA countries were classified as autocratic and non-democratic.
- **Limited Democratic Representation:** Only four countries – Israel, Algeria, Lebanon, and Turkey – achieved a democratic designation at some point during the analysed decade. However, data availability limitations for some countries may obscure a more nuanced picture.

- **Stagnant or Worsening Regimes:** Nearly half (48 per cent) of MENA countries exhibited no improvement in their democratic character throughout the period.
- **Restricted Regimes:** A significant majority (57 per cent) of countries fell within the lowest range of the CSP scale (-6 to -10), reflecting highly restricted and autocratic forms of governance.
- **Limited Signs of Improvement:** Only Egypt and Sudan demonstrated any improvement in their democratic scores despite remaining classified as autocratic overall.

Multiple international indices were employed to assess and rank Internet freedom across countries, with data coverage typically spanning the 2000-2009 period (Lokot and Wijermars 2023):

Ranking/Index	Organisation	Start-End year
Freedom of the Net	Freedom House	From 2009
Web Index	World Wide Web Foundation	2012-2014
Corporate Accountability Index	Ranking Digital Rights	From 2015
OpenNet Initiative	Citizen Lab, University of Toronto, Berkman Klein Center for Internet & Society, Harvard University, SecDev Group	2007-2013
Keep It On Internet Shutdowns Annual Report	Access Now	From 2016
Press freedom's digital predators	Reporters Without Borders	From 2020
Press freedom predators	Reporters Without Borders	From 2016

Internet Freedom – Freedom House's "Freedom on the Net" index, launched in 2009, provides another perspective on Internet freedom in the MENA region. The initial iteration of this index assessed 15 countries worldwide, including four from the MENA region:

- **Turkey and Egypt:** These countries were classified as "Partly Free" regarding Internet freedom.

- **Iran and Tunisia:** These countries were categorised as “Not Free.”

It is important to note that, except for Egypt, these classifications mirrored the corresponding designations in Freedom House’s “Freedom of the World” index. While Egypt received a “Partly Free” designation for Internet freedom in 2009, it remained classified as “Not Free” in terms of overall freedom throughout 2000-2009.

Chapter 7 - Internet Restrictions in the MENA

The widespread adoption of the Internet presents governments worldwide with a complex challenge. On the one hand, the Internet offers undeniable benefits, including democratising information through widespread accessibility across diverse communication channels. This accessibility has fuelled a significant information revolution.

On the other hand, this same accessibility can be a concern. The Internet provides unfiltered and direct access to vast information, including content that some governments may deem undesirable for specific audiences. Examples include pornography, gambling sites, and violent content. This abundance of potentially harmful material creates complex dilemmas for governments, particularly regarding the appropriate level of Internet regulation and the need, if any, to control online behaviour.

The challenges of Internet regulation are particularly acute in centralised governments lacking individual and media freedoms. These characteristics are often coupled with a sense of diminished government legitimacy within conservative and traditional societies. The Middle East is prominently featured in this category, with many countries displaying these characteristics. Consequently, it is unsurprising that this region is well-represented among those perceived as restrictive of Internet freedom.

Several Middle Eastern countries have implemented various measures to restrict citizens' Internet access. These restrictions are motivated by a combination of political and moral concerns.

- **Legislative Controls:** Governments have enacted legislation to regulate online activity.
- **Content Monitoring and Surveillance:** Authorities monitor and supervise user conduct and online activity. In some cases, this monitoring has led to arrests.

- **Website Blocking and Censorship:** Governments have blocked access to specific websites and censored online content deemed objectionable.

The Facebook website was blocked in Syria because it allows accessible communication between Syrians and Israelis. The site has been blocked in the country for about three years. In the UAE, an application enabling acquaintance between spouses was blocked on the website. Some of the governments have gone one step further, such as some in North Africa who infiltrated opposition websites and disabled them.

Levels of Internet freedom vary significantly across Middle Eastern countries. These variations can be partially attributed to a nation's openness to communication and its progress towards democratisation.

It is important to note that these variations exist even within countries that employ tactics like arresting Internet users.

Blocking

An analysis of legislation and Internet testing in MENA countries reveals two primary categories of website blocking and filtering:

- **Political Content:** Restrictions on political content emerged as the most consistent form of filtering across the region. This finding aligns with the observation that "political filtering continues to be the common denominator across the region".
- **Social Content:** The Gulf countries, along with Sudan, Tunisia, Gaza, and Yemen, implemented stricter social filtering practices. These practices targeted content deemed socially unacceptable, including pornography, nudity, LGBTQ+ content, escort services, dating services, and websites displaying revealing clothing.

Interestingly, while most MENA countries acknowledged social filtering, they often employed obfuscation tactics for political filtering. This involved presenting users with misleading error messages, making it difficult to discern the valid reason for blocked access (OpenNet Initiative, n.d.-b).

Bahrain – Following the introduction of the Internet in 1995, Bahraini residents adopted it as a crucial platform for expression in a context where the government tightly controlled traditional media outlets. Blogs emerged as a popular forum for discussing various topics, including domestic politics, and disseminating information beyond national borders.

However, the Bahraini government exerted significant control over Internet access and content. This control manifested in blocking opposition websites and those deemed to promote sedition or contain offensive material. Government justifications for these restrictions centred on maintaining public morality and preventing online content from inciting unrest.

A specific example occurred in March 2002, when the government blocked websites associated with the Bahraini opposition and others accused of "inciting sectarian divisions and containing offensive material". The Minister of Information at the time claimed that Bahrain welcomed constructive criticism but would not tolerate content promoting sectarianism or inciting violence. He further asserted that only four websites had been blocked and that this number could fluctuate depending on the content moderation practices employed by the website administrators. One prominent casualty of these restrictions was BahrainOnline.org, a highly active website known for facilitating discussions on Bahrain's social and political landscape, publishing human rights reports, and offering a forum for users to exchange information and opinions.

Unlike other countries in the region, Bahrain's approach to Internet regulation exhibited a degree of pragmatism. The government appeared to recognise the Internet's potential role in fostering economic development and attracting investment. This awareness was reflected in their decision to refrain from implementing overly restrictive measures. In some instances, the government even directed citizens towards resources for obtaining filtering software, suggesting a preference for self-regulation when possible.

nlike other countries in the region, Bahrain's approach to Internet regulation exhibited a degree of pragmatism. The government appeared to recognise the Internet's potential role in fostering economic development and attracting investment. This awareness was reflected in their decision to refrain from implementing overly restrictive measures. In some instances, the government even directed citizens towards resources for obtaining filtering software, suggesting a preference for self-regulation when possible. The issue of pornography in schools exemplifies the government's approach to content filtering. A school official, concerned about students accessing inappropriate websites in the computer lab, criticised the Ministry of Education for inadequate supervision. This criticism implied support for filtering software restricting student access to certain online content. Furthermore, the official advocated granting Internet access only through government-controlled connections, presumably allowing online activity monitoring (Bahrain Tribune 2005e).

A 2004-2005 OpenNet Initiative (ONI) test revealed that Bahrain blocked a relatively small percentage of websites – only 8 out of 6,000 tested. Of these blocked sites, three contained pornographies, while the remainder addressed religious and political topics deemed sensitive by the Bahraini government (OpenNet Initiative 2005a).

It is noteworthy that compared to similar ONI testing conducted in other Arab countries, Bahrain did not exhibit website blocking in several categories, including content related to:

- The LGBTQ+ community
- Regional news sources
- The Baha'i Faith
- Strong criticism of Islam, Israel, opposition groups, or leaders
- Human rights

While Bahrain's technical capabilities allow for stricter Internet controls, recent years have witnessed a trend towards a more symbolic level of website blocking.

These restrictions appear to be less about hindering citizens' Internet access and more about sending a message.

This observation is supported by the limited content filtering observed in the country and the lack of widespread restrictions on Internet access for citizens. Furthermore, government officials' tendency to deflect responsibility for Internet monitoring and blocking suggests a reluctance to adopt a more aggressive approach in these areas (OpenNet Initiative 2005a).

Egypt – Like Syria, Egypt faced challenges in maintaining government legitimacy. However, unlike Syria, where religious factors played a significant role, Egypt's primary concern stemmed from the potential threat posed by powerful religious opposition groups.

Egypt's approach to the Internet reflected this duality.

- **Economic and Technological Ambitions:** Egypt aspired to leverage the Internet's economic and technological benefits. This ambition was reinforced by Egypt's position as a leader in the Arab world in terms of communication and technology. Egypt was among the first Arab countries to connect to the Internet, driven by the goal of integrating into the global economy. This vision, championed by the president himself, aimed to establish Egypt as a regional Internet hub and software exporter. The government implemented various measures to achieve this objective, including promoting the domestic technology market, fostering competition through reduced communication costs, and launching a government initiative for free Internet access. These efforts resulted in a significant rise in Internet penetration rates despite the countries' relatively low human capital base, which continues to hinder broader Internet use compared to other Arab nations.
- **Maintaining Political Stability:** Concurrently, the government prioritised maintaining political stability, even if it meant restricting content deemed harmful to religion and its values. Government oversight of Internet activity began as early as 2001, with a focus on filtering content related to:

- Politics: This included bans on content promoting terrorist organisations, human rights violations within Egypt, and criticism of senior government officials.
- Religion: This included content addressing Coptic-Muslim relations and the promotion of modern interpretations of Islam.

Egypt's Internet regulation approach shares characteristics with Syria and Saudi Arabia but exhibits unique elements.

- **Similarities with Syria:** Like Syria, Egypt prioritised monitoring Internet activity to safeguard its political system. In both countries, content critical of the government, human rights abuses, and terrorist organisations was subject to restrictions.
- **Similarities with Saudi Arabia:** Egypt, like Saudi Arabia, established a dedicated unit to investigate Internet crimes. Additionally, both countries placed some responsibility on Internet cafe owners to identify and monitor users.
- **Egyptian Uniqueness:** Egypt's approach diverged from Saudi Arabia's focus on religious content. The Egyptian government restricted content related to interfaith relations and specific interpretations of Islam, reflecting its concern about challenges posed by religious opposition groups. Furthermore, unlike Saudi Arabia, which primarily targeted "immoral" content, Egypt maintained relatively high Internet access costs, potentially limiting Internet penetration.

While Egypt's Internet regulation exhibits some overlap with Syria and Saudi Arabia, its specific focus on religious content and its economic approach to Internet access distinguish it as a unique case.

Jordan – Jordan's approach to Internet regulation has been characterised by a degree of tolerance compared to its control of other media outlets. This stance has drawn criticism from conservative elements within the country who advocate for blocking pornography and gambling websites. Despite this pressure, the Jordanian authorities have generally granted preferential treatment to the Internet regarding content restrictions.

Two events exemplify this distinction:

- **1998 Magazine Ban and Online Availability:** In 1998, Jordanian authorities banned the import of the London-based magazine "Al-Quds al-Arabi," citing articles deemed critical of the government. However, the magazine's full text remained accessible online, with advertisements for the website appearing in Jordanian newspapers. This incident highlights the government's seemingly relaxed approach to online content compared to traditional print media (Human Rights Watch, n.d.-b).
- **2002 Blocking of Anti-Government Website:** A notable exception to this trend occurred in 2002, when Jordanian authorities blocked access to "Arab Times," an anti-government website. This action suggests that the government retains the capacity to restrict online content, particularly when it perceives a direct threat to its authority (Gomes 2002).

Jordan's Internet regulation exhibits a more nuanced approach than other countries in the region. While some level of content control exists, the government generally displays greater tolerance for online content than for content disseminated through traditional media channels.

Iran – Iranian authorities justify Internet censorship as a means of safeguarding public morality. However, this justification has been accompanied by a growing focus on restricting political content. Iran currently implements a policy to limit Internet access, with specific categories of websites targeted for blocking.

These blocked categories include:

- **Pornography:** Consistent with the stated goal of moral protection.
- **Reformist Party Websites:** Indicating an effort to control political discourse online.
- **News and Religious Websites:** Suggesting broader censorship beyond purely political content, although the specific criteria for blocking in these categories are unclear.

- **Women's Rights Websites:** Highlighting potential restrictions on content related to social issues.

The Iranian government implements a multi-faceted strategy to regulate Internet access and user activity. These restrictions have positioned Iran among countries perceived as hostile to Internet freedom. The intensity of these restrictions appears to correlate with national election cycles, with periods of heightened filtering observed around:

- Local council elections in February 2003
- Parliamentary elections in February 2004
- Presidential elections in June 2005
- Local council and Assembly of Experts elections in December 2006
- Presidential elections in June 2009

Estimates of the number of websites blocked by Iran vary considerably. Sources from the early 2000s suggest a range of 10,000 to 15,000 blocked sites. However, a mid-2004 report claimed that Iran blocked over 100,000 foreign and 200 domestic websites. This significant discrepancy highlights the difficulty of obtaining reliable data on Internet filtering practices in Iran.

The process of website blocking reportedly involves the Iranian government transmitting lists of targeted sites to local communication companies, who then relay these instructions to ISPs within the country.

Iranian authorities block a wide range of websites, including:

- News websites
- Blogs
- Online communities
- Pornography websites
- Websites of reformist groups
- Websites addressing women's rights issues

Interestingly, websites containing Farsi (Persian) content appeared more susceptible to blocking than identical content in English (Persian Journal 2005b; OpenNet Initiative 2004a).

This observation is supported by Iranian blogger Hossein Derakhshan's (hoder.com/weblog) claim that Iran does not have a specific policy targeting English-language websites. Derakhshan cites two pieces of evidence:

- The occasional lifting of blocks on some English-language websites after a short period.
- The accessibility of certain websites in English while their Farsi counterparts remain blocked.

These observations suggest a degree of inconsistency in Iran's website-blocking practices. The rationale behind this inconsistency, however, remains unclear.

Iranian authorities implemented website blocking measures to target a variety of content, including:

- **Reformist Party Websites:** The online sphere mirrored the competition between political conservatives and reformists in Iran. During election cycles, websites associated with reformist parties were frequently blocked. Examples include website blocks preceding the 2003 local council elections, the 2004 parliamentary elections, and the 2006 local council and Assembly of Experts elections. These blocked websites sometimes included content critical of the government's treatment of women.
- **Foreign Websites:** Foreign websites were also blocked, particularly those perceived as promoting viewpoints critical of the Iranian government (BBC News 2003; Scullion 2003a). Early targets included Voice of America and Farda Radio websites, known for broadcasting in Farsi and catering to Iranian audiences. In the lead-up to the 2006 local council elections, reports indicated blocking several Western websites, including Amazon, YouTube, Wikipedia, IMDB, and the New York Times (Tait 2006).

The rationale behind website blocking in Iran sometimes appeared inconsistent. For instance, some blocked English-language websites were occasionally unblocked after a short period. Additionally, certain websites remained accessible in English while their Farsi counterparts were blocked. These inconsistencies highlight the complexity of Iran's Internet filtering practices.

The Iranian government's approach to website blocking lacked complete transparency. In July 2003, a list allegedly containing dozens of targeted political websites, blogs, and circumvention tools reportedly circulated, instructing Internet and content providers to block them (EDITOR: MYSELF 2003).

However, the effectiveness of these blocking efforts remained unclear. Testing conducted in August 2003 revealed discrepancies between reported blocked websites and actual accessibility (The Hacktivist 2003).

A more extensive experiment in October 2005 identified 718 blocked websites out of 3,146 tested in Iran. This included:

- **129 out of 643 blogs:** Suggest filtering online political discourse.
- **21 out of 54 opposition websites:** Highlighting the government's targeting of content critical of the regime.
- **16 out of 40 anonymity services:** Indicating an interest in restricting access to tools that could circumvent online censorship.

Recognising the growing influence of user-generated content on blogs, Iranian authorities implemented measures to restrict access to platforms that facilitated blogging activity. In August 2005, the local communications company reportedly directed ISPs within the country to block access to "blogrolling.com." This website was a popular tool for bloggers to track updates on other blogs, making it a valuable resource for the Iranian blogging community (Stop Censoring Us 2005a).

Iraq – A 2006 test conducted at the Internet service provider Uruklink did not detect any evidence of Internet filtering in Iraq during that period. Furthermore, no documented government activity was aimed at restricting unrestricted Internet

access within the country during the second half of the first decade of the 21st century (2004-2006). However, it is essential to note that the absence of evidence for filtering in 2006 does not guarantee complete Internet freedom throughout the entire timeframe (OpenNet Initiative 2007; Hassan 2005).

Qatar – The Qatari government officially prohibits website blocking or content censorship. This stance is supported by the fact that Qatar boasts relatively high Internet accessibility for users in the MENA region, with pornography being the primary category of blocked content (The Arabic Network for Human Rights Information, n.d.-d). However, there have been allegations of a more nuanced reality. These allegations suggest that Internet filtering may occur through:

- **Blacklists:** A list of prohibited websites potentially maintained and updated by the Qatari Telecommunications Company (Q-Tel).
- **Filtering Software:** Software designed to restrict access to unwanted websites.
- **ISP Monitoring:** Potential government oversight of private Internet service providers.

Uncertainties and Inconsistencies: Reports also suggest inconsistencies in any potential filtering practices. These inconsistencies may manifest in the following:

- **Temporal Fluctuations:** Websites blocked at one point may become accessible later due to external pressure.
- **Geographic Variations:** Blocking practices may differ depending on the ISP used and the user's location within Qatar.

The available information regarding Internet censorship in Qatar presents a mixed picture. While the government officially rejects censorship, some evidence suggests a more restrictive approach may be implemented, with potential inconsistencies in its application.

Libya – The growing popularity of the Internet in Libya coincided with a heightened awareness of its potential among opposition groups. These groups recog-

nised the Internet's value as a communication tool, enabling them to connect with various parties domestically and internationally.

The rise of Internet use in Libya prompted a response from the authorities, who implemented stricter regulations on online activity. These restrictions were so severe that Libya was classified as one of the world's 15 worst offenders regarding Internet freedom (Reporters Without Borders 2005g).

Saudi Arabia – Saudi Arabia exhibits significant restrictions on freedom of expression in traditional media and online. The country consistently ranks among the lowest in press freedom within the MENA region, often placing alongside Iran and Libya at the bottom of these rankings. Similarly, Saudi Arabia is positioned among the world's worst offenders regarding Internet freedom.

Focus on Religious and Moral Content: The primary justification for Internet monitoring in Saudi Arabia stems from religious and cultural concerns rather than a focus on political opposition. This approach reflects the tension within the Saudi government between upholding traditional values and embracing the potential benefits of widespread Internet access. Unlike the Syrian regime, which prioritises economic benefits over political considerations, Saudi Arabia prioritises protecting its citizens from perceived social challenges that could undermine religious and moral values.

Focus on Content, Not Political Dissent: Consequently, Internet censorship in Saudi Arabia primarily targets content deemed religiously or morally offensive, as opposed to content critical of the government itself.

In 2004, Saudi Arabia implemented one of the world's most extensive Internet filtering systems. Official statements claimed that nearly 400,000 web pages were blocked, with the goal of "protecting citizens from offensive content and content that violates the principles of Islam and the social norms" (Reporters Without Borders 2004c).

This approach reflects a broader challenge many conservative regimes face in the digital age: balancing traditional censorship practices with the desire to participate in the global information society. The effectiveness of Saudi Arabia's filtering and monitoring measures in achieving their stated goals remains unclear. Some critics argue that these measures aim to restrict access to "inappropriate" materials and create the illusion that such content is entirely unavailable online.

Saudi Arabia's Internet censorship extends beyond pornography. The government also restricts access to websites that address sensitive topics or potentially conflict with religious or social norms. These categories include (Whitaker 2003):

- Women's rights
- Civil liberties
- LGBTQ+ issues
- Non-Islamic religions

The terrorist attacks of September 11, 2001, perpetrated primarily by Saudi nationals, triggered a significant shift in public discourse within the country. In the wake of these attacks and a subsequent wave of internal terrorism, discussions surrounding religious extremism, societal violence, terrorism, and incitement rose to prominence.

This newfound openness manifested in public forums beyond traditional media outlets. These discussions, characterised by a willingness to confront sensitive topics and challenge conventional norms, represented a poignant and honest attempt to grapple with complex issues. However, a reluctance to directly criticise the government or its leadership remained evident.

The Internet Service Unit (ISU) is the primary body responsible for Internet censorship in Saudi Arabia. This entity manages the country's technical infrastructure, including the ".sa" country code top-level domain. Furthermore, the ISU's control over the gateway used by all ISPs in the country grants it broad monitoring capabilities over online activity within Saudi Arabia.

Content Filtering and Blocking: The ISU implements content filtering and blocking through intermediary proxy servers between Saudi and global Internet users.

These proxy servers intercept website requests from local ISPs, filtering or blocking them based on a regularly updated list of prohibited website addresses.

Rationale and Oversight: The stated justification for blocking websites centres on content that violates Islamic traditions or national regulations. A committee overseen by the Minister of the Interior reportedly selects websites for blocking and supervises the overall process. The King Abdullah City for Science and Technology (KACST) has also been authorised to block pornography websites directly. However, blocking other websites remains less transparent, with security agencies sometimes issuing direct blocking instructions to the ISU.

Transparency Claims: Despite this lack of transparency in certain areas, Saudi Arabia's Internet monitoring and filtering policy is relatively straightforward. Users encountering a blocked website reportedly receive a notification and may even suggest websites they believe merit blocking to the ISU.

Alongside Internet censorship efforts, Saudi authorities have undertaken initiatives to close Internet cafes. An April 2005 report documented the closure of 25 Internet cafes within a single neighbourhood. These closures were reportedly part of a broader operation targeting criminal activity in the area, which included apprehending drug dealers and pickpockets.

The mechanism – According to Brian Whitaker, Saudi Arabia's Internet content filtering system reportedly operates in two stages (Whitaker 2000):

1. **Initial Filtering:** Upon receiving a user's request for a webpage, the King Abdullah City for Science and Technology (KACST) system automatically evaluates the content against a predefined list of approximately 30 blocking categories. Approved pages are cached within the system's memory to avoid excessive delays caused by repeated evaluations of the same content.

2. **Content Caching:** When a user requests a previously approved website, the system retrieves the cached copy stored on its special servers instead of directing the request to the original website. This approach expedites access to frequently visited websites by eliminating the need for real-time content evaluation.

In a unique approach, the Internet Service Unit (ISU) established an email address (abuse@isu.net.sa) and an online form for users to report websites they believe warrant blocking. This initiative reportedly receives hundreds of daily inquiries from a dedicated team within the ISU.

The level of public participation appears to be significant, although not always aligned with the authorities' decisions. For instance, news reports documented the dissatisfaction of some citizens whose requests to block a website teaching "sorcerers, spells, and fortune-telling" were not fulfilled.

The content – The Internet Service Unit (ISU) filters and blocks websites across various categories:

- **Sexual Content:** This includes websites with explicit sexual content and those associated with the LGBTQ+ community.
- **Political Content:** Website censorship has targeted political opposition for many years. Examples include the Movement for Islamic Reform (MIRA) website (miraserve.com), which has been blocked almost since the Internet arrived in Saudi Arabia. Similarly, websites advocating democratic reforms have been blocked, such as saudhouse.com (since 1999), belonging to the Committee against Corruption in Saudi Arabia. The censorship extends beyond direct opposition to include websites promoting reformist views, even if not explicitly critical of the government.
- **Religious Content:** To maintain a state-sanctioned interpretation of Islam, the ISU blocks websites associated with Shia Islam (e.g., shiaweb.org, yahosein.com, alshi3i.cjb.net) and those offering alternative interpretations to the dominant Wahhabi school of thought, including Sufi and Ismaili websites.

- **Human Rights Content:** Websites promoting human rights are also subject to blocking, including the Association for the Protection of Human Rights websites in the Kingdom of Saudi Arabia and The Arabic Network for Human Rights Information (HRinfo). A further example is the blocking of the Jordanian website amanjordan.org (August 5, 2003) due to articles on violence against women in Saudi society. This block was only lifted in September 2003 (Bashtahi 2003).

Economic Content: The ISU has also implemented website blocking, motivated by financial considerations. For instance, the websites of competing telecommunication companies are blocked to maintain the government-owned company's monopoly in the telecommunications market. This approach is justified by the argument that services like Internet telephony (VOIP) could harm the revenue of state-controlled communication companies.

A three-year study by the OpenNet Initiative examined the nature of website blocking in Saudi Arabia, analysing approximately 60,000 website addresses. The study revealed the following breakdown of blocked website categories (Reporters Without Borders 2004c):

- **Pornography:** This category exhibited the highest blocking rate, with 98 per cent of tested websites inaccessible. The Saudi government's sensitivity to pornography is further evidenced by the ISU's independent identification and blocking of new pornographic content at a significantly faster rate than the update frequency of the American filtering software used by the system.
- **Gambling:** Websites associated with gambling were blocked in 93 per cent of cases.
- **Drugs:** Websites related to drugs were blocked in 86 per cent of cases.
- **Religious Conversion and Circumvention Tools:** Websites promoting religious conversion and those offering tools to bypass Internet filtering were blocked in 41 per cent of cases

The OpenNet Initiative study also revealed the distribution of blocking efforts across different website categories. Significantly lower blocking rates were observed for:

- LGBTQ+ Content (11 per cent)
- Political Content (3 per cent)
- Israel-Related Content (2 per cent)
- Religious Content (Less than 1 per cent)
- Alcohol-Related Content (1 website)

These findings suggest a more targeted approach to website blocking than previously assumed. The data may indicate that, beyond pornography, most blocking actions stem from user reports to the authorities, resulting in a focus on specific content deemed inappropriate rather than a comprehensive filtering strategy.

However, the study also identified instances of over-blocking, potentially linked to the heightened sensitivity surrounding pornography within Saudi Arabia.

Syria – The OpenNet Initiative, an organisation advocating Internet freedom, has designated Syria the "biggest prison in the Middle East" for Internet users and bloggers (2007). In 2009, the organisation also ranked Syria among the ten worst countries globally for bloggers. These designations reflect the Syrian government's harsh treatment of online activity, including the detention and imprisonment of users for several years in some cases (Committee to Protect Journalists 2009).

Government Control and Monitoring: An essential element of Syria's Internet censorship strategy hinges on the government's control over the two primary ISPs operating in the country. This control enables the authorities to monitor Internet traffic, including email messages, to identify and track users' online activity.

The Syrian authorities maintain a continuously expanding blacklist of websites deemed inappropriate for access. These websites fall into two primary categories:

- **Morally and Religiously Objectionable Content:** This category encompasses websites offensive to local moral and religious values and traditions, such as pornography.
- **Politically Dissenting Content:** Websites categorised as "hostile" target the Syrian regime's legitimacy and are subject to blocking.

Internet cafes in Syria have reportedly served as a means for some young people to access pornography, a category of content restricted by the government. Some cafe owners have even cited this usage as a significant source of income.

A reporter's account from a Damascus Internet Cafe suggests a prevalence of young users, with estimates claiming that 90 per cent fall within this age group. However, it is essential to acknowledge that this is a single anecdotal account.

The potential for accessing restricted content through Internet cafes has reportedly led some parents to cancel Internet subscriptions and increase their supervision of children's online activity. In response, the Ministry of Communications has disseminated messages through media outlets, possibly reflecting parental concerns, urging vigilance and caution when using the Internet (The Arabic Network for Human Rights Information, n.d.-e).

The Syrian government's blacklist of "hostile websites" encompasses a broad range of content deemed critical of the regime or its policies. This category includes:

- **Israeli Websites:** All websites with the ".il" domain extension are blocked, along with websites hosted outside of Israel but associated with the country.
- **Human Rights Websites:** Organizations promoting human rights, such as the Syrian Human Rights Committee (shrc.org) based in London, are subject to blocking.
- **Minority Websites:** Websites affiliated with the Kurdish minority and those providing information about their situation are also blocked.

- **Dissenting Media:** Local and international websites offering news and articles critical of Syrian government actions and opposition websites are targeted for blocking.
- **Webmail Services:** Certain webmail services have also been blocked in Syria.

Like Internet censorship practices in other MENA countries, Syria's website blocking policy fluctuated over time, with periods of stricter or looser controls. Rorts suggest that "the policy of blocking websites narrowed and expanded from time to time" (Gooya news 2004; The Arabic Network for Human Rights Information, n.d.-e).

While Syria and Saudi Arabia restrict Internet access, the underlying motivations differ. In Syria, the government's censorship efforts likely stem from concerns about maintaining regime stability and controlling dissent. In contrast, Saudi Arabia's focus seems to be on preserving traditional moral values and religious principles.

Government Control and Monitoring: Both countries delayed introducing public Internet access until they established technological capabilities for monitoring online activity and identifying problematic users.

Western Service Restrictions: In addition to government-imposed website blocking, some Western companies have also restricted access to their services in Syria. For instance, LinkedIn temporarily blocked access in April 2009, citing human error, but lifted the ban shortly after that due to user protests, including those expressed on Twitter. However, other companies, such as Google and Sun Microsystems, have implemented more permanent restrictions on specific services, citing compliance with US regulations on trade with Syria.

Tunisia – Similar to other countries in the region, criticism of the government is a sensitive topic for Tunisian media, including online platforms. The government has implemented measures to restrict access to critical or politically sensitive websites. The nature and extent of these restrictions remain un-

clear, although filtering software like SmartFilter (used by Iranian authorities) may be employed.

A 2005 analysis suggested that Tunisia may utilise SmartFilter software for website blocking. However, unlike other countries that employ this software, Tunisia reportedly does not display a notification page informing users of blocked content. This lack of transparency makes it difficult for users to distinguish between blocked websites, technical difficulties, and unavailability (Reporters Without Borders 2004b).

Reports indicate that website blocking in Tunisia extends to various categories, including:

- Local and foreign news websites
- Websites of local and foreign human rights organisations
- Websites associated with opposition groups

Additionally, some webmail services, such as Hotmail, have reportedly been subject to blocking in the past. The justification for blocking these services may be related to the perceived challenges associated with monitoring traffic on such platforms compared to email services like Outlook Express.

Two independent analyses conducted in September 2005 shed light on the extent of website blocking in Tunisia.

- **Private ISP Test:** A private ISP test examined 1,947 websites within Tunisia. The results indicated that 184 websites (approximately 9.5 per cent) were blocked. Additionally, 39 out of 48 proxy servers (81 per cent) were found to be inaccessible, potentially hindering attempts to circumvent Internet restrictions.
- **OpenNet Initiative (ONI) Study:** In the same year, the ONI also conducted a website blocking analysis in Tunisia. Their investigation tested 1,923 websites, revealing that 187 (approximately 9.7 per cent) were blocked. The study further found that 95 per cent of tested pornography websites and 87 per cent of websites facilitating anonymous Internet access were blocked.

These analyses suggest that website blocking in Tunisia in 2005 primarily targeted pornography and tools for bypassing Internet censorship.

United Arab Emirates – The UAE filters and blocks websites primarily for cultural and religious reasons, with political and media considerations playing a lesser role. This approach may seem contradictory given the UAE's aspirations to become the economic and technological leader of the Middle East, actively promoting the IT industry and Internet access.

However, the UAE government appears to be balancing technological advancement and preserving traditional societal values. Some segments of Emirati society are concerned that unfettered cultural openness could undermine Islamic principles and empower political extremists. Website blocking thus serves as a tool to manage this perceived tension.

The UAE prioritises website filtering based on concerns related to:

- Pornography
- Gambling
- Homosexuality
- Interfaith relationships
- Religious conversion (mainly targeting Muslims)
- Activities of extremist groups
- Criticism of Islam
- Political criticism of the government

An analysis of website accessibility within the UAE suggests that approximately 15.4 per cent of tested addresses were blocked. This filtering is reportedly achieved through a centralised system utilising SmartFilter software, similar to the filtering systems employed by Iran, Tunisia, and Saudi Arabia.

Most of the blocked sites are pornography, gambling, hacking, alcohol, anonymised services, religious conversion, matchmaking sites in the English language and sites with the .il suffix. It can also find a blanket blocking of sites that

contain the word fuck regardless of the nature of the site. Because of this, pages and websites that have nothing to do with the stated goals of the UAE in blocking sites are blocked.

In July 2005, the UAE blocked access to the Armenian news website Hetq Online (hetq.am). This action stood out because the UAE tolerated websites critical of its internal politics and news. The block seemingly stemmed from an article Hetq published that exposed the trafficking of Armenian women into the UAE. Users attempting to access the website from within the UAE encountered a message stating: "Sorry, the site you are trying to connect to has been blocked because of content which infringes religious, political, cultural and moral values in the United Arab Emirates."

The UAE's blocking of Hetq Online in 2005 demonstrates two points. First, it confirms the UAE's practice of website censorship. Second, it reveals a degree of transparency as users receive a message explaining the block. This contrasts with some countries where users encounter inaccessible websites without any explanation, leaving them unsure if the site is blocked or malfunctioning (Reporters Without Borders 2005d).

Self-Censorship

Etisalat, the dominant communications company in the UAE, operated through its subsidiary EIM. While EIM theoretically facilitated easier monitoring of online activity, there was no evidence of this being actively practised. However, a combination of strict social and political limitations, coupled with the potential for email and online monitoring, fostered a culture of self-censorship among Internet users. This self-censorship extended to topics deemed sensitive, including religion, morality, government allies, and members of the ruling families. Local journalists practised self-censorship, and foreign residents depended on state-issued work permits for their livelihoods (Human Rights Watch 1999c; OpenNet Initiative 2005b).

The UAE prioritised website censorship for content deemed critical of Islam, targeting Muslims (although English-language Christian websites remained accessible), and discussions of homosexuality in the Middle East. Interestingly, authorities did not appear to identify and block all potentially objectionable content systematically. For instance, they made few attempts to block Arabic-language matchmaking sites, even those containing content about Israel (including Israeli sites without the ".il" suffix) or references to the ".il" domain itself.

The Reporters Without Borders organisation did not classify the UAE as either an "Enemy of the Internet" or a nation requiring Internet surveillance due to resistance.

Despite claims that censorship targeted only pornography, the UAE shared similarities with Saudi Arabia in its online content restrictions. Both countries restricted websites deemed harmful to their values and culture, including those promoting pornography, disrespecting Islam or its holy sites, criticising government officials, disrupting public order, or inciting violence.

Lack of uniformity in blocking websites in the same country - There are many examples of the phenomena of geographical unevenness in the blocking of websites:

- **Iran** – Concerns arose about the lack of uniformity in website blocking in Iran. A senior official from Delta Global, a local company that won a government tender to manage the Internet censorship system, expressed a desire to centralise the filtering system. He argued that the existing system, managed by hundreds of ISPs, resulted in inconsistencies. Websites could be accessible in one city but blocked in another (Reporters Without Borders 2005f). A possible explanation may be found in the following remark: "Not only has its approach been scattershot, diffused across duplicative and often competing power centres, but it has also often been reactive as it seeks to address problems posed by the public embracing new technologies" (Rubin 2019).
- **Saudi Arabia** – Saudi Arabia's website blocking practices exhibited inconsistencies. Evidence existed of previously blocked sites becoming accessible

again, and conflicting reports emerged regarding the status of specific websites (TheHacktivist 2003; Miller 2004). Users could sometimes access certain services within a blocked website while the rest remained inaccessible. Occasional technical failures even allowed access to all typically blocked sites. A foreign reporter in Riyadh described the censorship system as "clumsy". He highlighted the challenge for users seeking current news due to the slow update of cached content, citing outdated BBC information as an example. Furthermore, the system failed to block intrusive marketing messages displayed in pop-up windows despite their seemingly censorable nature (Whitaker 2000).

Additionally, reports suggested a gradual increase in the availability of non-Muslim religious websites compared to the past (Miller 2004).

In 2003, Saudi Arabian authorities appeared to exercise discretion in website blocking, considering international requests. They blocked GayMiddleEast.com in June but lifted the restriction a month later following a request from the International Press Freedom Organization. The organisation reportedly argued that the website did not contain pornography after a review by Saudi authorities (IFEX, n.d.).

- **United Arab Emirates** – A study in the UAE revealed inconsistencies in website blocking across different communication networks. The study compared the filtering results of two networks, particularly regarding websites originating from Israel. The discrepancies likely stemmed from variations in the filtering software version or its configuration. The study also aimed to analyse these differences across various blocking categories comprehensively. However, the specific details of this breakdown were not provided (OpenNet Initiative 2005b).

Pornography – Across the Middle East, website blocking practices varied in their focus. Some countries, like Egypt and Syria, prioritised blocking politically sensitive content. Others, particularly Gulf nations and Saudi Arabia, focused on restricting access to socially sensitive material. However, officially, most countries aimed to limit access to pornography.

Analyses revealed a range of approaches. Algeria, Jordan, and Lebanon rarely blocked websites containing pornography. Egypt implemented limited blocking but focused its Internet police on monitoring users who accessed such sites. Tests in Iraq did not detect website blocking, although reports suggested a single cellular network operator in Basra independently censored violent and pornographic content.

Finally, some countries like Libya and Morocco prioritised blocking opposition websites and news content.

Across the Middle East, website blocking practices varied in their focus. Some countries, like Egypt and Syria, prioritised blocking politically sensitive content. Others, particularly Gulf nations and Saudi Arabia, focused on restricting access to socially sensitive material. However, most countries, at least officially, aimed to limit access to pornography.

Analyses revealed a range of approaches. Algeria, Jordan, and Lebanon rarely blocked websites containing pornography. Egypt implemented limited blocking but focused its Internet police on monitoring users who accessed such sites. Tests in Iraq did not detect website blocking, although reports suggested a single cellular network operator in Basra independently censored violent and pornographic content.

Finally, some countries like Libya and Morocco prioritised blocking opposition websites and news content (vigilant tv 2002).

Website blocking in the Middle East encompassed various content categories beyond pornography. Tunisia, for instance, blocked a wide range of websites in 2005, including those related to human rights, opposition groups, and news outlets, alongside a significant portion (95 per cent according to a 2005 test) of pornography sites.

Similar restrictions on pornography emerged in other countries. Hamas in the Gaza Strip reportedly ordered a local Internet provider to block such websites in

2008 (Reuters 2008). Iran has also maintained a long-standing focus on blocking pornography. A regional network was shut down in 1995 due to concerns about its use for sex chat (Human Rights Watch 1996), and government officials have consistently defended website-blocking policies targeting "pornographic and immoral" content (Scullion 2003b).

Syrian website blocking targeted two main categories: content deemed harmful to society and morality (primarily pornography) and content critical of the state and government (opposition, human rights, and news websites). Public exposure to pornography reportedly led to a rise in parental concern. Parents cancelled subscriptions and increased supervision of their children's Internet usage. The Ministry of Communications, possibly responding to this public pressure, issued warnings about the need for vigilance and caution online (The Arabic Network for Human Rights Information, n.d.-e).

Saudi Arabia implemented a website blocking system that focused heavily on content deemed immoral, particularly pornography. The Internet Service Unit (ISU) was responsible for blocking pornographic websites, achieving a near-perfect success rate in tests. This censorship was stricter than for other categories. The ISU reportedly based its actions on targeted monitoring and public reports of inappropriate websites. However, Saudi Arabia's emphasis on moral control sometimes led to over-blocking, resulting in the censorship of websites with inoffensive content.

An analysis in Bahrain found that website blocking for morality, religion, and politics was uncommon. However, a specific incident highlighted public concerns about online pornography. Students accessed such websites from a school computer lab, causing tension. The school criticised the Ministry of Education for inadequate supervision and urged them to implement solutions, such as blocking software, to prevent inappropriate computer use in the lab.

Social Networks – The rise of social media coincided with increased Internet access, fundamentally changing how citizens receive and transmit information.

These platforms allowed users to bypass government restrictions on free speech and engage with various organisations. Consequently, online pressure groups emerged, advocating for social and economic reforms within the country.

- **Facebook** – In Syria, hundreds of Facebook groups focused on various topics emerged, attracting memberships ranging from a handful to several thousand. These groups catered to diverse interests like tourism, student life, business, technology, arts, music, cars, and sports. They served both Syrian residents and the diaspora, fostering a sense of community.

  Beyond social interaction, Facebook groups in Syria functioned as platforms for online activism, sometimes leading to real-world change. A public outcry erupted on Facebook regarding child sexual exploitation after the rape of a young girl. This online campaign fuelled a public debate and potentially influenced the authorities. Similarly, an online fight against a proposed marriage law, believed by some to be instrumental in its cancellation, highlighted the groups' influence. Facebook activism even extended to advocating for lifting website restrictions and a personal appeal to the president by one group. Locally, bloggers used Facebook to call for a boycott of cellular providers due to high costs and poor service quality. Additionally, Syrian groups campaigned for the release of detained bloggers, expressing protest against government actions.

  In 2009, the Syrian government escalated tensions with Facebook, calling for a boycott of the platform. This move stemmed from Facebook's decision to designate the Golan Heights as part of Israel and register users from these settlements as Israeli residents. The Syrian government had previously considered these users Syrian residents. Reports also indicated plans to block Facebook entirely within Syria. However, the website had already been inaccessible for roughly two years. This broader Internet censorship effort also targeted other social networking sites and tools that allowed users to circumvent government restrictions, including those facilitating anonymous Facebook access.

- **YouTube** – Since its launch in 2005, YouTube has faced frequent website blocking in many countries worldwide. The platform's reliance on video content makes it susceptible to hosting material deemed offensive from religious, moral, cultural, or political perspectives. Consequently, several Arab and Islamic countries have implemented various forms of YouTube censorship.

  Several Arab and Islamic countries have censored YouTube content that is deemed objectionable. The UAE blocked the platform in mid-2006 following a seven-part documentary exposing a prostitution ring involving Armenian women in Dubai. Iran followed suit in December 2006, citing concerns about immoral content on YouTube and other video-sharing websites (Tait 2006). In Egypt, reports emerged in November 2007 of a local user's YouTube account being blocked (Al Hussaini 2007). Similarly, Morocco blocked YouTube for five days in May 2007 in response to videos critical of the government's treatment of the people in Western Sahara (MOTIC 2007). Syrian authorities implemented a series of YouTube blockages in the second half of 2007. All Internet providers blocked the site in late July, resulting in a blank page upon attempted access (Moey 2007). This initial block was followed by another targeting a specific video in late August. The footage, deemed offensive, depicted the First Lady in a revealing outfit resembling Marilyn Monroe, welcoming her husband at the airport (Curt 2007). Finally, in late November, YouTube became part of a more significant censorship effort targeting 109 websites critical of the government (Reporters Without Borders 2007). This broader blocking campaign highlighted a growing trend of Internet censorship in Syria, with the number of blocked sites doubling in just two weeks. Tunisia also censored YouTube content on multiple occasions. In early November 2007, authorities blocked the site without any explanation. They implemented another block in May 2008, targeting a video containing testimonies from former political prisoners and human rights activists. This incident suggests that content critical of the government triggered censorship (Ben Gharbia 2008a). A Sudanese blogger also reported that the website was blocked in July 2008, though the reasons remain unclear (Too Huge World 2008).

Unlike other countries with one-time blocks or blanket censorship, Turkey employed a strategy of repeated YouTube blockades. A court order in March 2007 instructed the media authority to block the platform for several years, marking another instance of government censorship (Cashmore 2007). Turkey's system differed because legal authorities directed the block, not the government itself. The primary justification for these blockades centred on videos deemed harmful to the image of Mustafa Kemal Atatürk, the founder of Turkey, and national unity (Reporters Without Borders 2008d; Ben Gharbia 2007; Zaharov-Reutt 2007).

A distinct pattern emerged in the approach of Arab and Islamic countries towards YouTube. While website blocking occurred globally, it was most prevalent in this region. Like website blocking, motivations for YouTube censorship fell into two main categories: moral and cultural concerns and concerns about protecting government legitimacy. Countries with moral or cultural justifications blocked content deemed inappropriate. Others, fearing criticism of past or present rulers or discussions of human rights abuses, targeted content critical of the government.

The duration of blocking also varied. Some countries implemented temporary blocks lasting a few days, typically in response to specific videos. Others opted for permanent or long-term blocks. Unlike Turkey, where court orders triggered YouTube bans, most countries relied on government or media authority decisions. Interestingly, YouTube sometimes complied with government requests, removing targeted videos.

Regulations

Regulation of the Internet and its usage is widespread across most countries in the MENA. This trend gained momentum in the early 21st century, with a surge in regulations implemented between 2000 and 2009. These regulations often aimed to bring online publishing under the purview of existing press and publication laws. Additionally, they frequently required local websites to register with government authorities before launching (OpenNet Initiative, n.d.-b).

Bahrain – In 2004, five members of Bahrain's Shura Council introduced a bill advocating for regulations on multimedia communication in the country. The legislation aimed to adapt to advancements in various fields and technological changes. Proponents of the bill emphasised the importance of freedom of communication in a democratic society, highlighting its role in facilitating the expression of public opinion and ideas. They envisioned a law that embraced the spirit of the modern era, free from restrictions or penalties on information dissemination.

In December 2005, Bahrain's parliamentarians passed a bill restricting unsupervised Internet access for young people in cafes. This legislation envisioned measures like website blocking or access limitations to protect children. The proposal, approved by the parliament's services committee, called for increased government oversight of Internet cafes. This included the removal of existing partitions, ensuring physical separation between genders, and limiting operating hours, particularly at night. The proposed law also mandated license revocation for cafes violating these regulations. Notably, this legislation marked a significant shift, as Bahrain had no restrictions on website access or Internet cafe operations.

In April 2005, Bahrain mandated the registration of all websites, including private ones, with the Ministry of Information within six months. Unlike online registration common elsewhere, this process required in-person visits to government offices for verification and the issuance of an identification number. Website owners were then obligated to display this number on their sites. Despite assurances of automatic registration and content neutrality, the new regulations arguably narrowed Internet freedoms. The requirement for website administrators to register and potentially face liability for content mirrored the responsibility of newspaper editors, raising concerns about potential censorship (Reporters Without Borders 2005e).

Egypt – In December 2002, an amendment to Section 65 of the Communications Law in Egypt created a potential tension between citizen privacy and government surveillance. While the amendment reaffirmed the right to privacy, it also grant-

ed security authorities the legal power to violate communications confidentiality with a court order limited to 30 days. These orders could only be issued on suspicion of serious crimes punishable by more than three years in prison.

Further restrictions on Internet freedom emerged in February 2005. The Ministry of the Interior launched a campaign targeting Internet cafes, demanding owners maintain records of customers' names and ID numbers. Refusal to comply and submit such documents to the police resulted in cafe closures. These measures reportedly led to declining Internet cafe users, negatively impacting owners' income.

Jordan – Before September 2001, Jordan stood out among Arab countries due to its relatively unrestricted Internet environment. The lack of legislation or website blocking contributed to this freedom. However, signs of tightening regulations emerged in 2004. Reports indicated plans to incorporate the Internet into radio and television broadcasting laws. This draft law raised concerns, as it potentially criminalised students who posted songs or poems online without explicit permission.

Despite the proposed restrictions, the Jordanian government also enacted measures to facilitate public Internet access. One such decision lowered the age requirement for Internet cafe use with parental approval from 16 to 13. Additionally, Internet cafe location and size regulations were introduced (The Arabic Network for Human Rights Information, n.d.-a).

Iran – In Iran, the initially unregulated Internet landscape experienced a shift towards increased government oversight as its popularity grew. Despite official claims of protecting public morals, censorship efforts quickly expanded to target political content. This deliberate policy of Internet control involved legislative restrictions.

In January 2003, a government committee comprising representatives from cultural, intelligence, and media ministries was established. This committee com-

piled a list of unsuitable websites and forwarded it to the Ministry of Communications and Internet providers for blocking. This action marked a turning point towards a more restrictive Internet environment in Iran (Reporters Without Borders 2004a).

In May 2003, following the February local council elections in Iran, Prosecutor-General Abd Allenbi Namazi announced the formation of a committee dedicated to tackling online offences. Namazi stated that individuals uploading content to Iranian websites could be prosecuted for violating the constitution and press laws, even without a specific Internet law (Committee to Protect Journalists 2005).

In June 2004, the Iranian Ministry of Justice Spokesperson, Oulam Hossein Ilham, revealed that the Supreme Council of the Cultural Revolution was drafting a law to regulate Internet content. This legislation aimed to restrict criticism of the government and its officials, the sale or purchase of alcohol online, and content deemed disrespectful to President Khatami or Ayatollah Khamenei. The proposed law included harsh penalties, with sentences of up to three years for publishing information threatening state security and six months for spreading "false information" about government officials.

Later that year, the Chairman of the Committee for Internet Crimes, Reza Parvizi, announced the finalisation of the Penal Law for Internet Crimes. While Parvizi claimed the revisions primarily focused on penalties rather than crime definitions, he also acknowledged changes to ISPs' role in content filtering. This suggested a potential shift in enforcing censorship (Stop Censoring Us 2004b).

A legal expert from the Isfahan Ministry of Justice, Kamran Zamanifar, referred in December 2004, in the period between the parliamentary elections and the presidential elections, to the need to legally deal with the new offences involving the Internet, emphasising Hackers (Islamic Republic News Agency (IRNA) 2004e).

In January 2005, the communication department director at Tabatba'i University identified a regulatory gap regarding blogs in Iran. He argued that existing written media laws were inadequate for the burgeoning blogosphere, containing thousands of active blogs. He called for specific legislation to regulate online content (Stop Censoring Us 2005b). In response to the upcoming local council elections in December 2006, the Iranian government implemented regulations in November of that year. These regulations mandated website registration with the authorities. The move faced criticism, but the Culture and Islamic Orientation Minister defended the policy in February 2008. He emphasised that websites failing to register with the ministry would be shut down (Reporters Without Borders, n.d.-b). On November 17, 2008, the Minister of Culture and Islamic Guidance reiterated the government's stance. He declared that any local website not registered with his office would face closure (Reporters Without Borders 2008c).

In April 2009, the Iranian Parliament passed a significant amendment to the 1986 Press Law. This amendment extended the application of the Press Law to online media and websites. The revised law aimed to establish a clear framework for online content by outlining the "rights, duties, legal protection, crimes, punishments, jurisdiction and hearing procedures" applicable to online platforms (OpenNet Initiative 2009a).

ISPs – Private ISPs emerged in Iran in 1994. However, their operation was subject to stringent government oversight. The Ministry of Intelligence and the Ministry of Culture and Islamic Guidance required ISPs to implement filtering systems. These filtering systems aimed to restrict access to websites deemed "political" or "immoral" by the authorities. The criteria for filtering were not publicly disclosed, but ISPs received extensive blacklists of websites to block.

Furthermore, authorities reserve the right to determine additional continuous filtering criteria (Stop Censoring Us 2004a). The Iranian government enforced compliance with these regulations. In 2004, at least twelve ISPs nationwide were shut down for failing to implement the mandated filtering systems (Reporters Without Borders 2004a).

The Iranian government imposed strict eligibility criteria for ISP managers. These requirements, as outlined on the website of the Data Communications Company of Iran, mandated that managers possess the following qualifications:

- **Iranian Citizenship and Loyalty:** Hold Iranian citizenship and demonstrate loyalty to the Islamic Republic›s constitution.
- **Religious Affiliation**: Belong to one of the religions recognised by the Iranian constitution.
- **Educational Background**: Possess a relevant academic degree.
- **Technical Expertise**: Demonstrate the necessary technical skills for managing an ISP.
- **Age Requirement**: Be at least 25 years old.
- **Clean Criminal Record**: Have no criminal convictions or moral blemishes.
- **Political Affiliation**: Hold no affiliation with or support for organisations deemed “anti-revolutionary” by the government.

Iranian regulations imposed significant restrictions on online content, applicable to ISPs and individual users. These restrictions, as outlined in the regulations (Bensedrine, n.d.), prohibited the following:

- **Religious and Political Content:**
  - Dissemination of anti-Islamic material or content deemed harmful to Islam.
  - Information violating the constitution, undermining state independence, or insulting the supreme leader.
  - Content damaging Islamic values, the Islamic revolution, or the political ideology of Ayatollah Khomeini.
  - Material undermining national unity or the legitimacy of the Islamic system.
  - Promotion of illegal groups or parties.
- **Security and Privacy:**
  - Publication of government documents or information related to national security, the military, or law enforcement.
  - Unauthorized access to private websites or attempts to crack computer passwords.

  - Attacks on other websites to disrupt their activity.
  - Attempts to monitor network information without authorisation.
  - Establishing unauthorised radio or television networks.
- **Social and Moral Content:**
  - Posting immoral images or content promoting drugs or cigarettes.
  - Defamation of public officials or law enforcement officers.
  - Disclosure of private information or violation of individual privacy.
  - Posting computer passwords or methods for obtaining them.
- **Financial and Commercial Activity:**
  - Engaging in illegal online commerce, including forgery, embezzlement, or gambling.
  - Selling, buying, or advertising illegal goods.

The regulations also mandated ISPs to:

- **Hold User Information:** Maintain user data, including IP addresses.
- **Provide Information to Authorities:** Disclose user information to the Ministry of Communications upon request.

Internet Cafe – In May 2001, Iranian authorities in Tehran shuttered over 400 Internet cafes, constituting a significant portion of the city's 1,500 cafes. This closure coincided with a new mandate requiring cafes to obtain licenses for continued operation. However, reports suggested that these licenses were unavailable at that time (Nua Internet Surveys 2001). Interestingly, a letter published in November 2002, approximately 18 months later, indicated that the number of Internet cafes in Tehran had rebounded to 1,500 (Nua Internet Surveys 2002).

This action sparked conflicting justifications. While officials cited economic concerns, claiming the closures aimed to combat losses incurred by the Telecommunications Company of Iran (TCI) due to discounted international calls offered by cafes, the TCI denied involvement.

Adding to the confusion, a media company representative claimed the closures targeted cafes hosting content deemed "anti-Islamic." This suggests a potential secondary motive – content control – alongside the economic justification. Furthermore, reports indicate that users were required to sign a commitment to avoid accessing "non-Islamic" websites. The closures in Tehran were not an isolated event. On August 25, 2004, reports documented the closure of three Internet cafes in Bushehr, suggesting a broader trend of government oversight of Internet cafes in Iran (Reporters Without Borders 2004e).

Websites – In December 2004, representatives from a consortium of cultural and security organisations in Iran petitioned the Ministry of Islamic Guidance. Their request urged the Ministry to implement a system for identifying and registering all websites operated within the country. This initiative, they argued, was necessary to establish a mechanism for monitoring and regulating domestic websites (Gooya news 2004).

Iraq - Despite pronouncements from the Iraqi government during the second half of the first decade of the 21st century, indicating plans to control "immoral" content, monitor Internet activity, and regulate cafes, evidence suggests a period of relatively unrestricted Internet access in Iraq between 2005 and 2009.

- An August 2009 OpenNet Initiative report found no official national Internet filtering policy or evidence of filtering by the state ISP (OpenNet Initiative 2009b).
- Independent tests conducted during this period (2005-2009) further corroborated the lack of technical filtering for various content categories (OpenNet Initiative 2009b).

Saudi Arabia – The government implemented regulations to control Internet access and activity in Saudi Arabia. The Council of Ministers Resolution of February 2001 established the initial framework, followed by additional regulations targeting Internet cafes in July 2003 and Internet Cafe in July 2003 (Arab Media 2001b). These regulations aimed to exert greater control over users of public Internet cafes within the Kingdom.

The 2001 Resolution focused on restricting content deemed harmful to Islam, the nation, and its officials (Qutsi 2003). It imposed limitations and obligations on various actors within the Internet ecosystem, including:

- ISPs
- Internet Cafe Operators
- Individual Users

The decision from February 2001 consists of the following (all emphasis is in the original) (Arab Media 2001a):

- "All Internet users in the Kingdom of Saudi Arabia shall refrain from publishing or accessing data containing some of the following:
  1. Anything contravening a fundamental principle or legislation, infringing the sanctity of Islam and its benevolent Shari'ah, or breaching public decency.
  2. Anything contrary to the state or its system.
  3. Reports or news damaging to the Saudi Arabian armed forces without the approval of the competent authorities.
  4. Publication of official state laws, agreements or statements before they are officially made public unless approved by the competent authorities.
  5. Anything damaging to the dignity of heads of state or heads of credited diplomatic missions in the Kingdom or harms relations with those countries.
  6. Any false information ascribed to state officials or those of private or public domestic institutions and bodies liable to cause them or their offices harm or damage their integrity.
  7. The propagation of subversive ideas or the disruption of public order or disputes among citizens.
  8. Anything liable to promote or incite crime or advocate violence against others in any shape or form.
  9. Any slanderous or libellous material against individuals.

- Furthermore, specific trade directives stipulate that all companies, organisations and individuals benefiting from the service shall observe the following:

1. Not to carry out any activity through the Internet, such as selling, advertising, or recruitment, except by the commercial licenses and registers in force.
2. Not to carry out any financial investment activity or offer shares for subscription except when in possession of the necessary licenses to do so.
3. Not to promote or sell medicines or foodstuff carrying any medicinal claims, or cosmetics, except those registered and approved by the Ministry of Health.
4. Not to advertise, promote, or sell substances covered by other international agreements to which the Kingdom is a party, except for those with the necessary licenses.
5. Not to advertise trade fairs or organise trade delegations visits or tourist tours or trade directories except with the necessary licences.

- All private and government departments, and individuals, setting up websites or publishing files or pages, shall observe and ensure the following:
  1. Respect commercial and information convention.
  2. Approval of government authorities for setting up websites or publishing files or pages for or about themselves.
  3. Approval of the Ministry of Information for setting up of media-type websites which publish news on regular basis, such as newspapers, magazines and books.
  4. Good taste in the design of websites and pages.
  5. Effective protection of data on websites and pages.
  6. All government and private bodies, and individuals shall take full responsibility for their websites and pages, and the information contained therein.

- The Resolution refers to a set of regulatory and technical procedures aimed at ensuring the safety of the constituents of the national network (the Internet inside the Kingdom) through effective programming and mechanical means. These include the following:
  1. Service providers shall determine Internet access eligibility through access accounts, user identification and effective passwords for the use of the access point or subsequent points and linking that through tracing and in-

vestigation programmes that record the time spent, addresses accessed or to which or through which access was attempted, and the size and type of files copied, whenever possible or necessary.

2. The use of anti-virus programmes and protection against concealing addresses or printing passwords and files.
3. Endeavour to avoid errors in applications that may provide loopholes that may be exploited for subversive activities or to obtain data not permitted for use for whatever reason.
4. Restriction of the provision of Internet services to the end-user through the Internet service unit at King Abdulaziz city for sciences and technology.
5. Keep a manual and electronic register with comprehensive information on end-users, their addresses, telephone numbers, purpose of use, and private Internet access accounts, and provide the authorities with a copy thereof, if necessary.
6. Not to publish any printed directories containing subscribers' and end-users' names and addresses without their agreement."

The Council of Ministers Resolution of February 2001 prioritises the protection of religion, tradition, and morality within Saudi Arabia's online sphere. This prioritisation is evident in the document's structure: The first section prohibits content deemed harmful to these values, followed by a subsequent section addressing content targeting the state and its institutions.

In October 2002, Saudi Arabia became the only country to outlaw cell phones with built-in cameras. This ban stemmed from concerns that men might misuse the technology to photograph women and share the images online without consent. Despite the official ban, authorities initially exhibited leniency towards these devices, with camera phones still found for sale in stores.

A turning point arrived in June 2002 following the arrest of three individuals (two Saudis and one Nigerian) accused of raping a young woman. The crime was reportedly filmed and transmitted via the cellular network. This incident prompted

a stricter enforcement of the ban. Authorities began confiscating camera phones at entry points like airports and prohibiting their use in specific locations like hospitals. However, the ban's effectiveness remained questionable. Camera phones continued to be available for purchase, with some reports suggesting a surge in sales due to fears of a complete sales ban (BBC News 2004a).

In July 2003, Saudi Arabia implemented stricter regulations governing Internet cafe operations within the Kingdom. This move aimed to enhance government oversight of Internet cafe users. Security bodies received instructions to enforce more stringent rules regarding monitoring user activity by cafe owners. The authorities also distributed a comprehensive list of regulations to all Internet cafes, mandating their strict adherence (Qusti 2003):

1. "Users must be informed of fines and possible imprisonment for those who violate these regulations.
2. Users under 18 are not allowed to access the Internet. Exceptions will be made for those accompanied by their guardians and for trainees and students in computer science. Those in charge of trainees and computer centres will be held fully responsible for any misuse of computers by those under 18.
3. Public places will be held fully responsible for any failure to identify a person who has violated these conditions or for any misuse of their equipment.
4. Users must be guided to use the Internet positively, which is consistent with Islamic teachings and government laws. They should avoid anything that infringes on the regulations for public Internet usage, which include Material that violates Islamic Shariah in principle or anything that abuses the sacredness of Islam and its teachings; material used to exchange information, either sending or receiving, that contradicts Islam or Saudi government laws; material that runs counter to public security; material that propagates destructive ideas or the spread of anything that might be a danger to public order or that might lead to disunity among citizens; material that advocates crime calls for it or stimulates it in any way as well as anything that supports an assault or attack on others in any form and material that involves the exploitation of individuals."

Newly implemented regulations in July 2003 significantly increased user identification and monitoring requirements for Internet cafes in Saudi Arabia. These regulations mandated that all customers provide their ID numbers and names upon entry. Additionally, cafe owners were required to document user connection and disconnection times, maintaining these records for six months and making them available to authorities upon request.

The stricter regulations stemmed from concerns about some Internet cafes' lax enforcement of existing rules. This concern was heightened following the May 2003 arrest of terror suspects during a raid on a Medina Internet Cafe. Authorities suspected the suspects used the Internet to communicate with other terrorists.

Saudi Arabia's Internet regulations saw further development in January 2008 when a new law on technology use was implemented. Defining "penalties of ten years in prison and a fine for Web site operators who advocate or support terrorism; three years and fine for financial fraud or invasion of privacy; and five years and a fine for those guilty of distributing pornography or other materials that violate public law, religious values and social standards of the kingdom. Accomplices of the guilty parties and even those proven to have only intended to engage in unlawful IT acts can receive up to half of maximum punishments" (OpenNet Initiative, n.d.-b).

Sudan – For several years, Sudan restricted Internet access. These restrictions likely stemmed from a combination of factors: general media limitations, a desire to control content deemed offensive to Islam, and, potentially, a lack of initial government interest in Internet development. However, local pressure eventually led to a policy shift towards Internet access. Despite this change, widespread Internet adoption remained hindered by the monopoly control of Sudatel, the sole communications company in Sudan (El Fatih El Tigani, n.d.; Balancing Act, n.d.)

Tunisia – Tunisia has a complex position regarding Internet censorship within the region. While often cited as one of the first countries to implement Internet restrictions, the details paint a more nuanced picture.

On the one hand, Tunisia possesses some of the most detailed and restrictive legislation governing online activity compared to its neighbours. This legislation, coupled with government oversight and website blocking practices, reflects a historical tendency to limit freedom of expression and individual rights, including access to the Internet.

However, it is essential to acknowledge the enforcement mechanisms. Tunisia uses a combination of legal frameworks, security forces monitoring, and website blocking to discourage access to government-deemed undesirable content. While arrests occur, they may not be as prevalent as the overall system suggests.

Tunisia established the Agence Tunisienne d'Internet (ATI) in 1996, tasked with developing the Internet and overseeing online activity. This dual role meant that the ATI also functioned as a form of "Cyber Police" that monitored Internet usage and users. All Internet communication in Tunisia was funnelled through the ATI, a semi-governmental body under the Ministry of Communications. This structure facilitated close government supervision and enforcement of Internet regulations.

Limited access to the Internet stemmed from two key factors: economics and strict regulations. High usage rates made Internet access expensive for many Tunisians. Additionally, registration requirements were demanding, including mandatory identity card deposits with the police, effectively discouraging widespread Internet adoption.

Tunisia stands out as one of the first countries in the region to implement Internet restrictions. It established a detailed legal framework governing online activity. Two key decrees published in March 1997 laid the foundation for regulating communication and Internet use within the country ("Journal Officiel de La République Tunisienne" 1997). Further regulations specifically targeting Internet cafes followed in December 1998 ("Journal Officiel de La République Tunisienne - N° 100" 1998).

ISP – The limited number of ISPs operating in the country restricted early Internet access in Tunisia. While the state-run Agence Tunisienne d'Internet (ATI)

provided Internet services to government bodies, only two private ISPs existed, reportedly owned by individuals with close ties to the president (Human Rights Watch, n.d.-a). The Tunisian government further restricted Internet access through legal limitations imposed on ISPs. The following section details these legal restrictions:

1. **Licensing and Oversight:** All ISPs in the country required a license from the Ministry of Communications. The licensing process involved scrutiny by a committee, which included representatives from the Ministries of Defense and Interior and communication and technology specialists. This structure ensured close government oversight during the ISP authorisation process.
2. **Content Responsibility:** Tunisian law mirrored the press code, holding ISP managers personally responsible for content hosted on their servers. This responsibility mirrored that of a traditional journal editor, imposing a significant burden on ISPs to ensure content adhered to vague notions of "public order and good morals".
3. **User and Website Owner Responsibility:** The legal framework extended accountability beyond ISPs. Internet users and website owners also faced potential repercussions for unlawful online activity.
4. **Monitoring and Reporting:** ISPs must provide the Agence Tunisienne d'Internet (ATI) monthly lists of all Internet subscribers. This practice facilitated extensive user monitoring by the government agency.
5. **Data Encryption Restrictions:** Encryption, a standard security practice, was heavily restricted. ISPs could only use encryption methods pre-approved by the Ministry of Communications, and even then, they were required to surrender decryption keys to the Ministry upon request. This regulation significantly weakened online privacy protections.
6. **User Instructions:** ISPs were required to prominently display user guidelines outlining potential legal consequences for violating Internet regulations. This requirement served as a constant reminder of the limitations placed on online activity.

Institutional users in early Tunisia faced additional limitations beyond general Internet regulations. These users must sign a restrictive agreement before receiving Internet access from the Agence Tunisienne d'Internet (ATI). This agreement significantly curtailed their online activities:

1. **Limited Use Cases:** Users were contractually bound to restrict their Internet usage to "scientific, technological, and commercial" purposes directly related to their field of operation. This definition effectively excluded many other potential uses of the Internet.
2. **Strict Reporting Requirements:** Institutional users must provide the ATI with detailed information about all Internet accounts created within their organisation. Additionally, they were prohibited from granting remote access to their networks without explicit ATI permission and had to report any changes in address, equipment, or user details. These requirements placed a significant administrative burden on institutions.
3. **Suspension and Monitoring:** The ATI reserved the right to suspend Internet access without notice for violating the agreement's terms. Furthermore, the agency could conduct on-site inspections to verify Internet regulations and compliance with equipment usage. This created a climate of uncertainty and fear of reprisal for institutional users.

Tunisia's approach to Internet regulation extended beyond technical limitations. By applying press laws to online activity, the government further restricted freedom of expression in the digital sphere. This approach, uncommon in the region at the time, effectively imposed a form of self-censorship on Internet users wary of potential legal repercussions.

Internet Café – Legislation enacted in October 1998 formally introduced Internet cafes, known locally as "Publinets," to Tunisia. This move marked a shift in government policy, paving the way for rapid growth in the sector. Over 200 Publinets opened within two years; by 2004, their number had reached 300 nationwide.

The government adopted a two-pronged approach to promote Publinet development:

- **Financial Incentives:** To encourage entrepreneurship, the government offered a grant covering 50 per cent of the investment for the first 100 Publinet establishments. The remaining investment could be financed over two years at a favourable interest rate. These financial incentives aimed to stimulate the growth of Internet cafes.
- **Limited Competition:** Despite private ownership, all Publinets were subject to regulations issued by the Ministry of Communications in December 1998. Notably, 70 per cent of private users connected to the Internet through Planet, an ISP reportedly owned by a president's relative. This potential conflict of interest raised concerns about limitations on genuine competition within the Publinet landscape ("Service d'assistance Aux Centres Publics d'Internet En Tunisie" 1998).

The Agence Tunisienne d'Internet (ATI) established a website, SOS Publinets (sos-publinet.tn), to assist Internet cafes in the country. However, a closer look reveals a focus on regulatory control.

A vital element of this control is a decree issued by the Ministry of Communications outlining specific regulations for Publinet operations. While the decree seemingly aims to establish operational standards, it also imposes limitations:

- **Physical Space Requirements:** The decree divides Publinets into categories and dictates minimum space requirements for each computer and cafe, along with a minimum number of waiting chairs. It also mandates accessibility features for disabled users and ventilation/air conditioning systems based on the cafe's category.
- **Limited Functionality:** The decree restricts Publinet computers by requiring them to lack disk drives. However, an exception allows one computer with a disk drive to receive technical assistance and printing, actions limited to staff control. This limitation potentially hindered users' ability to save or transfer files.

- **User Data Collection:** The decree mandates that Publinet managers maintain user databases to track Internet usage charges. However, this data collection raises privacy concerns, as authorities could request access to user information and browsing history.

While presented as guidelines, these regulations reveal a government intent to exert significant control over Internet cafe operations and potentially restrict user activity within these establishments.

Syria – Unlike other countries in the region, Syria initially lacked legal restrictions on Internet usage. However, Internet access itself was limited by factors beyond legal constraints.

- **State Monopoly on Infrastructure:** Syrian law mandated that only the state-owned Syrian Telecommunications Establishment (STE) could possess the technological infrastructure for Internet connectivity. This monopoly effectively limited the potential for widespread Internet access.
- **Technological and Economic Barriers:** Limited infrastructure and economic constraints further hindered Internet adoption beyond the initial restrictions placed by the STE monopoly.

The Syrian government's approach to technology adoption manifested in a cautious and controlled rollout of new services. This caution stemmed from concerns about "cultural infiltration" through external influences. Examples of this approach include (Zenklo 2003):

- **Restrictions on Fax Machines:** The use of fax machines was initially prohibited until the government developed technology to intercept messages without disrupting communication. This episode highlights the government's prioritisation of control over new communication technologies.
- **Delayed Email Access:** The Syrian government reportedly delayed the introduction of email services due to a lack of monitoring capabilities. This further exemplifies the government's desire to maintain control over communication channels.

Sudan – In a notable move for a nation with a strong Islamic tradition, Sudan adopted a "free Internet" policy in late 2002. This policy stood in contrast to the approach of many neighbouring countries and represented a commitment to open Internet access.

Early indications suggest a remarkable lack of censorship during this initial period. There were no reported instances of website blocking or content restrictions, including access to pornography, even from Internet cafes. This hands-off approach to Internet regulation stands out in the regional context (maykal 2003; El Fatih El Tigani, n.d.)

United Arab Emirates –

Providers – The UAE initially lacked specific legislation governing the Internet. However, existing regulations tempered this apparent openness.

- **Contradictions and Control:** The Telecommunications Act of 1996 enshrined freedom of expression across media outlets. However, these guarantees contradicted Law No. 1 of 1991, the Communications Law. This earlier law established the state-owned Emirates Telecommunications Corporation (Etisalat) as the sole ISP and granted it exclusive control over the nation's communications infrastructure. Additionally, the law stipulated that at least 60 per cent of Etisalat's shares must remain under government control. This emphasis on a state-run monopoly limited competition and potentially foreshadowed future restrictions on Internet access.
- **Early Enforcement Actions:** Despite lacking specific Internet regulations, the UAE was willing to enforce control measures. A case involving two individuals sentenced to prison and fined for making Internet calls using Voice over Internet Protocol (VoIP) technology highlights this point. This incident suggests the government's intent to regulate online communication methods beyond traditional phone networks (Reporters Without Borders, n.d.-a).

Content – Like its control over traditional media, the UAE implemented limitations on online content. Freedom of expression in the digital sphere was curtailed through a series of legal restrictions:

- **Censorship Criteria:** The law prohibited content deemed offensive to Islam, the government, or national security, potentially restricting public discourse on sensitive topics. Additionally, disclosing classified information, military data, or government agreements before official publication was forbidden.
- **Ministry of Information Oversight:** The Ministry of Information held significant control over media production. Printers and broadcasters required ministry licenses, and all published or broadcasted materials must be deposited with the Ministry.
- **Website Registration:** Mirroring a practice implemented in Bahrain, the UAE introduced website registration with the Ministry of Information in mid-1999. The government justified this requirement to prevent commercial counterfeiting and copyright infringement. However, an anonymous Ministry official in 1998 downplayed the regulation, claiming it was a formality to verify business legitimacy and not a means for content monitoring. The veracity of this claim remains unclear.

The UAE officially maintains a policy of censoring only pornography on the Internet. However, this stance appears to diverge from the observed practices. Reports indicate that a broader range of online content is subject to government oversight, including seemingly innocuous topics (Human Rights Watch 1999c):

- **Restricted Topics:** Examples of censored content include websites related to Buddhism, Girl Scouts, religious sects, dating services, and even health websites displaying uncovered body parts. This suggests a more expansive definition of inappropriate content than just pornography.
- **Political and Social Issues:** Despite claims from unnamed sources denying censorship of political, social, or economic content, the lack of transparency surrounding Internet restrictions makes it difficult to verify these assertions.

Websites with content critical of the government or addressing sensitive social or political issues might also be blocked.

Monitoring

Jordan – Evidence suggests that Jordan began monitoring online activity relatively early in its Internet adoption. As early as 1996, reports emerged of intelligence services summoning individuals for questioning about politically charged messages posted on forums or chat platforms. This suggests a keen government interest in controlling online discourse from the outset. The establishment of the Higher Media Council in December 2001 marked a further step towards online regulation. This body, tasked with overseeing media policy changes in the Kingdom, also assumed responsibility for monitoring online behaviour. Their activities included observing Internet service provider and questioning their owners about access to prohibited websites. This development solidified a system of government oversight over Jordan's early Internet landscape (Privacy International and the GreenNet Educational Trust 2003).

Tunisia – The government tightly controlled early Internet access in Jordan. Public access points primarily existed in state-owned Internet cafes, known as "Publinets". These cafes operated under close supervision (Reporters Without Borders 2004b; MacFarquhar 2004):

- **Managerial and Governmental Oversight:** Publinet managers were tasked with monitoring customer Internet usage alongside broader oversight from the Ministries of Communications, the Interior, and the police. This multi-layered approach ensured high government control over online activity within these cafes.
- **Spyware Monitoring:** The government further tightened its grip by installing spyware on cafe computers. This software, controlled by the Ministry of Communications, allowed real-time user activity monitoring.

The government's focus on monitoring extended beyond Internet cafes.

- **Prioritization of Controllable Communication:** Jordan reportedly prioritised the development of private communication methods, likely due to their perceived ease of monitoring compared to open Internet access. This policy decision arguably contributed to a decline in Publinets nationwide, dropping to around 260.
- **Cyber-Police and Website Blocking:** In 2002, the Jordanian government established a "Cyber-Police" unit dedicated to Internet control. This unit's activities included blocking access to specific websites, monitoring attempts to access blocked sites, taking down servers, and even arresting Internet users deemed to be in violation.
- **Alleged Targeting of Human Rights Groups:** Furthermore, there have been claims that the Jordanian authorities deployed viruses to attack the email systems of human rights organisations operating within the country.

Technical Limitations

Speed Limitations

Iran – In the lead-up to the December 2006 local council elections in Iran, the government implemented significant restrictions on Internet usage, including drastic reductions in Internet speed. This action effectively transformed the Internet from a versatile communication tool capable of sharing audio, video, and images into a limited and text-based platform. This throttling significantly hampered the Internet's potential and rolled back its functionality by several years.

The timing of these restrictions suggests a deliberate attempt to manipulate the political landscape. The announcement of Internet speed limitations at the end of October 2006, just weeks before the elections, raises concerns about the government's motives. Two potential objectives can be identified:

- **Limiting Exposure to Western Media:** By throttling Internet speeds, the government may have aimed to restrict access to Western audio and video content, potentially seen as a source of influence for reformist movements.
- **Hobbling Reformist Communication:** Slower Internet speeds could have significantly hampered reformist parties' online dissemination of their messages and publications, potentially hindering their campaign efforts.

Accessibility

Syria – Government control extended beyond Internet access in Iran. The availability of personal computers themselves was also restricted. Reports in 2003 suggested that despite approximately 300 personal computers in the country, the vast majority belonged to government institutions. This limited access to personal computers likely served as another tool to restrict individual user freedom and Internet adoption in Iran (The Arabic Network for Human Rights Information, n.d.-e). Syrian users reported encountering various restrictions. Attempts to access blocked websites sometimes resulted in the inability to type in Arabic or English. Additionally, the filtering system reportedly prevented users from accessing websites containing the word "search" on specific domains. While demonstrating the extent of government control, these measures also highlight the technical limitations of early filtering systems, which often produced unintended consequences (Al'ustuani 2005).

Software

Iraq – In February 2009, Iraq's Ministry of Communications announced a collaborative effort with a French company to implement an Internet security system for the nation's network. The Minister stated that the new system "it will be possible to monitor the Internet and to block access to specific online content, especially if there is a concern over national security information or information related to public morals" (OpenNet Initiative 2009b).

Iran – Iran employed website filtering to control access to online content. However, the exact source of the filtering technology remains unclear.

- **Domestic Products** - Alireza Manafi, director of the Information Technology Laboratory at the Informatics Research Center, highlighted the capabilities of a domestically developed filtering software called "Delta Global". This software boasted features like identifying unauthorised Persian and foreign websites, optimising review algorithms based on user feedback, and performing rapid website scans. Manafi also reported that Delta Global identified 572 prohibited websites out of 6,500 analysed in domestic Internet traffic. This made Iran the only country, apart from China, that blocks the Internet extensively using domestic technology. This suggests that filtering may not have been as extensive as in other countries like China (Iranian Students' News Agency 2004).
- **Foreign Products -**
  - SmartFilter: In 2005, reports emerged that Iran utilised SmartFilter, software produced by an American company, for website blocking. However, the CEO of SmartFilter publicly denied selling the software to Iran, casting doubt on these claims. (OpenNet Initiative, n.d.-a)
  - Nokia Siemens Networks (NSN): Reports indicate that NSN installed a communication system in Iran that year, allegedly granting the government the ability to monitor users' cellular and online activity. This development raised concerns about government surveillance capabilities. These concerns were seemingly corroborated by accounts from arrested individuals who reported being confronted by authorities with details of their phone conversations and text messages during interrogations. This suggests the potential use of the monitoring system to target specific users. A study around the same period revealed a significant drop in Internet traffic entering and leaving Iran following the 2008 presidential elections. This 50 per cent reduction suggests a deliberate government intervention to throttle Internet traffic. The study further indicates that this throttling may have been selective, targeting specific applications rather than completely severing Internet access (Kamali Dehghan 2010).

Saudi Arabia – From the outset of Internet access in Saudi Arabia, the government exercised significant control over online content. Even the initial Internet connection established in the Kingdom routed traffic through an American company that filtered content before it reached Saudi Arabia. This practice ensured government oversight from the very beginning (Privacy International and the GreenNet Educational Trust 2003). Website blocking relied on American-made SmartFilter software, like Iran's and other regional countries' approaches. A dedicated team within Saudi Arabia maintained a list of prohibited websites alongside updates provided by SmartFilter's supplier (Internet Services Unit 2006). The government invested heavily in state-of-the-art surveillance equipment from Germany and the Netherlands. These systems boasted capabilities like website blocking, user activity monitoring, and email tracking.

Arrests

Bahrain – The Internet's early days in Bahrain witnessed government crackdowns on online activity. These cases highlight the potential risks associated with online dissent.

- **1997: Engineer Arrested for Online News Transmission:** In 1997, an engineer working for the local telecommunications company Batelco faced arrest. The charges against him stemmed from transmitting news via the Internet to the opposition group "Bahrain Freedom Movement". However, the authorities eventually released him without charges after two years of detention (Human Rights Watch 1999; Human Rights Watch 1999a).
- **2005: Forum Managers Detained for Alleged Emir Insult:** Another incident occurred in 2005 when the administrators of the online forum "Barhainonline.org" were arrested. The government accused them of "insulting the Emir". They refused to pay a fine in exchange for release but were freed two weeks later (Reporters Without Borders 2005h).

Egypt – Egypt's approach to Internet regulation has been characterised by close government control and monitoring. This approach has led to its inclusion on Re-

porters Without Borders' "Internet Enemy" list throughout the analysed period. Several factors contributed to this designation:

- **Content Monitoring and User Surveillance:** The Egyptian government implemented measures to monitor Internet content and user activity within its borders. This fostered an environment of online censorship and limited free expression.
- **Early Website Registration:** Egyptian authorities mandated the early registration of all domestic websites. This requirement likely served as a tool to identify and potentially control online content.
- **Crackdown on Sensitive Topics (2001-2002):** In 2001, Egyptian authorities warned Internet users, explicitly discouraging them from engaging with sensitive topics online. These topics included Coptic-Muslim relations, content linked to terrorist organisations, discussions of human rights violations, criticism of the government, and advocacy for modern interpretations of Islam (Reporters Without Borders 2008a).
- **Arrests of Homosexuals (2001-2003):** Coinciding with the online restrictions, Egyptian authorities conducted a large-scale arrest of homosexual individuals between 2001 and 2003. Estimates suggest the number arrested ranged from several dozen to several hundred. These arrests stemmed from online activity, with authorities reportedly using a bait advertisement to target individuals. Homosexuality is illegal in Egypt, and convictions can result in up to five years in prison (Sodomylaws.org 2007; Human Rights Watch 2003).
- **Establishment of Internet Monitoring Unit (2002):** The government further tightened its grip on online activity in September 2002 by establishing the "Computer and Internet Crime-fighting Unit". This unit's activities included real-time monitoring of Internet traffic, with a reported focus on identifying users visiting pornography websites. This focus was possible because Egypt's ISPs connect through a government-controlled communications company. The unit's first publicised case involved the arrest of a man who allegedly attacked a government official and his family on a website he created.

- **Arrests and Acquittal of Activists (2003):** A case involving five members of the "Revolutionary Socialist" group in April 2003 demonstrates the limitations of government control. These activists were arrested for using the Internet to publish information about human rights violations, particularly against Coptic Christians. The government accused them of attempting to undermine the state and disseminating "false news". However, the accused were ultimately acquitted in March 2004, highlighting the challenges for authorities in suppressing Internet-based activism, especially when evidence is easily accessible online (Human Rights Watch 2005a).

The 2008 report by Reporters Without Borders provided further evidence of press freedom violations in Egypt, particularly during 2007. The report documented the use of fatwas against journalists, a tactic likely intended to silence regime critics. It also detailed the prosecution of a dozen journalists and President Hosni Mubarak's passage of controversial constitutional amendments, seen by some as a threat to media freedom.

Jordan – Despite its reputation as one of the most liberal countries regarding Internet access, Jordan witnessed a press freedom controversy in 2002. Toujan el-Faisal, a television journalist and former sole female member of parliament, faced arrest in May 2002. The charges stemmed from an open letter she published on the news website Arab Times (arabtimes.com) in March of that year. In the letter, she accused the Prime Minister of corruption, an act deemed harmful to "the integrity of the state and its honour" by Jordanian authorities. Sentenced to the maximum penalty of 18 months in prison, el-Faisal went on a hunger strike that lasted 29 days. In June, King Abdullah II granted her a pardon, ending the ordeal (Reporters Without Borders 2002b; 2002a).

Morocco – In December 2009, Moroccan authorities cracked down on online dissent. A blogger faced trial for "spreading false information that harmed the image of the kingdom on the issue of human rights," according to the charges. The accusations stemmed from photos, information, and a statement the blogger pub-

lished regarding police raids during student demonstrations. Additionally, the Internet cafe owner who provided the blogger with a platform was sentenced to up to a year in prison on similar charges, including the accusation of offering a platform for activities that oppose the government ("Un Blogueur et Un Propriétaire de Café Internet Condamnés à de La Prison Ferme" 2009).

Iran – An analysis of Iranian Internet user arrests reveals several vital patterns:

- **Focus on Reformist Voices and Bloggers:** Beyond large-scale arrests, Iranian authorities targeted two main groups: journalists publishing content on reformist websites and editors/bloggers (both men and women) posting on their blogs. Notably, Iran often arrested the writers and technical staff operating these websites, seemingly avoiding action against the political leaders potentially backing these outlets. Iranian authorities exhibited sensitivity towards blogs, especially those created by Iranian users (Reporters Without Borders 2004a).
- **Sensitivity to Cultural and Moral Issues:** The government's heightened sensitivity to cultural and moral issues is evident in the arrest of approximately seventy young people on March 3, 2003. These individuals met through an unauthorised dating website, leading to speculation in Iranian newspapers that authorities may have been monitoring online chat rooms (Sedarat 2003).
- **Arrests Spiked Around Elections:** The Iranian government displayed a heightened focus on Internet activity during political change, particularly elections. Most arrests occurred between September and October 2005, eight months after the parliamentary elections and eight months before the presidential election. Following the June 2005 presidential election, no arrests were reported until the end of the analysed period. This pattern is further illustrated by the arrests of bloggers leading up to and around the February 2004 elections (E. McLaughlin 2003). A second wave of arrests began in May 2004 (after the February parliamentary elections), targeting a blogger who wrote for a reformist newspaper shut down by the authorities (Reporters Without Borders 2005c). This wave continued until a few months before the June 2005 presidential elec-

tion. A similar pattern emerged in early 2009, with another wave of arrests coinciding with various Internet restrictions implemented roughly a year before the June 2009 presidential election. Bloggers and online journalists were often sentenced to imprisonment for several years during these periods.

- **Reported Harsh Conditions and Torture:** Reports suggest that most detainees endured harsh prison conditions and torture despite being released after a few weeks or months (Human Rights Watch 2005b).

Libya – In January 2005, Libyan authorities arrested an Internet journalist for publishing critical articles about Libyan society and government on the British website Akhbar-libya.com. The journalist reportedly authored around 50 articles throughout the previous year (Reporters Without Borders 2005b).

Saudi Arabia – In early August 2004, a landmark case emerged in Saudi Arabia. Three Internet users belonging to the Ismaili Shiite sect were sentenced to two years in prison and 750 lashes each. The charges stemmed from their "participation in forums that harm security and the homeland," according to Saudi authorities. This case marked the first instance in Saudi Arabia where individuals were arrested and tried solely for their online activity. No further documented arrests of Internet users or journalists were found within the kingdom during the analysed period (Alshaqa'i 2002).

Syria – Syrian authorities implemented a series of crackdowns on online activity between 2002 and 2004, targeting users who expressed dissent or shared information deemed sensitive.

- **Mass Arrests and Harsh Sentences (2002-2004):** In September-October 2002, four Internet users were arrested by Syrian authorities. Three of them were later sentenced in July 2004 to prison terms ranging from two to four years. The charges included "spreading false information online," possessing classified information, sharing information with a foreign country, and publishing content without approval that could potentially damage Syria's relations with another nation (Reporters Without Borders 2004g).

- **E-mail with Banned Website Content (2003-2004):** In February 2003, another Internet user faced arrest for sending an email containing content from the banned website thisissyria.net. He was sentenced in June 2004 to two and a half years in prison on charges of "publishing lies" online that "damaged the image and national security" of Syria (BBC News 2004b).
- **Kurdish Journalist Targeted (2003-2005):** In July 2003, a 29-year-old Kurdish journalism student was arrested after posting pictures of a Kurdish demonstration on a German website focused on Kurdish culture (amude.net). While he claimed the website had 5,000 daily visitors, authorities accused him of belonging to an "illegal organisation" and sentenced him to three years in prison in October 2004. Paradoxically, he was awarded the "Cyberdissident" prize by Reporters Without Borders in December 2005 (Reporters Without Borders 2006).
- **Journalist Detained and Released (2004):** A local journalist was briefly detained in November 2004 for 33 days without charges being filed. He believed his arrest stemmed from creating a political forum (liberalsyria.com) and his critical articles tackling corruption and religious extremism, as well as advocating for democratisation and freedom of expression (Reporters Without Borders 2004d).

Tunisia – Beyond website blocking and Internet monitoring, Tunisian authorities employed a systematic strategy to discourage online dissent. This strategy included:

- **Arrests:** Tunisian authorities targeted journalists and Internet users who published online content critical of the president or human rights abuses, such as the torture of political prisoners. These individuals faced arrest because of their online activity.
- **Harassment:** Beyond arrests, journalists and Internet users who were critical of the government were harassed. This likely aimed to silence potential critics and instil fear in others considering online activism (Reporters Without Borders 2004f; 2005a; 2003).

Economic Restrictions

Egypt – Government policies in Egypt hindered widespread Internet access. One example involved penalties imposed on ADSL companies that offered discounted Internet service. High Internet access prices effectively restricted usage to a wealthier population segment. This approach limited affordability and prevented the broader public from joining the online community (IFEX 2008).

Jordan – In the late 1990s, Jordan's approach to Internet access created a barrier to widespread adoption. This resulted from a combination of factors:

- **High Call Rates Dictated by Government:** Private ISPs were subject to high call rates set by the state-owned telecommunications company. This inflated the final cost for consumers, making basic Internet browsing expensive compared to the relatively inexpensive cost of email.
- **Limited Affordability for Average Citizens:** In the late 1990s, the combined cost of Internet access and phone charges placed Internet use beyond the reach of the average Jordanian citizen. At the beginning of 1999, an average Internet subscription, including phone charges, could reach around USD 70.
- **State Monopoly on Communication Lines:** Despite multiple ISPs, the state-owned telecommunications company maintained a monopoly on communication lines, hindering efforts to lower prices.

This combination of factors effectively created a form of economic censorship in Jordan. While email remained relatively affordable, full Internet access was a luxury for many citizens (Human Rights Watch, n.d.-b; Dahan, n.d.)

Qatar – A wave of discontent concerning Internet access emerged in Qatar. Many citizens expressed anger toward the 15-year monopoly granted to the Qatari Telecommunication Company (QTC) as the sole ISP. This frustration stemmed from the perception that the QTC had unrestricted control over Internet pricing.

In response to these concerns, several Qatari business ventures expressed interest in offering Internet services within the country. This local competition aimed to challenge the QTC's pricing structure.

Meanwhile, the QTC defended its practices by citing the Gulf States' relatively small user base. The company argued that Internet service costs would naturally decrease as users increased (The Arabic Network for Human Rights Information, n.d.-d).

Syria – Syrian authorities implemented a combination of economic restrictions that limited early widespread Internet access in the country (The Arabic Network for Human Rights Information, n.d.-e).

- **Prohibitive Initial Costs (1998):** The costs were extremely high in 1998, just one year after Internet access arrived in Syria. These included a USD 40 monthly fee, a USD 2 per-hour usage charge, and a USD 100 one-time installation cost. To encourage adoption, the government reduced the monthly fee by 5 per cent in July of that year, but other charges remained unchanged.
- **Limited Internet Cafes and High Usage Rates (1998-2000):** Despite the high costs, Internet cafe usage rates in Damascus remained high compared to other countries. However, state-licensed cafes were reportedly intended for foreigners due to their high per-minute charges (11 cents) and potentially due to the cafes' ownership structures. Owning a personal computer with Internet access was also impractical for most Syrians due to the high cost of equipment.
- **Unaffordable Packages for Home Users (2001-2003):** Even by the end of 2001, four years after Internet access, a 12-hour monthly package cost a staggering USD 80, with additional hours at USD 2.4 each. In a country where the average monthly salary was around USD 120, Internet access was far out of reach for most citizens. Limited affordability kept the number of Internet users to a mere 7,000 out of a population of 17 million in 2001.
- **Modest Price Reduction (2003):** Some price reductions were implemented by the end of 2003, bringing the Internet access cost down to USD 1 per hour.

However, this price remained high, considering the average Syrian's monthly income of USD 110.

Tunisia – Tunisia utilised economic measures to restrict widespread Internet access. Initially, authorities set high prices, discouraging many citizens from subscribing to or using the Internet regularly. To address this issue, a series of price reductions were implemented:

- **May 1998**: Internet usage costs were cut in half.
- **March 1999**: A further 30 per cent reduction in usage costs occurred.
- **January 2001**: Another 30 per cent decrease in usage costs was implemented.

High storage costs also presented a significant barrier. Due to these prohibitive storage fees, setting up a website within the country proved excessively complex and, for some, practically impossible.

Pro-Blocking Discourse

This policy of website blocking received the endorsement of the state leadership. The approach also found support among various countries throughout the Middle East:

Iran – Iranian authorities implemented a website blocking policy targeting content deemed immoral or politically critical:

- **Ministerial Request for Blocking (May 2003):** In May 2003, Iranian ministers called for blocking access to "immoral sites" and political websites critical of the country's religious and political figures (BBC News 2003).
- **President Confirms Blocking (December 2003):** In 2003, President Mohammad Khatami acknowledged blocking 40 websites containing "pornographic and immoral" content (Scullion 2003c).

Deputy Minister Details Policy (May 2004): In May 2004, Deputy Minister of Communications Masoud Dawari-Najed elaborated on the blocking policy. He specified that access was restricted to "immoral websites and political web-

sites that harm the country's political and religious leaders". Dawari-Najed added that users attempting to access blocked sites would receive a warning message citing an order from the Ministry of Posts and Communications (Reporters Without Borders 2004a).

- **Attorney General Calls for Continued Cooperation (January 2005):** In January 2005, Tehran's Attorney General, Said Mortazavi, met with Ministry of Communication officials. During the meeting, Mortazavi emphasised the need for continued collaboration between the two ministries to maintain website filtering and called for further discussions on this topic (Stop Censoring Us 2005c).

Saudi Arabia – Saudi Arabian authorities defended their website-blocking practices by emphasising the protection of religious and social values (Jehl 1999; Whitaker 2000).

- **Focus on Immoral and Anti-Social Content (1999):** In early 1999, Abdullah Al-Rashid, deputy director of the King Abdulaziz City for Science and Technology (KACST), took a clear stance on Internet censorship in the kingdom. He asserted that only websites deemed offensive to religion or society were blocked.
- **Technology for Value Protection Cited as Delay Reason (May 2000):** The KACST director later clarified the rationale behind the delayed introduction of Internet access in Saudi Arabia. He explained that authorities awaited the development of technology capable of preventing access to "materials that may corrupt or harm our Muslim values, tradition and culture".
- **Government Official Emphasized Social and Religious Protection:** The director of the governmental body overseeing the Internet offered similar justifications. This official countered the claim that website filtering targeted politically sensitive content. Instead, he framed it as a measure to protect local users' social and religious traditions while accessing the Internet.

Syria – In a 2002 interview, the Syrian Minister of Communications outlined plans to reduce the cost of computers and Internet connections and improve Internet

speed. However, these efforts towards affordability came with a caveat. The Minister emphasised that the government would maintain control over the internet, including restricting access to certain websites deemed incompatible with the "tradition and customs of the country".

The Syrian Computer Society (SCS) executive presented a contrasting view on Internet access for Syrian residents. He advocated for unrestricted access, including email. However, he acknowledged the government's right to restrict access to "immoral websites". Recognising the limitations of government control, he suggested a more nuanced approach. Instead of blocking all problematic websites, he proposed an initiative to raise awareness among young people about these sites. Therefore, the organisation will encourage a policy of expanding awareness of these sites among young people rather than blocking them in the future and mentioning that "**The motto of the SCS** now is **'Internet for everybody' in Syria**" (Emphasis in the original). In addition, the senior official concluded his remarks with the following sentence: "I believe all Syrians under the new plan would have free access to all electronic mail sites" (SyriaLive.net 2002; Jayoush 2000).

Arab governments exhibited varying degrees of openness towards the Internet. While some citizens relied on the Internet as a platform for independent information and expression, many countries implemented various measures to restrict Internet access and control its usage. These measures aimed to limit the spread of information deemed unfavourable to the regime.

Control Mechanisms:

- **Legal Restrictions:** Legislation and regulations were enacted to restrict the activities of ISPs, users, and website owners.
- **Monitoring of Use:** Authorities monitored Internet use in Internet cafes and among private and institutional users.
- **Economic Barriers:** High Internet access costs were established, effectively excluding a significant portion of the population.

- **Website Blocking and Filtering:** Websites considered misaligned with the government's ideology, expressing dissent, or violating moral values were blocked or filtered.
- **Suppression of Online Activity:** Users and individuals who published content deemed problematic by the authorities were arrested.

Part D – The Countermeasures

The Internet's arrival in the Arab world undeniably transformed the daily lives of its users. It fostered new connections while strengthening existing ones, enhanced computer and English language skills, and created new avenues for diverse business opportunities. Furthermore, it provided a platform for anonymous expression on various issues.

This digital revolution spurred the development of a sophisticated Internet culture in the Middle East. This culture, however, thrived "underground," employing creative methods to circumvent government restrictions on Internet access and content.

Over time, various actors emerged to challenge these limitations. A concerted effort arose from individuals and entrepreneurs seeking to bypass technical restrictions on Internet use. Entrepreneurs, in particular, pushed boundaries in their endeavours to expand the possibilities of the Internet within the Middle East.

Circumventions

Arab governments actively censored and blocked websites deemed objectionable. In response, users, particularly those with technical expertise, consistently and successfully developed methods to circumvent these restrictions and achieve unrestricted Internet access (Kettmann 2001b).

It is essential to understand that websites often record user data such as IP address, operating system, browser type, and the referring website. Bypassing these tracking mechanisms is a crucial strategy for achieving anonymity online and overcoming Internet filters and blocks. Users and organisations may resort to Internet bypassing for various reasons. The primary goals are typically to maintain online anonymity or bypass censorship filters. However, organisations and entities may also employ indirect methods for other objectives, utilising a wide range of tools (Kettmann 2001b):

Technology

Bypass sites – Responding to government censorship, Arab users adopted various techniques to access blocked websites. One standard method involved proxy servers. Proxy servers act as intermediaries between users and the websites they wish to visit. By routing requests through a proxy server, users could mask their IP address and circumvent website blocking imposed by their governments. ("How to Disable Your Blocking Software," n.d.)

- **Anonymizer**: a popular proxy service offering free and paid anonymous browsing options. The free service allowed users to enter the desired website address and access it indirectly through Anonymizer's servers, effectively disguising the user's true destination from censorship software. The paid services provided additional features for enhanced privacy protection. In August 2003, Anonymizer partnered with the US government's International Broadcasting Bureau (IBB) to launch a service designed to help Iranian citizens bypass Internet filtering within their country. This initiative, the IBB Anonymizer, offered another potential tool for users seeking to circumvent government censorship ("Unintended Risks and Consequences of Circumvention Technologies: The IBB's Anonymizer Service in Iran" 2004; Poulsen 2003).

  Several other websites employed similar methods to offer anonymous browsing services. These additional options provided users with various choices for bypassing censorship restrictions. Several websites offered free and paid anonymous browsing services:
- **Anonymouse.org:** This service claimed to have been operational since 1997.
- **Megaproxy.com:** Like many others, Megaproxy.com provided a free basic service alongside more extensive paid options for anonymous browsing**.**
- **Safeweb.com:** Symantec Corporation acquired Safeweb.com in October 2003, which also offered anonymous browsing capabilities (Captain 2001).

Additional services addressed specific user needs:

- **StupidCensorship.com:** This website maintained a mailing list to inform users about new bypass sites and alert them when governments blocked existing ones. StupidCensorship.com also provided information about accessing censored websites.
- **Unipeak.com:** Unipeak.com offered a multi-purpose service that filtered unwanted advertisements, masked user IP addresses, prevented online activity tracking, and established secure connections to non-secure websites.
- **Riseup.net:** While Riseup.net offered a more comprehensive range of tools, one key feature was its secure and encrypted private email account service.

Bypass Software – In response to government censorship, Arab users adopted various software tools to access blocked websites.

- **CiviSec –** The University of Toronto's Citizen Lab developed CiviSec to enable anonymous Internet browsing. This software was designed to provide secure and private communication for at-risk individuals, such as human rights activists residing in countries with restricted online communication (nart 2006).
- Peacfire – Peacfire offered a unique method for bypassing website blocking. Instead of installing software on the censored computer, Peacfire software was installed on a machine with unrestricted Internet access. This software then generated a new unblockable web address (URL) that could be used on the censored computer to access the desired website. The developers claimed effectiveness against known blocking software and even country-wide Internet filtering systems like those in China (Haselton, n.d.)
- Psiphon – Another Citizen Lab project, Psiphon, was bypass software designed for individual users. Installed on a personal computer with unrestricted Internet access, Psiphon allowed users to bypass censorship restrictions in their location ("Psiphon," n.d.; "Talk: Psiphon/Archive 1," n.d.)
- Six/Four System – This software uses encryption to create a secure and anonymous communication channel between two computers. Users could leverage

Six/Four to access websites blocked by firewalls within their network (SourceForge.net, n.d.).

- Tor – This software created a secure and anonymous communication channel between two computers using encryption. Users could leverage Six/Four to access websites blocked by firewalls within their network.

Reports suggested that some users purchased software designed to bypass these restrictions, often for as little as one dollar. Alternatively, other users turned to freely available tools, leveraging international email service providers like Hotmail and Yahoo or employing different techniques to evade censorship measures (The Arabic Network for Human Rights Information, n.d.-e).

Email Services – Faced with restrictions on personal email accounts, Arab users adopted web-based email services to maintain communication channels. Unlike traditional email clients, these services allowed users to send and receive emails from any location, regardless of whether local authorities blocked their primary accounts. This flexibility proved critical for users seeking to circumvent censorship efforts. Popular web-based email services included regional providers like http://mail.arabchat.org and international platforms like Google's Gmail.

Foreign Internet providers – Limited Internet access in Syria and Saudi Arabia prompted users to explore alternative connection methods.

- **Syria:** With Internet restrictions, Syrian users have adopted various strategies to access blocked content—one method involved connecting through neighbouring countries, with Lebanon being a popular choice due to its proximity. However, limited international telephone lines in Damascus hampered this approach for some users in the capital city.

  Reports from June 2000 suggested that an Internet cafe in Damascus offered access to websites blocked by the authorities, including Israeli websites and tools for anonymous browsing. This anomaly likely arose because the cafe catered to foreign residents, who may have benefited from less restricted Internet access than Syrian citizens.

- **Saudi Arabia:** Before formalising Internet service regulations in Saudi Arabia, many residents sought alternative connection methods, driven by the high costs associated with official channels. These users resorted to expensive international dial-up connections with ISPs in neighbouring countries like Bahrain. Large foreign companies operating in Saudi Arabia also played a role. Before public access was authorised, they offered free Internet access to Saudi businesses. A 2004 report by the OpenNet Initiative suggests that unregulated Internet access through satellite connections emerged as a potential alternative in Saudi Arabia. If such connections existed, they likely operated outside the purview of government regulations (Human Rights Watch 1996; Reporters Without Borders 2004c; Miller 2004; OpenNet Initiative 2004b).

Automatic addresses for websites – in response to website blocking measures, the Saudi opposition organisation MIRA implemented a creative strategy to ensure user access to its publications. MIRA distributed unblockable website addresses to users through automated emails. These addresses were reportedly generated dynamically, allowing the organisation to create infinite access points. This dynamic generation bypassed static blocking methods employed by censors.

Syria: There is evidence from June 2000 about the ability to reach various websites from an Internet cafe in Damascus (including Israeli websites and websites for anonymous Internet use), which were supposed to be blocked by the authorities, but this is apparently because the place is out of reach of the country's residents and that it serves foreign residents.

Cache – Faced with Internet censorship in Saudi Arabia, users adopted various strategies to access blocked content. One method involved leveraging the search engine cache. By searching for the desired website on Google, users could potentially access cached versions of the site's pages stored by the search engine. Unlike the live website, these cached pages often bypassed blocking measures and even included links to other unblocked content.

Knowledge

Guides – websites and online articles that explain workarounds; some are technical and intended for those with extensive knowledge in the field. There is also a discussion of the considerations for choosing the bypass means (nart 2004; Greene 2001; "Everyone's Guide to By-Passing Internet Censorship for Citizens Worldwide" 2007; "Bypassing Restrictive Proxies" 2002). Some guides offered technical explanations for advanced users, while others provided more general information.

Specific recommendations for proxy websites offering censorship avoidance were also available. For instance, resources like "Waynes Proxy Censorship Avoidance Site" offered options for users in the UAE, Saudi Arabia, Kuwait, China, and Singapore (Wayne, n.d.)

Additionally, resources catered to users seeking anonymous online activity. The guides explain methods for anonymous surfing and even provide details onow to set up anonymous blogs ("How to Blog Safely (About Work or Anything Else)" 2005; Zuckerman 2005). Reporters Without Borders published a comprehensive "Handbook for Bloggers and Cyber-Dissidents" in 2005, offering a range of strategies for online access, audience building, filtering bypass, and security maintenance (Pain et al. 2005). Some resources focused on specific countries, like a technical article that provided detailed instructions for accessing blocked websites in Iran (Persian Journal 2005a).

References – These references, likely in the form of websites or online resources, functioned as bibliographies for tools to bypass and prevent Internet filtering and blocking mechanisms. They served as valuable resources for users seeking to circumvent censorship measures ("ProxyTools Download," n.d.; "EPIC Online Guide to Practical Privacy Tools," n.d.).

Personal knowledge – Despite government efforts to restrict Internet access, users with technical expertise found ways to circumvent these limitations. Even senior officials in Saudi Arabia acknowledged the challenges of blocking access

for such users. Evidence from 1997 suggested that young people across the Arab world were already adept at bypassing Internet censorship measures implemented by their governments (McCullagh 1997). These workarounds likely contributed to the Saudi officials' admission of difficulty completely restricting access for technically savvy users (Palfrey 2005).

Reports also indicated a market for circumventing Internet filters in Saudi Arabia. Users could reportedly pay computer experts to access blocked websites, with prices ranging from 26 USD to 67 per website.

Similarly to users in other countries, Syrians also employed bypass software programs to circumvent restrictions. Additionally, some reports suggested that tech-savvy users found workarounds for Internet filters implemented by ISPs. These users reportedly leveraged online resources such as professional forums to acquire the knowledge needed to bypass restrictions.

United Arab Emirates – Despite state efforts to enforce Internet filtering systems implemented in the late 1990s, government officials acknowledged the relative ease with which these restrictions could be bypassed. The effectiveness of the filtering system hinged on the specific proxy server a user accessed, as filtering occurred at this level. This vulnerability was highlighted in November 2003 when the America Online (AOL) website was blocked due to an advertisement promoting methods to circumvent the filtering system.

Public Discourse

Opinions regarding the Internet's influence on everyday life varied across the Arab world. Proponents highlighted the Internet's potential for positive societal impacts, mainly when utilised for religious education, national identity reinforcement, and social cohesion. However, concerns also emerged about the Internet's potential downsides in its unfiltered state. Critics argued that the Internet fostered unproductive activities like online gaming, racial discrimination, and cultural elitism. Additionally, they expressed anxieties about the potential for the In-

ternet to undermine religious authority and sow discord through sectarian online debates (Fuaad, n.d.).

Government efforts to limit Internet access and control content faced opposition from various voices within the Arab world. Critics argued against government control, citing the Internet's potential to promote freedom of information and knowledge sharing, even if it contained inappropriate content. Proponents of open access believed that restrictions could be implemented without government intervention, suggesting methods like password protection, specialised filtering software, and parental guidance (Rashid 2004). Human rights organisations emerged as vocal critics of Internet restrictions in the Arab world. While these groups opposed the spread of pornography online, their primary concern centred on the potential for political censorship. They argued that political control rather than religious or moral concerns often motivated government restrictions. This perspective suggests that governments limited Internet access to suppress dissent and restrict the flow of information (Karoui 2002).

Government efforts to restrict Internet access in the MENA region triggered public frustration and unrest. This discontent manifested in demonstrations by Internet users across several countries, including IranScullion (n 201). and Syria ('iislam 'uwn layin 2003). Even within countries known for stricter content control, calls for reform emerged. For instance, the Information and Culture Minister in the UAE publicly advocated against government censorship, arguing for individual freedom of access (vigilant tv 2002).

Bahrain – In May 2002, protests erupted in Bahrain in response to government Internet censorship. A group of 20 demonstrators gathered outside the offices of Batelco, a communications company, to denounce the blocking of several news websites. They argued that these restrictions violated the fundamental right to freedom of expression in Bahrain and called for the dismissal of the Minister of Information (BBC News 2002a). Another instance of public opposition involved a member of parliament, Muhammad Al-Khiyat. On April 31, 2002, he sent a formal

letter to the Minister of Information, copied to the Minister of the Interior and the Minister of Communications. The letter demanded an explanation for blocking a forum website (jiddafs.org/vb) that had hosted a review of his parliamentary activity.

Egypt – In 2004, Egyptian authorities took a significant step by blocking three official websites affiliated with the Muslim Brotherhood movement for the first time. These websites included alshaab.com, alarabnews.com, and ikhwanonline.com. The Egyptian Journalists' Association's Freedoms Committee condemned the government's action. In October 2004, representatives of the three websites submitted a petition formally protesting the closure (Shabakat Allaadiniiyn Alearab 2004; Aljazirat Nit 2004).

Iran – In mid-2001, tensions arose between Iranian ISPs and the Ministry of Communications. Around one hundred ISPs banded together to protest what they perceived as unfair government competition. They argued that despite the government's self-proclaimed reformist agenda, the Ministry refused to provide additional phone lines to private ISPs, hindering their ability to compete effectively.

Adding to the internal debate, the head of the Supreme Council for Information issued a surprising statement in January 2005. He urged the legal system to intervene and halt the unilateral filtering of websites, particularly in light of the widespread blocking of blogs that had occurred that month. Expressing concern about the lack of adherence to basic legal procedures, he called for a thorough investigation by the Supreme Council of the Cultural Revolution, the body responsible for managing such matters. He hoped this investigation would rectify the filtering process and bring it back into compliance with legal principles.

In conjunction with the World Summit on the Information Society held in Tunis in mid-November 2005, a petition titled "Protest against Filtering of Information on Women in Iran" emerged. The petition, reportedly authored by various Iranian organisations, expressed strong opposition to government censorship and information filtering practices: "We, the undersigned, representing civil society organisations in Iran, women's organisations, web bloggers, technical professionals,

human rights organisations, academics, professionals, and concerned citizens, would like to express our serious concern and strongly object to the policy of filtering, censorship and blocking of information on the Internet in Iran, particularly information related to women's issues and gender" (Marzbandi, n.d.)

Saudi Arabia – Discussions arose within Saudi Arabia regarding the potential benefits of loosening restrictions on Internet access. This debate followed the failed launch of a chat website in early 1999. Proponents of the chat site argued that it could provide a healthy and controlled environment for communication between genders, particularly given the limitations on physical interaction in Saudi society. The implication was that online communication, where users could not see or hear each other directly, might offer a more acceptable alternative (Jehl 1999).

Syria – Syrian opposition figures challenged the government's strict Internet censorship policies. They argued that the government was unreasonably targeting email communication and blocking websites that discussed Syrian political issues. They further highlighted cases of individuals imprisoned for allegedly using the Internet illegally despite a lack of legal provisions concerning "electronic advertising"(Almarkaz Alsuwriu Lilqalam 2004). In addition to these criticisms, a Syrian media personality addressed an open letter to the Minister of Communications. The letter called for an end to the blocking of various websites, including Elaph.com, a prominent news website in the Arab world that was inaccessible within Syria. The author acknowledged that users with sufficient technical expertise could likely circumvent these restrictions but argued for unrestricted access regardless (Niufa 2004).

United Arab Emirates – In September 2000, Mohammed Al-Abar, director general of the Dubai Economic Department, highlighted the increasing difficulty of Internet censorship due to the growing popularity of satellite access and Internet use. The Minister of Culture and Information echoed this sentiment in an interview, predicting that Internet filtering would become more complex as Internet technology advanced. He argued that "the mechanisms responsible for Internet supervision" would eventually recognise the futility of such efforts.

These statements suggest that Internet censorship in the UAE was primarily motivated by cultural concerns and a desire to preserve traditional values. The Minister explicitly mentioned that censorship focused on blocking pornography to protect customs and traditions. He emphasised the government's right to ban inappropriate content but did not elaborate on the criteria for such decisions.

In late 2002, Sheikh Abdullah bin Zayed Al Nahyan, the Minister of Culture and Information, advocated for a significant shift in Internet policy. He argued for the government to cease nationwide Internet blocking, refrain from imposing individual censorship, and compel the country's sole ISPs to stop restricting access to specific websites. Sheikh Abdullah believed Internet censorship should only be a last resort, emphasising trust in citizens' judgment and intentions.

However, this stance contrasted with public opinion and the prevailing policy. The Minister of Communications reported receiving numerous subscriber requests to block pornography. This exemplified the broader issue of automatic website blocking based on perceived social, political, or religious inappropriateness. A public survey revealed that over half of residents supported Internet censorship to protect families from harmful content (The Arabic Network for Human Rights Information, n.d.-f).

Part E - Conclusions

The Internet emerged in the late 20th century as a transformative communication medium. Characterised by its speed, multi-directionality, and lack of intermediaries, it democratised access to information for diverse populations. This novel platform presented both opportunities and risks for governments, particularly those in totalitarian regimes. It fundamentally reshaped the relationship between administrations and individuals/groups within their societies.

The Internet's unique characteristics presented a double-edged sword for governments, demanding a severe and cautious approach. As a communication tool, it offered a range of strengths, weaknesses, opportunities, and threats (SWOT analysis) that would be detailed below. Strengths and opportunities reflected the Internet's positive aspects for governments, while weaknesses and threats captured the negative. Traditionally, a SWOT analysis differentiates between internal (strengths/weaknesses) and external factors (opportunities/threats). However, in the context of government-public relations and Internet use, the analysis focused primarily on the Internet's inherent features (strengths/weaknesses) and the potential outcomes (positive/negative) of Internet penetration within a country. These possible outcomes constituted the study's key conclusions.

Strengths

Accessibility to multifaceted information in real-time – the Internet allows direct access to information and its exchange in an immediate and unmediated way both within and outside the destination country.

Routing information accurately ensures that the information reaches the end user directly while allowing the user to characterise the data according to his nature and needs.

Weaknesses

Technological barriers to Internet penetration – Widespread Internet access requires significant infrastructure investments. Governments must deploy communication networks, equipment, and computing resources to enable broad Internet adoption within their countries.

Cultural barriers to Internet penetration – Cultural factors also impede Internet penetration. Basic literacy (local language and often English) and computer skills are necessary to utilise the Internet's full potential.

Sectorial disparities in Internet access – Compared to traditional media like radio, television, and newspapers, Internet access remained uneven during the period under review. It often varied based on geographical location and demographics, limiting accessibility for specific population segments.

Opportunities

Economic benefits – The Internet emerged as a powerful driver of economic growth, presenting many business opportunities for countries and their local economies. Recognising this potential, the UAE, particularly Dubai, took proactive steps to establish itself as a regional leader in the digital economy. Similarly, Egypt voiced its ambition to become a prominent player in this domain.

A virtual space for public 'letting off steam' – In centralised regimes, the Internet emerged as a double-edged sword for governments. It provided a virtual space for controlled dissent, allowing educated, oppositional, and religious groups critical of the administration to vent their frustrations. This online platform offered a degree of anonymity compared to traditional media outlets, which were often more closely monitored by the authorities.

Tracking moods among different audiences – However, the Internet's unique characteristics also allowed governments to gauge public sentiment. The ability of diverse populations to express opinions quickly, exchange views, and even

contact officials directly via email made the Internet a valuable tool for "checking the public pulse" on various issues. While this monitoring necessarily focused on those with Internet access, it still provided valuable insights into public opinion.

Self-positioning of the government – The Internet empowered governments to become proactive players in the online sphere. Beyond reacting to citizen or foreign actions, governments could use websites to shape public discourse and cultivate a desired image for domestic and international audiences. For instance, Syrian websites regarding the Golan Heights presented the issue from the government's perspective.

Improved ability to prevent access to content – Compared to traditional media, the Internet provided governments with a significantly enhanced capacity to manage information. Filtering content became akin to redacting specific sentences rather than censoring entire books (blocking whole websites). This granular control allowed governments to tailor information dissemination to target audiences, starkly contrasting to the past, where control centred on publication approval. Now, governments can selectively edit content and determine who can access it. By strategically blocking websites and monitoring user activity, they could influence information flow and restrict online and offline actions.

Threats

The Internet as a challenge for the government – The Internet presented a complex challenge for governments, particularly centralised regimes. It created a new arena fraught with potential disruptions, as detailed below:

- **Openness vs. Closure:** Governments faced a dilemma in determining the level and manner of internet access within their countries. Balancing openness with the need for control proved to be a significant challenge.
- **Monitoring Challenges:** Effective online monitoring requires significant technological investment. Governments needed resources to track individuals accessing "problematic" websites 24/7.

- **Western Influence:** The Internet, often perceived as a Western-dominated sphere, presented content potentially subversive to established government and societal norms.
- **Platform for Dissent:** The Internet offered opposition parties a new platform to critique government policies and actions, particularly during periods of crisis or uncertainty.
- **Managing Public Image:** Governments needed to actively counter potentially harmful online narratives by providing alternative information and shaping their public image.

The evaluations required to limit Internet use – Governments faced a daunting task in curtailing Internet use. Careful evaluation across various domains was necessary:

- **Technology:** Governments seeking to control Internet access employed a multi-pronged approach. Technological measures included monitoring online activity, tracking users, and blocking specific content. This strategy necessitated significant investments in surveillance infrastructure.
- **Legislation:** Beyond technology, some countries enacted legal restrictions. These restrictions could take two forms: high Internet access costs to limit affordability or regulations specifying the types of content users could access or create.
- **Comprehensive system:** Governments often establish dedicated bodies for comprehensive control. Saudi Arabia's Internet Service Unit (ISU) serves as an example. This agency functioned as the country's Internet router and assumed responsibility for blocking websites and content. The ISU actively solicited public participation by encouraging citizens to report inappropriate websites.
- **Motivations for Internet Monitoring**: This study suggests that Internet monitoring in Middle Eastern countries stemmed from perceived threats to regime stability or societal values. In Syria and Egypt, governments prioritised monitoring content that challenged their legitimacy and was seen as an immediate

threat. In contrast, Saudi Arabia and the UAE focused on content perceived as undermining moral values, which they believed could eventually destabilise the political order.

- **The Openness Paradox:** Centralized governments faced a constant dilemma regarding internet access. Embracing the Internet and its potential benefits (widespread access, information sharing, and economic growth) also meant accepting the possible spread of Western culture and ideas perceived as threatening. Conversely, restricting Internet access could hinder progress, information access, and global integration.

The Internet as a Challenge to Regimes – The analysis suggests that the Internet posed a significant challenge to regime stability and societal values. Governments seeking to maintain control needed to:

- **Monitor online activity:** Tracking content, the public sentiment expressed online, and user behaviour across different demographics.
- **Analyse trends and adapt:** Leaders must understand emerging online trends and formulate tactical responses for immediate situations alongside long-term strategies.

Future Research Directions:

This study lays the groundwork for further exploration of the Internet's impact on the Middle East. Several potential areas of future research include:

- **Self-censorship on websites:** Examining the prevalence and motivations behind self-censorship practices on various websites.
- **Content analysis:** Delving into the nature of content found on Middle Eastern websites.
- **Gender, language, and culture:** Investigating the Internet's impact on these aspects of Middle Eastern societies.
- **Citizen engagement:** Analysing the Internet's influence on individual lives and civic participation.

- **Infrastructure and technology:** Exploring the region's technological infrastructure and developments related to Internet access.
- **Government utilisation:** Examining how governments in the Middle East actively leverage the Internet.

This research offers a springboard for a wide range of future studies that can deepen our understanding of the Internet's complex role in the MENA.

REFERENCES

1. 3abdelbasset. 2007. "Suar Aikhtiraq Mawqie Ghurfat Alhaki (Arabic)." Muntadayat 'ansar al Muhamad. September 19, 2007. http://www.ansaaar.net/vb/showthread.php?p=152054.
2. 1923Turk. n.d. "1923Turk." Zone-h. Accessed December 11, 2023. http://www.zone-h.org/archive/defacer=Swan.
3. aB0 m0h4mM3d. n.d. "Yoshra.Co.Il Hacked. Notified by AB0 M0h4mM3d." Zone-h.Org. Accessed December 12, 2023. http://www.zone-h.org/mirror/id/9063873.
4. Abdel Hameed, Alaa. 1999. "Saudi Arabia's Online Population Explosion." Internetnews.Com. August 1999. https://web.archive.org/web/20050322091647/http://www.internetnews.com/bus-news/article.php/173321.
5. Abdulla, Rasha A. 2005a. "Taking the E-Train: The Development of the Internet in Egypt." *Http://Dx.Doi.Org/10.1177/1742766505054630* 1 (2): 149–65. https://doi.org/10.1177/1742766505054630.
6. ———. 2005b. "Taking the E-Train: The Development of the Internet in Egypt." *Http://Dx.Doi.Org/10.1177/1742766505054630* 1 (2): 149–65. https://doi.org/10.1177/1742766505054630.
7. Abohamza Almohajir. 2009. "Mycustomphoto.Com Hacked. Notified by Abohamza Almohajir." Zone-h.Org. July 19, 2009. http://www.zone-h.org/mirror/id/9258284.
8. Abu Omar. 2005. "Majlis Alfatwaa al'aelaa Yuhddd Miqdar Sadaqat Alfitr Wafidyat Alsawm Wanisab Alzakaa (Arabic)." Amilatqua Alftihaawi. October 5, 2005. http://fatehforums.com/showthread.php?t=11837.
9. "Access Denied Version 2.0: The Continuing Threat Against Internet Access and Privacy and Its Impact on the Lesbian, Gay, Bisexual and Transgender Community." 1999. https://web.archive.org/web/20030617085152/http://www.glaad.org/documents/media/AccessDenied2.pdf.

10. admin. 2008. “Bayan Suhufiun Hawl Aikhtiraq Shabakat Alqisat Alearabia (Arabic).” Wikalat Wata Lilainiba’. November 19, 2008. http://www.watan-ews.com/news.php?action=view&id=1433.
11. Agd_Scorp. n.d. “Agd_Scorp.” Zone-H. Accessed December 10, 2023. http://zone-h.org/archive/defacer=Agd_Scorp?hz=1.
12. ’ajwad alfasi, Hitun. 2008. “Hal Bayt Allah Alharam Lilrijal Faqat? (Arabic).” Alriyad. April 6, 2008. https://www.alriyadh.com/332214.
13. Akdeniz, Yaman. 1998. “Who Watches the Watchmen? Internet Content Rating Systems and Privatised Censorship.” *The Australian Library Journal* 47 (1): 28–42. https://doi.org/10.1080/00049670.1998.10755831.
14. “Al Diwan Al Amiri.” n.d. Accessed December 3, 2023. https://web.archive.org/web/20061215181824/http://www.da.gov.kw/langsel.php.
15. Albikri, Yusuf. 2009a. “Akhtiraq Aleadui Warihabih (Arabic).” Almultaqaa Alqasamaa. January 18, 2009. http://www.almoltaqa.ps/arabic/showthread.php?t=99477.
16. ———. 2009b. “Mawaqie Mashbuha (Arabic).” Almultaqaa Alqasamaa. January 17, 2009. http://www.almoltaqa.ps/arabic/showthread.php?t=99482.
17. ———. 2009c. “Tariqat Sahlat Liakhtiraq Almawaqie Alyahudia (Arabic).” Almultaqaa Alqasamaa. January 18, 2009. http://www.almoltaqa.ps/arabic/showthread.php?t=99831.
18. Albiqaeiu, Murih. 2007. “Sharq Alghayb Wagharb Almaerifa (Arabic).” ’iilaf. October 24, 2007. https://elaph.com/ElaphWeb/AsdaElaph/2007/10/273736.htm.
19. Aldaahir, Maryam. 2007. “Al’iielam Alearabiu Wa<<maa Yusamaa Bial’iirhabi>> (Arabic).” Alsharq Al’awsat. June 16, 2007. https://web.archive.org/web/20070823180515/http://www.asharqalawsat.com/leader.asp?section=3&article=423910&issue=10427.
20. Aleuayjan, Khalid. 2008. “Mawqie <<alearabiat Nat>> Kharij Alkhidmati.. Wa’asabie Aliaitiham Tatajih Li<<hakrz Shieat>> (Arabic).” Alsharq Al’awsat. October 11, 2008. https://archive.aawsat.com/details.asp?section=4&issueno=10910&article=490286&feature=.

21. "AlGathafi Speaks." n.d. Accessed December 3, 2023. https://web.archive.org/web/20230303000844/http://www.algathafi.org/.
22. Alhamdan, Nasir. 2008. "Qanaat Alearabiat Taht Qasf Qarasinat Alshabaka .. Aikhtiraq Jadid Limawqie Alqanaat Ealaa Alantirnit (Arabic)." Alwiam. October 14, 2008. https://web.archive.org/web/20081109022820/http://www.alweeam.com/news/news-action-show-id-5833.htm.
23. Alhuidar, Wajiha. 2008. "Aielamuu ...2 (Arabic)." Alhiwar Almutamadin. February 23, 2008. https://www.ahewar.org/debat/show.art.asp?aid=125832.
24. Aljazirat Nit. 2004. "Daewaa Qadayiyatan Dida 'iighlaq Alhukumat Almisriat Mawaqie 'Iilikturuniatan (Arabic)." October 18, 2004. https://web.archive.org/web/20080702004801/http://www.aljazeera.net/News/archive/archive?ArchiveId=95911.
25. Almarkaz Alsuwriu Lilqalam. 2004. "Ghiab Sahafat Muearidat Wataqyid Mutashadid Ealaa Alantirnit Waqame Huriyat Altaebir (Arabic)." March 13, 2004. https://web.archive.org/web/20050211200011/http://www.rezgar.com/debat/show.art.asp?aid=15798.
26. "Almawqie Alrasmiu Lijalalat Almalik Eabdallah Althaani Aibn Alhusayn (Arabic)." n.d. Accessed December 3, 2023. https://www.kingabdullah.jo/.
27. Almeida, Marcelo (Vympel). n.d. "Statistics Report 2005-2007." Zone-h. Accessed December 9, 2023. http://www.zone-h.org/news/id/4686?hz=1.
28. Almeida, Marcelo (Vympel), and Fernandez Kevin (Siegfr). 2008. "ICANN and IANA Domains Hijacked by Turkish Crackers." Zone-h. June 26, 2008. http://zone-h.org/news/id/4695.
29. "Almithliiyn Alearab (Arabic)." n.d. Accessed November 24, 2023. https://web.archive.org/web/20000511055844/http://www.geocities.com/saudigays/aindex.htm.
30. Alshaqa'i, Muhamad. 2002. "Alantarnit 'Tihat Almuraqabata' Walan Natruk Alhabl Ealaa Algharib Qamaran Saeudiaan Yata'alaqan Fi Alfada'i.. Waleata' Mutawasil (Arabic)." Alyawm Alsueudiu. July 7, 2002. https://web.archive.org/web/20070616112837/http://www.alyaum.com/issue/page.php?IN=10614&P=1&G=2.

31. ALTBT. n.d. “Www.Sportreport.Gr Hacked. Notified by ALTBT.” Zone-h.Org. Accessed December 10, 2023. http://www.zone-h.org/mirror/id/9846618.
32. Alterman, Jon B. 1998. “New Media, New Politics? From Satellite Television to the Internet in the Arab World.” *The Washington Institute*. https://www.washingtoninstitute.org/policy-analysis/new-media-new-politics-satellite-television-internet-arab-world-0.
33. Al’ustuani, Salwaa. 2005. “Tashdid Raqabat Almawaqie ‘Almueadiati’ Bi’iintirnit Suria (Arabic).” ’iislam ’Uwn Layin. May 23, 2005. https://web.archive.org/web/20061104232051/http://www.islamonline.net/Arabic/news/2005-05/23/article05.shtml.
34. “Alwaan - Arab Lesbian Women & Allies Network.” n.d. Accessed December 5, 2023. http://alwaandykes.blogspot.com/.
35. “Amiri Diwan, Doha, Qatar.” n.d. Accessed December 3, 2023. https://web.archive.org/web/20020605033316/http://www.diwan.gov.qa/.
36. Anderson, Jon. 1997. “The Internet and the Middle East: Commerce Brings Region On-Line.” *Middle East Executive Reports* 20 (12). https://web.archive.org/web/19991005170959/http://www.georgetown.edu/research/arabtech/meer97.htm.
37. Anderson, Jon W. 1996. “Middle East Diasporas on the Internet.” In . Montreal, Canada: Transforming Our Society Now. https://web.archive.org/web/20160202161155/http://www.isoc.org/inet96/proceedings/e8/e8_2.htm.
38. ———. 1997. “Cybernauts of the Arab Diaspora.” In . University of Maryland. https://web.archive.org/web/19991005012131/http://www.georgetown.edu/research/arabtech/anders97.htm.
39. api-3801794. 2008. “HOWTO-Hacking Wireless Networks-Arabia.” https://www.scribd.com/doc/7007945/HOWTO-Hacking-Wireless-Networks-Arabia.
40. Arab Club for Media and Information Technologies. 2002. “Muntadi ’urduniyun Hawl Musharakat Almar’at Fi Qitae Tiknulujia Almaelumat (Arabic).” November 13, 2002. https://web.archive.org/web/20040824003213/http://www.ac4mit.org/_jordan.asp?FileName=20021113180418.
41. “Arab Lounge.” n.d. Accessed December 5, 2023. https://arablounge.com/.

42. Arab Media. 2001a. "Council of Ministers Resolution." February 25, 2001. https://web.archive.org/web/20011110075826/http://www.al-bab.com/media/docs/saudi.htm.
43. ———. 2001b. "Saudi Internet Rules." February 25, 2001. https://web.archive.org/web/20010608092102/http://www.al-bab.com/media/docs/saudi.htm.
44. "Arab Sex." n.d. Accessed December 5, 2023. https://web.archive.org/web/20070519100946/http://www.arab-sex.com/.
45. "Arabic Sex Movies. Arab Girls - Arab Sex Models - Arabicsex." n.d. Accessed December 5, 2023. https://web.archive.org/web/20070827002441/http://www.arabicsexonline.com/.
46. "Arab-Slut." n.d. Accessed December 5, 2023. https://web.archive.org/web/20100204061218/https://arab-slut.com/.
47. Arnum, Eric, and Sergio Conti. 1998. "Internet Deployment Worldwide: The New Superhighway Follows the Old Wires, Rails, and Roads." In . Geneva, Switzerland: Internet Society. https://web.archive.org/web/20160103141908/https://www.isoc.org/inet98/proceedings/5c/5c_5.htm.
48. Askhita, Hasna. 2000. "The Internet in Syria. NMIT Working Papers." Georgetown University. March 2, 2000. https://web.archive.org/web/20050307085243/http://nmit.georgetown.edu/papers/askhita2.htm.
49. Atkin, David J., Leo W. Jeffres, and Kimberly A. Neuendorf. 1998. "Understanding Internet Adoption as Telecommunications Behavior." *Journal of Broadcasting & Electronic Media* 42 (4): 475–90. https://doi.org/10.1080/08838159809364463.
50. Bahrain Tribune. 2005a. "A Day of Joy for E-Visa Project Team Shaikh Rashid Honors Staff for Winning IT Award." November 26, 2005. http://www.bahraintribune.com/ArticleDetail.asp.
51. ———. 2005b. "Batelco to Cut ADSL Rates." December 21, 2005.
52. ———. 2005c. "Batelco to Spend BD50m to Be More Competitive." December 26, 2005.
53. ———. 2005d. "Security Net: Around Kids Bill Proposes Close Vigil on Minors at Internet Cafés." Bahrain Tribune. December 19, 2005.

54. ———. 2005e. "Students Viewing Porn Sites in School Labs." December 22, 2005. http://www.bahraintribune.com/ArticleDetail.asp.
55. Bakier, Abdul Hameed. 2007. "The New Issue of Technical Mujahid, a Training Manual for Jihadis - Jamestown." *Terrorism Monitor, The Jamestown Foundation* 5 (6). https://jamestown.org/program/the-new-issue-of-technical-mujahid-a-training-manual-for-jihadis/.
56. Balancing Act. n.d. "Sudan: Proxy Government Monopoly Impedes Growth." Balancing Act. Accessed December 8, 2023. https://web.archive.org/web/20010215172408/https://www.balancingact-africa.com/news/back/balancing-act24.html.
57. Barak, Sylvie. 2008. "India and Pakistan Hack It out Online." SC Magazine Australia/NZ. November 28, 2008. https://web.archive.org/web/20090116181247/http://www.securecomputing.net.au/News/129656,india-and-pakistan-hack-it-out-online.aspx.
58. Bashir Mohamed, Mohamed El. 2005. "The State of the Internet in Sudan." Network Startup Resource Center (NSRC). May 10, 2005.
59. Bashtahi, Nahid. 2003. "Hajb Almawaqie Alalikturuniat 'am Hajb Aleuquli?! (Arabic)." Shabakat Rasid al'iikhbaria. August 17, 2003. https://web.archive.org/web/20050212072645/http://www.rasid.com/artc.php?id=116.
60. Bazar, Bayaarma, and Gregg Boalch. 1997. "A Preliminary Model of Internet Diffusion within Developing Countries." July 1997. https://web.archive.org/web/20020219095349/http://ausweb.scu.edu.au/proceedings/boalch/paper.html.
61. BBC News. 2002a. "Net Ban Sparks Protests in Bahrain." May 4, 2002. http://news.bbc.co.uk/2/hi/middle_east/1968446.stm.
62. ———. 2002b. "Web Gives a Voice to Iranian Women." June 17, 2002. http://news.bbc.co.uk/2/hi/science/nature/2044802.stm.
63. ———. 2003. "Iran Steps up Net Censorship." BBC News. May 12, 2003. http://news.bbc.co.uk/2/hi/technology/3019695.stm.
64. ———. 2004a. "Saudi Crackdown on Camera Phones." July 20, 2004. http://news.bbc.co.uk/2/hi/middle_east/3911219.stm.

65. ———. 2004b. "Syrian Jailed for Internet Usage." June 21, 2004. http://news.bbc.co.uk/2/hi/middle_east/3824595.stm.
66. Beaver, Kevin. 2006. "Hacking for Dummies, 2nd Edition," 388. https://dl.acm.org/doi/book/10.5555/1200398.
67. Bensedrine, Sihem. n.d. "La Navigation Sous Haute Surveillance." Accessed December 13, 2023. https://web.archive.org/web/20070124211113/http://www.kalimatunisie.com/html/num1/Internet.htm.
68. "Bnat-Zone." n.d. Accessed December 5, 2023. https://web.archive.org/web/20100212195830/http://bnat-zone.com/.
69. Buck, Kames. 2008. "'Arrested.'" X. April 10, 2008. https://twitter.com/james-buck/status/786571964.
70. "Bulletin 002." 2004. https://web.archive.org/web/20040610172701/http://opennetinitiative.net/bulletins/002/.
71. Burkhart, Grey E. 1998. "National Security and the Internet in the Persian Gulf: Saudi Arabia." March 1998. https://web.archive.org/web/20070601175630/http://www.georgetown.edu/research/arabtech/pgi98-9.html.
72. Burkhart, Grey E., and Seymour E. Goodman. 1998. "The Internet Gains Acceptance in the Persian Gulf." *Communications of the ACM* 41 (3): 19–24. https://doi.org/10.1145/272287.272290.
73. "Buslman." n.d. Accessed December 3, 2023. https://web.archive.org/web/20070109072619/http://www.bahrainking.net/site.
74. "Bypassing Restrictive Proxies." 2002. http://www.flurnet.org.
75. "Campaign to Free Ahmad Sa'adat." n.d. Accessed December 6, 2023. https://freeahmadsaadat.org/.
76. Captain, Sean. 2001. "SafeWeb's Anonymous Browsing Service." PCWorld. April 6, 2001. https://web.archive.org/web/20010807041329/http://www.pcworld.com/reviews/article/0,aid,46303,00.asp.
77. Cashmore, Pete. 2007. "YouTube Blocked in Turkey." Mashable. March 7, 2007. https://mashable.com/archive/youtube-blocked-turkey.

78. Center for Systemic Peace (CSP). n.d. "Polity5 Project, Political Regime Characteristics and Transitions, 1800-2018." Accessed November 28, 2023. https://www.systemicpeace.org/inscrdata.html.
79. "Change for Equality." n.d. Accessed December 5, 2023. https://web.archive.org/web/20080903095408/http://www.forequality.info/english.
80. Chickowski, Ericka. 2006. "Pakistan Makes Arrests in Ransom-Hacking Case." SC Magazine Australia. December 12, 2006. https://web.archive.org/web/20070923122052/http://www.securecomputing.net.au/News/70021,pakistan-makes-arrests-in-ransomhacking-case.aspx.
81. Committee to Protect Journalists. 2005. "Attacks on the Press 2004: Iran." Committee to Protect Journalists. March 14, 2005. https://cpj.org/2005/03/attacks-on-the-press-2004-iran/.
82. ———. 2009. "10 Worst Countries to Be a Blogger." April 30, 2009. https://cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger/.
83. Curt. 2007. "YouTube Blocked in Syria." Committee to Protect Bloggers. August 30, 2007. https://web.archive.org/web/20080224053639/http://committeetoprotectbloggers.org/2007/08/30/youtube-blocked-in-syria/.
84. Dahan, Michael. n.d. "Internet Usage in the Middle East." The Hebrew University of Jerusalem. Accessed November 24, 2023. https://web.archive.org/web/20001007180945/http://www.mevic.org/papers/inet-mena.html.
85. Daily Mail. 2006. "Fake Relics Sold on EBay 'Funding Terrorism.'" November 22, 2006. https://www.dailymail.co.uk/news/article-417967/Fake-relics-sold-eBay-funding-terrorism.html.
86. "Dalia Ziada Blog." n.d. Accessed December 5, 2023. http://daliaziada.blogspot.com/.
87. Damari, Kfir, Ami Chayun, and Gadi Evron. 2006. "Case Study: A Cyber-Terrorism Attack, Analysis and Response." http://www.zone-h.net/defaced/2006/07/10/www.otherhackedsite.co.il/.
88. DATA ir Security Group. n.d. "Www.Un.Org.Ir Hacked. Notified by DATA Ir Security Group." Zone-h.Org. Accessed December 10, 2023. http://zone-h.org/mirror/id/9058635.

89. Department of Justice. 2002. "#734: 12-18-02 SENIOR LEADER OF HAMAS AND TEXAS COMPUTER COMPANY INDICTED FOR CONSPIRACY TO VIOLATE U.S. BAN ON FINANCIAL DEALINGS WITH TERRORISTS." Department of Justice. December 18, 2002. https://www.justice.gov/archive/opa/pr/2002/December/02_crm_734.htm.
90. Dholakia, Ruby Roy, Nikhilesh Dholakia, and Nir Kshetri. 2003. "Gender and Internet Usage." In *The Internet Encyclopedia*, 1–34. New York: Wiley. https://web.archive.org/web/20040310180802/http://ritim.cba.uri.edu/wp2003/pdf_format/Wiley-Encycl-Internet-Usage-Gender-Final.pdf.
91. Dimaggio, Paul, Eszter Hargittai, W Russell Neuman, and John P Robinson. 2001. "Social Implications of the Internet." *Annual Review of Sociology*, 307–36. http://www.casa.ucl.ac.uk/cyberspace/dimaggio_social_implications_ofthe_internet.pdf.
92. "Documenting Internet Content Filtering Worldwide." 2004. The OpenNet Initiative. 2004. https://web.archive.org/web/20040602211740/http://www.opennetinitiative.net/modules.php?op=modload&name=Archive&file=index&req=viewarticle&artid=5.
93. Dz-Boys Team. n.d. "Ratiohomini.Hu Hacked. Notified by Dz-Boys Team." Zone-h.Org. Accessed December 12, 2023. http://www.zone-h.org/mirror/id/9258327.
94. Eabd Aleaziz Alkhutayb, Abtihal. 2008. "'ayn <<finughradna>>? (Arabic)." Sahifat 'awan. February 4, 2008. https://web.archive.org/web/20100215060810/http://www.awan.com/pages/oped/31332.
95. Edelman, Ben. 2003. "Sites Blocked by Internet Filtering Programs." https://cyber.harvard.edu/archived_content/people/edelman/mul-v-us/.
96. EDITOR: MYSELF. 2003. "Latest Blacklist." July 21, 2003. https://web.archive.org/web/20040216000733/http://hoder.com/weblog/archives/007715.html.
97. Emirates Internet and Multimedia. 2002. "Emirates Internet and Multimedia (EIM) Reduces Internet Leased Line Rates by More than 50% Leased Line Cost in the Middle East; Supports e-Business Drive in the UAE, Says EIM." April 10, 2002. https://web.archive.org/web/20031125141939/http://eim.ae/eim/isp/english/news/press/dedicated_slash_10apr02.html.

98. "EPIC Online Guide to Practical Privacy Tools." n.d. Electronic Privacy Information Center (EPIC). Accessed November 24, 2023. https://archive.epic.org/privacy/tools.html.
99. "Everyone's Guide to By-Passing Internet Censorship for Citizens Worldwide." 2007.
100. "Fact Sheet on Internet Filters." 2003. The Free Expression Policy Project. July 2003. https://web.archive.org/web/20021017101052/http://www.fepproject.org/factsheets/filtering.html.
101. Fatih El Tigani, Mohamed El. n.d. "Sudan Internet and .Sd Experience." Accessed December 8, 2023. https://www.itu.int/itudoc/itu-t/workshop/cctld/cctld050.pdf.
102. Fighel, Jonathan. 2006. "US Shuts down Hamas Charity." International Institute for Counter-Terrorism. May 28, 2006. https://web.archive.org/web/20090203151943/http://www.ict.org.il/NewsCommentaries/Commentaries/tabid/69/Articlsid/127/currentpage/9/Default.aspx.
103. "Free Arab Sex Movies | Arabsex Pictures | Arabic Porn Videos." n.d. Accessed December 5, 2023. https://web.archive.org/web/20080208105132/http://arabsexweb.com/.
104. Freedom House. 2023. "Freedom in the World." 2023. https://freedomhouse.org/report/freedom-world#Data.
105. Freedom.IRAN. n.d. "Mdb.Economy.Gov.Ru Hacked. Notified by Freedom.IRAN." Zone-h.Org. Accessed December 10, 2023. http://zone-h.org/mirror/id/9258832.
106. Friedman, Thomas L. 1999. *The Lexus and the Olive Tree*. Farrar, Straus, Giroux. https://search.worldcat.org/title/40609510.
107. Fuaad, Abarahim. n.d. "Alaintarnit Wathaqafatuna Alwataniat Almuhadada (Arabic)." Qdaya Alkhalij. Accessed November 26, 2023. https://web.archive.org/web/20020605043308/http://www.gulfissues.net/mpage/gulfarticles/article0020.htm.
108. Gardner, Frank. 1998. "Saudi Arabia Awaits Internet Connection." BBC News. October 12, 1998. http://news.bbc.co.uk/2/hi/middle_east/192222.stm.

109. Gaza Hacker Team. n.d.-a. "Gaza Hacker Team." Zone-h. Accessed December 10, 2023. http://zone-h.org/archive/defacer=Gaza%20Hacker%20Team.
110. ———. n.d.-b. "Gaza Hacker Team." Zone-h. Accessed December 12, 2023. http://zone-h.org/archive/defacer=Gaza%20Hacker%20Team.
111. ———. n.d.-c. "Kuwait-Fm.Com Hacked. Notified by Gaza Hacker Team." Zone-h. Org. Accessed December 12, 2023. http://zone-h.org/mirror/id/7710320.
112. Gharbia, Sami Ben. 2007. "Turkey Blocks YouTube. Again." Global Voices Advocacy. September 19, 2007. https://web.archive.org/web/20080127163002/http://advocacy.globalvoicesonline.org/2007/09/19/turkey-blocks-youtube-again/.
113. ———. 2008a. "Human Rights Videos Besiege the Tunisian Presidential Palace." Global Voices Advox. May 27, 2008. https://advox.globalvoices.org/2008/05/27/human-rights-videos-besiege-the-tunisian-presidential-palace/.
114. ———. 2008b. "Silencing Online Speech in Tunisia." Global Voices Advox. August 20, 2008. https://advox.globalvoices.org/2008/08/20/silencing-online-speech-in-tunisia/.
115. ———. 2009. "North Africa: Are Political Websites More Likely to Get Hacked?" Global Voices Advox. January 30, 2009. https://advox.globalvoices.org/2009/01/30/north-africa-are-political-websites-more-likely-to-get-hacked/.
116. Ghashmary, Ahmad. 2009. "'Girls Only': Arab Women Live and on-Air." Mideast Youth. March 31, 2009. https://web.archive.org/web/20091001053836/http://www.mideastyouth.com/2009/03/31/%E2%80%9Cgirls-only%E2%80%9D-arab-women-live-and-on-air.
117. Ghasiba, Zaynab. 2008. "Alnisa' Wal'iirhab... (Arabic)." Alhayaa. July 5, 2008. https://web.archive.org/web/20100819075928/http://zavita.co.il/archives/301.
118. Gomes, Lee. 2002. "College Town in Jordan Is Full of Internet Cafes." The Wall Street Journal. November 18, 2002. https://www.wsj.com/articles/SB1037578457174429308.
119. Gooya news. 2004. "Eghdaam Dolat Baraaye Shenaasaayi Gardaanandegaan Sit-Haaye Eeinterneti Dar Iraan, Baaztaab (Persian)." December 8, 2004. https://web.archive.org/web/20050208153538/http://mag.gooya.com/politics/archives/020024.php.

120. Greene, Thomas C. 2001. "Do-It-Yourself Internet Anonymity." The Register. November 14, 2001. https://www.theregister.com/2001/11/14/doityourself_internet_anonymity.
121. Greenfield, Paul. 2001. *Effectiveness of Internet Filtering Software Products*. [Sydney : Australian Broadcasting Authority],. https://catalogue.nla.gov.au/catalog/3619546.
122. Guillén, Mauro F., and Sandra L. Suárez. 2005. "Explaining the Global Digital Divide: Economic, Political and Sociological Drivers of Cross-National Internet Use." *Social Forces* 84 (2): 681–708. https://doi.org/10.1353/SOF.2006.0015.
123. Hamidoui, Hassan. 2009. "Saudis Create Their Own World in Virtual Island." Al Arabiya. April 20, 2009. https://web.archive.org/web/20090422003508/http://www.alarabiya.net/articles/2009/04/20/71059.html.
124. Hargittai, Eszter. 1999. "Weaving the Western Web: Explaining Differences in Internet Connectivity among OECD Countries." *Telecommunications Policy* 23 (10–11): 701–18. https://doi.org/10.1016/S0308-5961(99)00050-6.
125. Haselton, Bennett. n.d. "Instructions for Getting around Blocking Software." Accessed November 24, 2023. http://www.peacefire.org/circumventor/simple-circumventor-instructions.html.
126. Hassan. 2005. "Internet in Iraq." An Average Iraqi. July 10, 2005. https://web.archive.org/web/20060209180058/http://aviraqi.blogspot.com/2005/07/internet-in-iraq.html.
127. Heins, Marjorie, and Christina Cho. 2001. "Internet Filters: A Public Policy Report." https://ncac.org/wp-content/uploads/import/Internet%20Filter.pdf.
128. "Her Highness." n.d. Accessed December 3, 2023. https://web.archive.org/web/20051025002929/http://www.mozahbintnasser.qa/.
129. "Her Royal Highness Princess Haya Bint Al Hussein." n.d. Accessed December 3, 2023. https://hrhprincesshaya.net/.
130. "His Highness Sheikh Mohammed Bin Rashid Al Maktoum." n.d. Accessed December 3, 2023. https://web.archive.org/web/20021126135627/https://www.sheikhmohammed.ae/.

131. "How to Blog Safely (About Work or Anything Else)." 2005. Electronic Frontier Foundation. May 31, 2005. https://www.eff.org/wp/blog-safely.
132. "How to Disable Your Blocking Software." n.d. PEACEFIRE – Open Net for the Net Generation. Accessed November 24, 2023. http://www.peacefire.org/bypass/.
133. Human Rights Watch. 1996. "SILENCING THE NET: The Threat to Freedom of Expression On-Line." *Human Rights Watch*. https://archive.epic.org/free_speech//intl/hrw_report_5_96.html.
134. Human Rights watch. 1999. "Bahrain: Human Rights Developments." https://www.hrw.org/legacy/worldreport99/mideast/Bahrain.html.
135. Human Rights Watch. 1999a. "The Internet In The Mideast And North Africa - Country Profiles - Bahrain." Human Rights Watch. June 1999. https://www.hrw.org/legacy/advocacy/internet/mena/bahrain.htm.
136. ———. 1999b. "The Internet In The Mideast And North Africa - Country Profiles-Saudi Arabia." June 1999. https://www.hrw.org/legacy/advocacy/internet/mena/saudi.htm.
137. ———. 1999c. "The Internet In The Mideast And North Africa - Country Profiles-United Arab Emirates." June 1999. https://web.archive.org/web/20050204100734/http://www.hrw.org/advocacy/internet/mena/uae.htm.
138. ———. 1999d. "The Internet In The Mideast And North Africa - Cybercensorship: Its Various Forms." Human Rights Watch. June 1999. https://www.hrw.org/legacy/advocacy/internet/mena/censorship.htm.
139. ———. 2003. "Egypt: End Internet Entrapment, Homosexual Prosecutions." February 21, 2003. https://www.hrw.org/legacy/press/2003/02/egypt022003.htm.
140. ———. 2005a. "False Freedom Online Censorship in the Middle East and North Africa." https://www.hrw.org/reports/2005/mena1105/mena1105no-appendices.pdf.
141. ———. 2005b. "Iran: Judiciary Should Admit Blogger Abuse." April 4, 2005. https://web.archive.org/web/20060211005040/http://hrw.org/english/docs/2005/04/04/iran10415.htm.

142. ———. n.d.-a. “The Internet In The Mideast And North Africa - Country Profiles-Tunisia.” Accessed December 13, 2023. https://www.hrw.org/legacy/advocacy/internet/mena/tunisia.htm.
143. ———. n.d.-b. “The Internet In The Mideast And North Africa: Jordan.” Human Rights Watch. Accessed November 30, 2023. https://www.hrw.org/legacy/advocacy/internet/mena/jordan.htm.
144. Hussaini, Amira Al. 2007. “Egypt: YouTube Disables Activist’s Account.” Global Voices. November 28, 2007. https://globalvoices.org/2007/11/28/egypt-youtube-disables-activists-account/.
145. IFEX. 2008. “New Internet Café Measures Tantamount to Censorship, Says ANHRI.” IFEX. August 11, 2008. https://ifex.org/new-internet-cafe-measures-tantamount-to-censorship-says-anhri/.
146. ———. n.d. “Ban on Gay Websites Lifted.” Accessed December 19, 2023. https://web.archive.org/web/20041229092047/http://www.ifex.org/en/content/view/full/57758/.
147. ’iilaf. 2004a. “Al’iintiha’ Min ’iiedad Mashrue Qanun Altawqie al’iiliktiruni Bimisr (Arabic).” April 1, 2004. https://elaph.com/ElaphWeb/Archive/1033202442782508500.htm.
148. ———. 2004b. “Tawaqueat Dirasat Misriatin: Hajm Altijarat Alalkitruniati6,9 Alf Milyar Dular Fi Eam2004 (Arabic).” April 1, 2004. https://elaph.com/ElaphWeb/Archive/1029828570219493400.htm.
149. ———. 2008. “Talaq Alfakis (Arabic).” September 15, 2008. https://elaph.com/Web/AsdaElaph/2008/9/365790.htm.
150. ’iislam ’uwn layin. 2003. “Alsuwriuwn Ghadibun Lihajb Mawaqie Bial’iintirnit (Arabic).” June 17, 2003. https://web.archive.org/web/20040622195426/http://www.islam-online.net/arabic/news/2003-06/17/article10.shtml.
151. InfoCom Corporation. n.d. “Profile.” Accessed December 6, 2023. https://web.archive.org/web/20111004164727/http://www.historycommons.org/entity.jsp?entity=infocom_corporation.

152. "International Islamic News Agency (IINA) Bulletin." 2004. February 8, 2004. https://web.archive.org/web/20040220065536/http://www.islamicnews.org/english/en_weekly.html.
153. "Internet Filtering Alternatives." n.d. Accessed November 23, 2023. https://silo.tips/download/special-report-internet-filtering-alternatives.
154. Internet Services Unit. 2006. "Local Content Filtering Procedure." 2006. https://web.archive.org/web/20070219053239/http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring-mechanism.htm.
155. Internet World Stats. n.d. "Middle East Internet Usage & Population Statistics." Accessed November 24, 2023. https://www.internetworldstats.com/stats5.htm.
156. Iranian Students' News Agency. 2004. "Be Hemat Motekhasesaan Markzeh Tahghighaat Sanaaye' Aanfoormatik, Filtering Hooshmand Boomi Aamaadeh-i Bahreh-Bardaari Ast (Persian)." November 12, 2004. https://web.archive.org/web/20050210112613/http://isna.ir/news/NewsCont.asp?id=453307&lang=P.
157. "Iraqi Presidency." n.d. Accessed December 3, 2023. https://web.archive.org/web/20051015024509/http://www.iraqipresidency.net/index.php?language=arabic.
158. Islam Online. 2003a. "Advice to Muslims Who Visit Chat Rooms." December 4, 2003. https://web.archive.org/web/20090709160749/http://www.islamonline.net/servlet/Satellite?pagename=IslamOnline-English-Ask_Scholar/FatwaE/FatwaE&cid=1119503547670.
159. ———. 2003b. "Advice to Overcome Porn Addiction." September 3, 2003. https://web.archive.org/web/20080111015304/http://www.islamonline.net/servlet/Satellite?pagename=IslamOnline-English-Ask_Scholar/FatwaE/FatwaE&cid=1119503547360.
160. ———. 2004. "Internet Related Fatwas." February 23, 2004. https://web.archive.org/web/20061122115742/http://www.islamonline.net/livefatwa/english/Browse.asp?hGuestID=LayrZP.

161. ———. 2005a. "Internet Chats Between Males and Females." November 13, 2005. https://web.archive.org/web/20060720010217/http://www.islamonline.net/servlet/Satellite?pagename=IslamOnline-English-Ask_Scholar/FatwaE/FatwaE&cid=1119503543228.
162. ———. 2005b. "Running an Internet Café." Islam Online. November 17, 2005. http://www.islamonline.net/servlet/Satellite?pagename=IslamOnline-English-Ask_Scholar/FatwaE/FatwaE&cid=1119503544580.
163. ———. 2008. "Choosing a Husband Through the Internet." November 6, 2008. https://web.archive.org/web/20090329034927/http://www.islamonline.net/servlet/Satellite?pagename=IslamOnline-English-Ask_Scholar/FatwaE/FatwaE&cid=1225697952817.
164. "Islamic Association for Palestine." n.d. Accessed December 6, 2023. https://web.archive.org/web/20110514233643/http://www.historycommons.org/entity.jsp?entity=association_for_palestine.
165. Islamic Ghosts Team. n.d. "Kokisunda.Net Hacked. Notified by Islamic Ghosts Team." Zone-h.Org. Accessed December 12, 2023. http://www.zone-h.org/mirror/id/8943999.
166. Islamic Republic News Agency (IRNA). 2004a. "Investment in IT Is 1000-1500 Billion Rials Annually." November 20, 2004. https://en.irna.ir/news/8952481/annually-rials-billion-1000-1500-is-IT-in-Investment.
167. ———. 2004b. "Iran-Kharrazi." October 20, 2004. http://www.irna.ir/en/news/view/line-25/0410200994194748.htm.
168. ———. 2004c. "Masjed Jamei Underlines Role of Internet in Dissemination of Cultural Information." November 26, 2004. https://en.irna.ir/news/8952946/of-dissemination-in-Internet-of-role-underlines-Jamei-Masjed.
169. ———. 2004d. "National Culture Can Be Promoted on Website via Persian Language." December 5, 2004. https://en.irna.ir/news/8953637/language-Persian-via-Website-on-promoted-be-can-culture-National.
170. ———. 2004e. "Punishment Fair Face Should Hackers Says Expert." December 20, 2004. https://en.irna.ir/news/8954688/punishment-fair-face-should-hackers-says-Expert.

171. ———. 2005a. "1st Governmental E-Payment Project to Launch in Isfahan." April 4, 2005. https://en.irna.ir/news/8920542/Isfahan-in-launch-to-project-e-payment-governmental-1st.
172. ———. 2005b. "Haddad Adel-University." June 13, 2005. http://www.irna.ir/en/news/view/line-25/0506130271105320.htm.
173. ———. 2005c. "Iran's Embassy in Madrid Launches Internet Site." January 15, 2005. https://en.irna.ir/news/8956463/site-internet-launches-Madrid-in-embassy-Iran-s.
174. ———. 2005d. "Iran's e-Trade Center Opens Officially." July 23, 2005. https://en.irna.ir/news/8927155/officially-opens-Center-E-Trade-Iran-s.
175. ———. 2005e. "Iran's Tourism Website Launched: Daily." November 6, 2005. https://en.irna.ir/news/8932662/Daily-launched-website-tourism-Iran-s.
176. ———. 2005f. "Motamedi: Number of Fixed Phones up 100 PC in 3rd Plan." February 16, 2005. https://en.irna.ir/news/8958848/plan-3rd-in-pc-100-up-phones-fixed-of-Number-Motamedi.
177. ———. 2005g. "Official :Internet through Obtainable Iran for Visas." February 8, 2005. https://en.irna.ir/news/8958166/official-Internet-through-obtainable-Iran-for-Visas.
178. ———. 2005h. "President's Advisor: Electronic Money to Be Introduced in 6 Months." February 3, 2005. https://en.irna.ir/news/8957818/6-in-introduced-be-to-money-Electronic-advisor-President-s.
179. itayzil. 2006. "Arab-American Psychologist Wafa Sultan." YouTube. August 14, 2006. https://web.archive.org/web/20070403084214/http://www.youtube.com/watch?v=mAXoDHy3_Ek.
180. ITP. 2004. "Iran Tops Middle East Internet Growth Chart." February 7, 2004. https://web.archive.org/web/20040209202937/http://www.itp.net/news/details.php?id=10957&tbl=itp_news.
181. Jayoush, Kinda. 2000. "Syria Begins Internet Expansion." Cafe-Syria.Com. August 4, 2000. https://web.archive.org/web/20020610074224/http://www.cafe-syria.com/Internet.htm.

182. Jehl, Douglas. 1999. "The Internet's 'Open Sesame' Is Answered Warily." The New York Times. March 18, 1999. https://web.archive.org/web/20021226022538/http://www.library.cornell.edu/colldev/mideast/saudint.htm.
183. "Journal Officiel de La République Tunisienne." 1997. https://web.archive.org/web/20070728011724/http://www.infocom.tn/fileadmin/Documentation/Juridiques/Jort_Ar/jort_24_25_3_1997.pdf.
184. "Journal Officiel de La République Tunisienne - N° 100." 1998. https://web.archive.org/web/20071005094244/http://www.infocom.tn/fileadmin/uploads/cahiers_charges_ligne/cc2_publitel_complement_fr_vf.pdf.
185. Kalathil, Shanthi, and Taylor C Boas. 2001. "The Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution." Washington. https://carnegieendowment.org/files/21KalathilBoas.pdf.
186. Kamali Dehghan, Saeed. 2010. "Iranian Activist Sues Telecoms Firm over 'Spying System.'" The Guardian. August 24, 2010. https://www.theguardian.com/world/2010/aug/24/iranian-sues-nokia-siemens-networks.
187. Kamel, Sherif. 1997. "The Birth of Egypt's Information Society." *International Journal of Computer and Engineering Management* 5 (3). https://web.archive.org/web/20020826073813/http://www.journal.au.edu/ijcem/sep97/article2.html.
188. Kamel, Tarek. 1997. "Internet Commercialization in Egypt: A Country Model." Information and Decision Support Center/Regional Information Technology and Software Engineering Center. 1997. https://web.archive.org/web/20160103124917/https://www.isoc.org/inet97/proceedings/E6/E6_2.HTM.
189. Kaplan, Carl S. 1997. "Filtering Companies Assailed for Blocking 'Unpopular' Voices." The New York Times. December 11, 1997. https://archive.nytimes.com/www.nytimes.com/library/cyber/law/121197law.html.
190. Kaplan, Dan. 2006. "Experts Release Al Qaeda Hack Alert." ITnews. December 4, 2006. https://www.itnews.com.au/news/experts-release-al-qaeda-hack-alert-69486.
191. ———. 2008. "Olympic Champion Phelps' Website Defaced in Turkish Hack." SC Media. August 21, 2008. https://www.scmagazine.com/news/olympic-champion-phelps-website-defaced-in-turkish-hack.

192. Karoui, Hichem. 2002. "The World Oldest Profession." UK Indymedia. July 14, 2002. https://web.archive.org/web/20041201061548/http://www.indymedia.org.uk/en/2002/07/35995.html.
193. Kettmann, Steve. 2001a. "1,001 Arabian Nights of Sex." WIRED. 2001. https://www.wired.com/2001/04/1001-arabian-nights-of-sex/.
194. ———. 2001b. "1,001 Arabian Nights of Sex." WIRED. April 24, 2001. https://www.wired.com/2001/04/1001-arabian-nights-of-sex/.
195. Khaldu, Hayfaa'. n.d. "Mubadarat Altalaq Alsueudii (Arabic)." Altalaq Alsueudiu. Accessed December 4, 2023. https://web.archive.org/web/20110806174050/http://saudidivorce.org/DIV.
196. "King Abduallah, Saudi Arabia." n.d. Accessed December 3, 2023. https://www.the-saudi.net/al-saud/abduallah.htm.
197. "King Fahd Bin Abdul Aziz." n.d. Accessed December 3, 2023. https://web.archive.org/web/20011107163929/https://www.kingfahdbinabdulaziz.com/.
198. King_Wolf. n.d. "Mysunnydaleschool.Com Hacked. Notified by King_Wolf." Zone-h.Org. Accessed December 11, 2023. http://www.zone-h.org/mirror/id/9258366.
199. Kirchner, Henner. 2001. "Internet in the Arab World: A Step Towards 'Information Society?'" In *Mass Media, Politics & Society in the Middle East*, 137–58. https://web.archive.org/web/20030312124143/http://www.journalism-islam.de/Internet/massmedia.pdf.
200. "Kuluna Laylaa (Arabic)." n.d. Accessed December 5, 2023. https://web.archive.org/web/20081217033518/http://kolenalaila.com/.
201. l0gic. 2005. "Governing the Internet." NewOrder - Computer Security and NetworkingPortal.March6,2005.https://web.archive.org/web/20051018144748/http://neworder.box.sk/newsread.php?newsid=13345.
202. Lemos, Robert, and Ian Fried. 2003. "Arab News Site Suffers Outages." CNET News.Com. March 26, 2003. https://web.archive.org/web/20080316083059/http://news.zdnet.co.uk/itmanagement/0,1000000308,2132484,00.htm.
203. Lokot, Tetyana, and Mariëlle Wijermars. 2023. "The Politics of Internet Freedom Rankings" 12 (2). https://doi.org/10.14763/2023.2.1710.

204. "Love in a Headscarf." n.d. Accessed December 5, 2023. https://web.archive.org/web/20120110180502/http://www.loveinaheadscarf.com/site/.
205. MacFarquhar, Neil. 2004. "In Tunisia, a Heavy Hand on Web Cafés." The New York Times. June 26, 2004. https://web.archive.org/web/20041212023230/http://www.iht.com/bin/print.php?file=526755.html.
206. Mahmoud. 2008. "CAN 2008: Moroccan Hackers Bring down Ghana 2008 Website." WorldCupBlog. January 30, 2008. http://morocco.worldcupblog.org/uncategorized/can-2008-moroccan-hackers-bring-down-ghana-2008-website.html.
207. "Majalat Filastin Almuslima (Arabic)." n.d. Accessed December 6, 2023. https://web.archive.org/web/20090417183026/http://www.fm-m.com/2009/apr/subscription.php.
208. Marshall, Monty G, and Ted Robert Gurr. 2020. "POLITY5 Political Regime Characteristics and Transitions, 1800-2018 Dataset Users' Manual." https://www.systemicpeace.org/inscr/p5manualv2018.pdf.
209. Marzbandi, Fatemeh. n.d. "Protest against Filtering of Information on Women in Iran Petition." Accessed December 12, 2023. https://web.archive.org/web/20070108083419/http://www.petitiononline.com/womeno/petition.html.
210. "Mawqie Alhamlat al'iintikhabiat Lilrayiys Zayn Aleabidin Bin Eali (Arabic)." n.d. Accessed December 3, 2023. https://web.archive.org/web/20080722161026/http://www.benali.tn/.
211. "Mawqie Muasasat Alshahid (Arabic)." n.d. Accessed December 6, 2023. https://web.archive.org/web/20060203145617/http://www.alshahid.org/.
212. maykal. 2003. "Maykal's Sudan Travel Tips." VirtualTourist.Com. October 30, 2003. https://web.archive.org/web/20041020002043/http://www.virtualtourist.com/m/20ab6/fc1/1/.
213. McCullagh, Declan. 1997. "Arab Youths Bypass Government's CyberPatrol Net-Censorship (Fwd)." September 23, 1997. https://www.fitug.de/debate/9709/msg00037.html.
214. McLaughlin, Erin. 2003. "Iran Keeps an Eye on the Bloggers." CNN. July 18, 2003. http://edition.cnn.com/2003/WORLD/meast/07/16/iran.blogs/index.html.

215. McLaughlin, Sean W. 2003. "The Use of the Internet for Political Action by Non-State Dissident Actors in the Middle East." *First Monday* 12 (8). https://doi.org/10.5210/FM.V0I0.1791.
216. Middle East Online. 2009. "Saudi Clerics Call for Women Ban from Media, TV." March 24, 2009. https://web.archive.org/web/20100820233606/http://www.middle-east-online.com/english/?id=31157.
217. Middle East Quarterly. 1997. "Steven Emerson: Get Ready for Twenty World Trade Center Bombings," June. https://www.meforum.org/353/steven-emerson-get-ready-for-twenty-world-trade.
218. Miller, Robin "Roblimo." 2004. "Meet Saudi Arabia's Most Famous Computer Expert." Linux.Com. January 14, 2004. https://www.linux.com/news/meet-saudi-arabias-most-famous-computer-expert/.
219. Moey. 2007. "Youtube Is Blocked in Syria." July 28, 2007. https://web.archive.org/web/20090923145735/http://moeys.net/2007/07/28/youtube-is-blocked-in-syria.
220. Mor, Gal, and Ehud Kinan. 2006. "Major Israeli Websites Hacked." Ynet. June 28, 2006. https://www.ynetnews.com/articles/0,7340,L-3268449,00.html.
221. MOTIC. 2007. "YouTube Censuré Par Maroc Telecom!!!" May 25, 2007. https://web.archive.org/web/20070627165616/http://motic.blogspot.com/2007/05/youtube-censur-par-maroc-telecom.html.
222. Naeimi99. 2004. "Lubnaniat Tahtariq Mawqie 'iisrayiyliin .. Khabar Eajil." Shabakat Hijr. May 17, 2004. http://www.hajr-network.net/hajrvb/showthread.php?t=402760899.
223. Naeuti, Fatima. 2008. "Aldyn Lilhi, Fahal Alwtn Liljamiei? (Arabic)." Alhiwar Almutamadin. January 5, 2008. https://www.vizsweet.com/.
224. nart. 2004. "Choosing Circumvention." Internet Censorship Explorer. July 18, 2004. https://web.archive.org/web/20061015133120/http://ice.citizenlab.org/?p=33.
225. ———. 2006. "Citizen Lab Is Hiring!" Citizen Lab. January 16, 2006. https://web.archive.org/web/20070816051118/http://www.citizenlab.org/modules.php?op=modload&name=News&file=article&sid=911&mode=thread&order=0&thold=0.

226. Network Startup Resource Center (NSRC). n.d. "Connectivity Providers Database." Accessed December 8, 2023. https://nsrc.org/db/lookup/ISO=SD.
227. News.lt. 2002. "Experts: Don't Dismiss Cyberattack Warning." November 20, 2002. https://www.news.lt/IT-News/Experts-Dont-dismiss-cyberattack-warning.im?id=42841&f=c&p=13.
228. News-Medical.Net. 2009. "Fake Internet Drugs Could Be Funding Terrorism." January 29, 2009. https://web.archive.org/web/20090206151022/http://www.news-medical.net/?id=45341.
229. Niufa, Hayaan. 2004. "Mutalabatan Biwaqf Hajb 'iilaf Fi Suria (Arabic)." 'iilaf. October 14, 2004. https://elaph.com/Politics/2004/10/15689.htm.
230. Nua Internet Surveys. 2001. "Crackdown on Cybercafés in Iran." May 15, 2001. https://web.archive.org/web/20050302054135/http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905356762&rel=true.
231. ———. 2002. "Internet Use on the up in Iran." November 6, 2002. https://web.archive.org/web/20050302034512/http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905358529&rel=true.
232. "Official Website of the President of the Islamic Republic of Iran." n.d. Accessed December 3, 2023. https://www.president.ir/en.
233. Okui, Katsuyoshi. 2005. "Causality between Political Freedom and Economic Freedom." https://web.archive.org/web/20070707030109/http://www.pubchoicesoc.org/papers2005/Okui.pdf.
234. OpenNet Initiative. 2004a. "Internet Content Filtering in Iran: Verification of Reported Banned Websites." August 13, 2004. https://web.archive.org/web/20041208071852/http://opennetinitiative.net/bulletins/004/.
235. ———. 2004b. "Internet Filtering in Saudi Arabia in 2004." OpenNet Initiative. 2004. https://opennet.net/studies/saudi.
236. ———. 2005a. "Internet Filtering in Bahrain in 2004-2005: A Country Study." http://www.opennetinitiative.net/studies/bahrain/ONI_Bahrain_Country_Study.pdf.
237. ———. 2005b. "Internet Filtering in the United Arab Emirates in 2004-2005: A Country Study Citation Terms of Use Share Your Story." https://dash.harvard.edu/bitstream/handle/1/2794916/Internet%20Filtering%20in%20the%20UAE.pdf.

238. ———. 2007. “Internet Filtering in Iraq in 2006-2007.” OpenNet Initiative. 2007. https://opennet.net/studies/iraq2007.
239. ———. 2009a. “Internet Filtering in Iran.” https://web.archive.org/web/20090711025755/http://opennet.net/sites/opennet.net/files/ONI_Iran_2009.pdf.
240. ———. 2009b. “Iraq.” August 10, 2009. https://opennet.net/research/profiles/iraq.
241. ———. n.d.-a. “Internet Filtering in Iran in 2004-2005: A Country Study.” *OpenNet Initiative*. Accessed December 4, 2023. https://opennet.net/sites/opennet.net/files/ONI_Country_Study_Iran.pdf.
242. ———. n.d.-b. “Middle East and North Africa.” Accessed December 23, 2023. https://opennet.net/research/regions/mena.
243. ottoman-empire. n.d. “Ottoman-Empire.” Zone-h. Accessed December 11, 2023. http://zone-h.org/archive/defacer=ottoman-empire.
244. Pain, Julien, Cyril Fiévet, Marc-Olivier Peyer, Dan Gillmor, and Mark Glaser. 2005. “Handbook for Bloggers and Cyber-Dissidents.” https://web.archive.org/web/20060221084822/http://www.rsf.org/IMG/pdf/Bloggers_Handbook2.pdf.
245. Palfrey, John G. 2005. “Local Nets: Filtering and the Internet Governance Problem.” In *The Global Flow of Information*, 1–14. https://cyber.harvard.edu/wg_home/uploads/502/13-LocalNetsFiltering.pdf.
246. Parry, Jane, Myles Gorton, Shirley Brown, Graham Titterington, and Craig Skinner. 2003. “Internet Content Filtering A Report to DCITA.” https://web.archive.org/web/20050717150843/http://www.dcita.gov.au/__data/assets/file/10915/Ovum_Report_-_Internet_content_filtering.rtf.
247. Peled, Alon. 2000. “Debunking the Internet Myth: Technological Prophecies and Middle East Politics.” *Middle East Quarterly* 7 (3): 41–54. https://www.meforum.org/71/debunking-the-internet-myth.
248. Persian Journal. 2005a. “Beating the Mullahs’ Block.” October 20, 2005. https://web.archive.org/web/20051204032325/http://www.iranian.ws/iran_news/publish/article_10378.shtml.

249. ———. 2005b. "Iran's Web Censorship among World's Strictest." June 21, 2005. https://web.archive.org/web/20051127143456/http://www.iranian.ws/iran_news/publish/article_7722.shtml.
250. Pitts, Peter J. 2006. "Pharmaceutical Fakery Is Health Care Terrorism." Baltimore Sun. August 15, 2006. https://www.baltimoresun.com/2006/08/15/pharmaceutical-fakery-is-health-care-terrorism/.
251. Poulsen, Kevin. 2003. "US Sponsors Anonymiser – If You Live in Iran." The Register. August 29, 2003. https://www.theregister.com/2003/08/29/us_sponsors_anonymiser_if_you/.
252. PowerDream. n.d. "Www.Arzuffisrl.It Hacked. Notified by PowerDream." Zone-h.Org. Accessed December 11, 2023. http://zone-h.org/mirror/id/7137962.
253. Preatoni, Roberto. 2009. "Army Mil and NATO Parliament Hacked by Turks." Zone-h. January 8, 2009. http://zone-h.org/news/id/4706.
254. Preatoni, Roberto (SyS64738). 2006a. "Electronic Jihad." Zone-h. October 6, 2006. http://www.zone-h.org/news/id/4481.
255. ———. 2006b. "New Defacements' Messages Threatening the Pope." Zone-h. September 28, 2006. http://www.zone-h.org/news/id/4472.
256. "Presidency of The Islamic Republic of Iran." n.d. Accessed December 3, 2023. https://web.archive.org/web/20080926041853/http://un.president.ir/en/.
257. "Presidency of the Republic of Lebanon." n.d. Accessed December 3, 2023. http://www.presidency.gov.lb/.
258. "President Ali Abdullah Saleh - Yemen." n.d. Accessed December 3, 2023. https://web.archive.org/web/20060107002604/http://www.presidentsaleh.gov.ye/.
259. "President de La Republique." n.d. Accessed December 3, 2023. https://web.archive.org/web/20010926043110/http://www.elmouradia.dz/.
260. "Prince Faisal." n.d. Accessed December 3, 2023. https://web.archive.org/web/20080222055047/http://www.princefaisalbinsultan.com/.
261. Privacy International and the GreenNet Educational Trust. 2003. "Silenced: An International Report on Censorship and Control on the Internet." https://web.archive.org/web/20050319235927/http://pi.gn.apc.org/survey/censorship/Silenced.pdf.

262. "ProxyTools Download." n.d. SourceForge.Net. Accessed November 24, 2023. https://sourceforge.net/projects/proxytools/.
263. "Psiphon." n.d. Accessed November 24, 2023. http://www.citizenlab.org/.
264. Qusti, Riad. 2003. "Internet Regulations Tightened." Arab News. July 6, 2003. https://web.archive.org/web/20060203021740/http://www.arabnews.com/?page=1&section=0&article=28447&d=6&m=7&y=2003.
265. Qutsi, Raid. 2003. "Internet Regulations Tightened." Arab News. July 6, 2003. https://web.archive.org/web/20030721013906/https://www.arabnews.com/?page=1&section=0&article=28447&d=6&m=7&y=2003.
266. Radding, Alan. 2004. "Content Filtering: Monitoring and Measuring Web Use Delivers Productivity Payback." Karlsruhe. https://web.archive.org/web/20051226215818/http://www.astaro.com/content/download/157/726/file/Whitepaper_Content_Filtering_en.pdf.
267. Rantanen, Miska. 2007. "Virtual Harassment, but for Real." Helsingin Sanomat. May 16, 2007. https://web.archive.org/web/20070516180907/http://www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868.
268. Rashid, Tariq. 2004. "Kayfiat Alraqabat Ealaa Alaintirnit .. Alshakal Alealamiu Qadiat Fard Raqabat Ealaa al'iintirnit Tueadu Mathar Jadal (Arabic)." Al-Jazirah Corporation. April 18, 2004. https://www.al-jazirah.com/digimag/18042004/por33.htm.
269. Reporters Without Borders. 2002a. "Cyber-Dissident Jailed for 18 Months." Reporters Without Borders. May 16, 2002. https://rsf.org/en/cyber-dissident-jailed-18-months.
270. ———. 2002b. "Cyber-Dissident Pardoned by King Abdullah." Reporters Without Borders. June 28, 2002. https://rsf.org/en/cyber-dissident-pardoned-king-abdullah.
271. ———. 2003. "Cyber-Dissident Zouhair Yahyaoui Freed after 18 Months in Jail." November 18, 2003. https://rsf.org/en/cyber-dissident-zouhair-yahyaoui-freed-after-18-months-jail.

272. ———. 2004a. "Internet - Iran." Reporters Without Borders. 2004. https://web.archive.org/web/20040710210636/http://www.rsf.org/article.php3?id_article=10733.
273. ———. 2004b. "Internet - Tunisia." Reporters Without Borders. 2004. https://web.archive.org/web/20051126211346/http://www.rsf.org/article.php3?id_article=10768.
274. ———. 2004c. "Internet Under Surveillance 2004 - Saudi Arabia." 2004. https://www.refworld.org/docid/46e69192c.html.
275. ———. 2004d. "Journalist Nabil Fayad Freed after Being Held for 33 Days without Charge." November 8, 2004. https://rsf.org/en/journalist-nabil-fayad-freed-after-being-held-33-days-without-charge.
276. ———. 2004e. "New Attacks on Internet Freedom Deplored." August 28, 2004. https://web.archive.org/web/20060116054031/http://www.rsf.org/article.php3?id_article=11275.
277. ———. 2004f. "Reporters Without Borders Calls for Full Investigation into Assault on Sihem Bensedrine." January 9, 2004. https://web.archive.org/web/20040224012847/http://www.rsf.org/article.php3?id_article=9009.
278. ———. 2004g. "Three Internet-Users Sentenced to Prison Terms of Two to Four Years." July 26, 2004. https://rsf.org/en/three-internet-users-sentenced-prison-terms-two-four-years.
279. ———. 2005a. "Courageous Young Cyber-Dissident Dies of Heart Attack." March 14, 2005. https://rsf.org/en/courageous-young-cyber-dissident-dies-heart-attack.
280. ———. 2005b. "Internet Writer Al Mansouri Gets 18-Month Prison Sentence." November 7, 2005. https://rsf.org/en/internet-writer-al-mansouri-gets-18-month-prison-sentence.
281. ———. 2005c. "Release of Cyberjournalist Mojtaba Lotfi and Blogger Mohamad Reza Nasab Abdolahi." August 29, 2005. https://web.archive.org/web/20060116204137/http://www.rsf.org/article.php3?id_article=14807.

282. ———. 2005d. "Reporters Without Borders Calls for End to Blocking of News Website." December 5, 2005. https://rsf.org/en/reporters-without-borders-calls-end-blocking-news-website.

283. ———. 2005e. "Reporters Without Borders Denounces Press Freedom Threat in Website Registration." April 26, 2005. https://rsf.org/en/reporters-without-borders-denounces-press-freedom-threat-website-registration.

284. ———. 2005f. "Tehran Seeking New Ways to Censor the Internet and Track Dissidents." October 18, 2005. https://web.archive.org/web/20051027170937/http://www.rsf.org/article.php3?id_article=15343.

285. ———. 2005g. "The 15 Enemies of the Internet and Other Countries to Watch." November 17, 2005. https://rsf.org/en/15-enemies-internet-and-other-countries-watch.

286. ———. 2005h. "Two More Online Forum Moderators Arrested." February 28, 2005. https://web.archive.org/web/20050308032905/http://www.rsf.org/article.php3?id_article=12687.

287. ———. 2006. "Massoud Hamid, Winner of 2005 Reporters Without Borders Internet Freedom Prize, Released at End of Prison Sentence." July 25, 2006. https://rsf.org/en/massoud-hamid-winner-2005-reporters-without-borders-internet-freedom-prize-released-end-prison.

288. ———. 2007. "More than 100 Websites Blocked in Growing Wave of Online Censorship." December 7, 2007. https://web.archive.org/web/20080213122206/http://www.rsf.org/article.php3?id_article=24671.

289. ———. 2008a. "Annual Report 2008 - Egypt." February 13, 2008. https://www.refworld.org/publisher,RSF,ANNUALREPORT,EGY,47b418d525,0.html.

290. ———. 2008b. "Iran." Reporters Without Borders. February 7, 2008. https://web.archive.org/web/20100819090827/http://en.rsf.org/iran-iran-07-02-2008,25431.

291. ———. 2008c. "List of the 13 Internet Enemies 2008: Iran." 2008. https://web.archive.org/web/20080922182756/http://www.rsf.org/article.php3?id_article=26154&Valider=OK.

292. ———. 2008d. "YouTube Censored yet Again by Another Court Order Blocking Access." November 25, 2008. https://web.archive.org/web/20090214025241/http://www.rsf.org/article.php3?id_article=29421.
293. ———. n.d.-a. "Internet - United Arab Emirates." Accessed December 19, 2023. https://web.archive.org/web/20041014014751/http://www.rsf.org/article.php3?id_article=10769.
294. ———. n.d.-b. "Internet Enemies: Iran." Reporters Without Borders. Accessed December 3, 2023. https://web.archive.org/web/20080922182756/http://www.rsf.org/article.php3?id_article=26154&Valider=OK.
295. ———. n.d.-c. "World Press Freedom." Accessed November 27, 2023. https://rsf.org/en/index.
296. Reuters. 2008. "Hamas Bans Pornographic Websites in Gaza Strip." May 19, 2008. https://www.reuters.com/article/idUSL1920867720080519/.
297. "Riasat Aljumhuriat Altuwnisia (Arabic)." n.d. Accessed December 3, 2023. https://www.carthage.tn/ar/index.php.
298. Rinnawi, Khalil. n.d. "The Internet and the Arab World as a Virtual Public Sphere." Accessed November 25, 2023. https://web.archive.org/web/20040808143637/http://burdacenter.bgu.ac.il/publications/finalReports2001-2002/Rinnawi.pdf.
299. Rjiba, Neziha. 2008. "Kalima Website Targeted; Police Attack OLPEC Secretary General - IFEX." IFEX. October 14, 2008. https://ifex.org/kalima-website-targeted-police-attack-olpec-secretary-general/.
300. Rohozinski, Rafal. n.d. "'Secret Agents' and 'Undercover Brothers': The Hidden Information Revolution in the Arab World." Accessed November 24, 2023. https://web.archive.org/web/20050818043551/https://www.ssrc.org/programs/itic/publications/ITST_materials/rohozinskibrief3_4.pdf.
301. Rubin, Michael. 2019. "Evolution of Iranian Surveillance Strategies Toward the Internet and Social Media." The Institute for Policy, Advocacy, and Governance. December 10, 2019. https://www.aei.org/articles/evolution-of-iranian-surveillance-strategies-toward-the-internet-and-social-media/.

302. Saleh, Nivien. 2003. "Transforming the Political Elite through New Technologies: The Case of Egypt." *New Media and Information Technology Working Papers*. https://web.archive.org/web/20040222023538/http://nmit.georgetown.edu/papers/saleh.htm.
303. "Saudiwoman's Weblog." n.d. Accessed December 4, 2023. https://web.archive.org/web/20080803000802/http://saudiwoman.wordpress.com/.
304. Sayd Alfawayid. n.d. "Risalat Min Eashiq Lilsuwar Aljinsiat 'iilaa Mawqie Sayd Alfawayid (Arabic)." Accessed December 2, 2023. http://saaid.org/gesah/58.htm.
305. Scambray, Joel., Mike. Shema, and Caleb. Sima. 2006. "Hacking Exposed : Web Applications," 520. https://dl.acm.org/doi/book/10.5555/1146340.
306. Scullion, Aaron. 2003a. "Iranian Bloggers Rally against Censorship." BBC News. December 11, 2003. http://news.bbc.co.uk/2/hi/technology/3310493.stm.
307. ———. 2003b. "Iran's President Defends Web Control." BBC News. December 12, 2003. http://news.bbc.co.uk/2/hi/technology/3312841.stm.
308. ———. 2003c. "Iran's President Defends Web Control." BBC News. December 12, 2003. http://news.bbc.co.uk/2/hi/technology/3312841.stm.
309. Sedarat, Firouz. 2003. "Iran Internet Use at Risk from Conservatives." 16beaver. June 18, 2003. https://web.archive.org/web/20060618174842/http://www.16beavergroup.org/mtarchive/archives/000228.php.
310. Sedgwick, Mark. 1998. "Marginal Muslims in Cyberspace." In *The Fourth Nordic Conference on Middle Eastern Studies: The Middle East in Globalizing World*. Oslo. https://web.archive.org/web/20001212154600/http://www.hf.uib.no/smi/pao/sedgwick.html.
311. "Service d'assistance Aux Centres Publics d'Internet En Tunisie." 1998. December 10, 1998. https://web.archive.org/web/20010221233607/http://www.sospublinet.tn/cahier.htm.
312. Shabakat alfaysal nit. 2008. "Hakarz Magharibat Yakhtariqun Mawaqie Jazayiriatan Rafdan Liaistimrar Ghalq Alhudud (Arabic)." November 14, 2008. https://web.archive.org/web/20090221212640/http://www.fesal.net/news-action-show-id-2386.htm.

313. Shabakat Allaadiniiyn Alearab. 2004. "Hajb Mawqie Alakhawan Almuslimin Fi Misr (Arabic)." October 5, 2004. https://web.archive.org/web/20050207181420/http://www.ladeeni.net/pn/Article124.html.
314. Sims, Michael. 1998. "Why Filters Can't Work." The Censorware Project. August 3, 1998. https://www.spectacle.org/cs/sims.html.
315. Singh, Nihal S. 2000. "Dilemmas of a Free Media." Al-Bab.Com. February 2000. https://al-bab.com/dilemmas-free-media.
316. Sodomylaws.org. 2007. "Egypt." April 14, 2007. https://web.archive.org/web/20100404033045/http://www.sodomylaws.org/world/egypt/egypt.htm.
317. SourceForge.net. n.d. "The Six/Four System." Accessed November 24, 2023. https://sourceforge.net/projects/sixfour/.
318. Southwell, Matthew. 2004. "Evolving Emirates." The Information & Technology Publishing Co. Ltd. January 25, 2004. http://www.itp.net/features/print.php?id=1644.
319. Spigelman, Shai-Lee. n.d. "Islam and Internet: The Correlation Between Islamic Religion and Internet Diffusion." Accessed November 24, 2023. https://web.archive.org/web/20020107045611/http://www.ksg.harvard.edu/iip/stp305/Fall2000/spigelman.PDF.
320. Stensgaard, Anne-Birte. 2005. "E-Commerce Reaches New Highs in the Middle East." AME Info. May 31, 2005. https://web.archive.org/web/20060111060741/http://www.ameinfo.com/61444.html.
321. Stop Censoring Us. 2004a. "Blacklist, Latest Version." June 16, 2004. https://web.archive.org/web/20040617041532/http://stop.censoring.us/archives/011038..php.
322. ———. 2004b. "Cyber Crime Law to Be Finalized." November 22, 2004. https://web.archive.org/web/20041209073330/http://stop.censoring.us/archives/012852.php.
323. ———. 2005a. "Blogosphere 'Attacked.'" August 13, 2005. https://web.archive.org/web/20051229144437/http://stop.censoring.us/archives/014408.php.

324. ———. 2005b. “Different Law Needed for Blogs.” January 19, 2005. https://web.archive.org/web/20050211221417/http://stop.censoring.us/archives/013218.php.
325. ———. 2005c. “Mortazavi Defends Unilateral Filtering of ‘immoral and Sacrilegious’ Websites.” Stop Censoring Us. January 14, 2005. https://web.archive.org/web/20050211215742/http://stop.censoring.us/archives/013181.php.
326. SyriaLive.net. 2002. “Syrian Internet Installation and Subscription Rates to Be Scrapped.” March 5, 2002. http://www.syrialive.net/computer/archive/computer_2002.htm.
327. “Syrian Arab News Agency (SANA).” n.d. Accessed December 3, 2023. https://web.archive.org/web/20080731120618/http://sana.sy/eng/article/5.htm.
328. Tait, Robert. 2006. “Censorship Fears Rise as Iran Blocks Access to Top Websites.” The Guardian. December 4, 2006. https://www.theguardian.com/technology/2006/dec/04/news.iran.
329. “Talk: Psiphon/Archive 1.” n.d. Wikiwand. Accessed November 24, 2023. https://www.wikiwand.com/en/Talk:Psiphon/Archive_1.
330. !TeAm RaBaT-SaLe! n.d.-a. “Crazymirc.Com Hacked. Notified by !TeAm RaBaT-SaLe!” Zone-h.Org. Accessed December 10, 2023. http://zone-h.org/mirror/id/9029421.
331. ———. n.d.-b. “Www.Arabwatercouncil.Org Hacked. Notified by !TeAm RaBaT-SaLe!” Zone-h.Org. Accessed December 10, 2023. http://zone-h.org/mirror/id/9257886.
332. The Arabic Network for Human Rights Information. n.d.-a. “Jordan A Ray of Light.” Accessed November 30, 2023. https://web.archive.org/web/20040712091349/http://www.hrinfo.net/en/reports/net2004/jordan.shtml.
333. ———. n.d.-b. “Libya: The Internet in a Conflict Zone.” Accessed December 14, 2023. https://web.archive.org/web/20061010062947/http://www.hrinfo.net/en/reports/net2004/libya.shtml.
334. ———. n.d.-c. “The Internet In the Arab World: A New Space of Repression?” Accessed November 24, 2023. https://web.archive.org/web/20040806080704/http://www.hrinfo.net/en/reports/net2004/intro.shtml.

335. ———. n.d.-d. "The Internet In the Arab World: A New Space of Repression? - Qatar A Step Forward." The Arabic Network for Human Rights Information. Accessed November 30, 2023. https://web.archive.org/web/20040712091317/http://www.hrinfo.net/en/reports/net2004/qatar.shtml.
336. ———. n.d.-e. "The Internet In the Arab World: A New Space of Repression? - Syria Internet under Siege." The Arabic Network for Human Rights Information. Accessed December 2, 2023. https://web.archive.org/web/20040712091326/http://www.hrinfo.net/en/reports/net2004/syria.shtml.
337. ———. n.d.-f. "United Arab Emirates The Best, But . . ." Accessed December 19, 2023. https://web.archive.org/web/20040712091046/http://www.hrinfo.net/en/reports/net2004/uae.shtml.
338. "The Current Status of the Internet in the Arab World." n.d. Accessed November 24, 2023. https://web.archive.org/web/20000511174312/http://www.library.cornell.edu/colldev/mideast/nusacci.htm.
339. "The Egyptian Presidency." n.d. Accessed December 3, 2023. https://web.archive.org/web/20040602044835/http://www.presidency.gov.eg/.
340. The Estimate. 1998. "The Internet in the Arab World: An Update as the Saudis Go Online," December. https://web.archive.org/web/19991123211653/http://www.theestimate.com/public/121898.html.
341. The Guardian. 2001. "US Pulls the Plug on Muslim Websites." September 10, 2001. https://www.theguardian.com/technology/2001/sep/10/internetnews.worlddispatch.
342. The Hacktivist. 2003. "Testing Indicates Iranian Censorship." August 28, 2003. https://web.archive.org/web/20031024074622/http://www.thehacktivist.com/modules.php?op=modload&name=News&file=article&sid=274&mode=thread&order=0&thold=0.
343. The International Telecommunication Union (ITU). n.d. "Internet in Sudan." Accessed December 8, 2023. https://web.archive.org/web/20031217150240/https://www.itu.int/arabinternet2001/documents/pdf/document26.pdf.

344. The Internet Corporation for Assigned Names and Numbers (IANA). 2002a. "IANA Report on Redelegation of the .Sd Top-Level Domain." December 20, 2002. https://www.iana.org/reports/2002/sd-report-20dec02.html.
345. ———. 2002b. "Letter from E-Zubeir Besher Taha to Yassir Elamin." The Internet Corporation for Assigned Names and Numbers (IANA). March 23, 2002. https://www.iana.org/reports/2002/sd-redelegation/taha-to-elamin-23mar02.html.
346. The Investigative Project on Terrorism. 2008. "Former IAP President Indicted For Naturalization Fraud." January 30, 2008. https://www.investigativeproject.org/593/former-iap-president-indicted-for-naturalization-fraud.
347. The Middle East Media Research Institute (MEMRI). 2006. "Islamist Website Presents First Issue of Technical Mujahid Magazine." November 30, 2006. https://www.memri.org/reports/islamist-websites-monitor-no-29.
348. ———. 2008. "Al-Azhar Fatwa: Hacking U.S., Israeli Websites Is Permissible as Part of Electronic Jihad." August 29, 2008. https://www.memri.org/reports/al-azhar-fatwa-hacking-us-israeli-websites-permissible-part-electronic-jihad.
349. "The Office of King Hussein I of Jordan." n.d. Accessed December 3, 2023. http://www.kinghussein.gov.jo/office.html.
350. "The Office of the Supreme Leader." n.d. Accessed December 3, 2023. https://www.leader.ir/en.
351. The Open Research Network. 1999. "Iran's Telecom and Internet Sector: A Comprehensive Survey." 1999. https://web.archive.org/web/20010208202847/http://www.science-arts.org/internet/internet.html.
352. TheHacktivist. 2003. "Anti-Censorship and Incorrect Data." November 4, 2003. https://web.archive.org/web/20041126075225/http://www.thehacktivist.com/modules.php?op=modload&name=News&file=article&sid=338.
353. Tolbert, Caroline, Karen Mossberger, and Ramona Mcneal. 2002. "Beyond the Digital Divide: Exploring Attitudes about Information Technology, Political Participation, and Electronic Government." In , 1–44. Boston, Massachusetts: American Political Science Associaton. https://web.archive.org/web/20031215113054/http://fs.huntingdon.edu/jlewis/FOIA/eGov/McNeal-RamoAPSA02ppr.pdf.

354. Too Huge World. 2008. "Youtube Blocked." July 27, 2008. https://web.archive.org/web/20080925200029/http://toohugeworld.wordpress.com/2008/07/27/youtube-blocked/.
355. Tucker, Diane. 2009. "Arab Women Beginning To Crack The Glass Ceiling." HuffPost The World Post. April 17, 2009. https://www.huffpost.com/entry/arab-women-beginning-to-c_b_176137.
356. Tung, Liam. 2008. "Jihadists Get World-Class Encryption Kit." ZDNET. January 28, 2008. https://www.zdnet.com/article/jihadists-get-world-class-encryption-kit/.
357. "Un Blogueur et Un Propriétaire de Café Internet Condamnés à de La Prison Ferme." 2009. December 15, 2009. https://web.archive.org/web/20100328072638/http://www.rsf.org/spip.php?page=article&id_article=35346.
358. UNESCO. 2000. "Only 4% of Internet Users in the Arab World Are Women." June 5, 2000. https://web.archive.org/web/20010421035040/http://www.unesco.org/webworld/news/000605_beijing.shtml.
359. "Unintended Risks and Consequences of Circumvention Technologies: The IBB's Anonymizer Service in Iran." 2004. OpenNet Initiative. May 5, 2004. https://opennet.net/advisories/001/.
360. United Nations. 2010. "World E-Government Rankings." https://web.archive.org/web/20101214051536/http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan038848.pdf.
361. vigilant tv. 2002. "UAE Minister Calls for End to Internet Censorship." October 14, 2002. https://web.archive.org/web/20050126130236/http://vigilant.tv/article/2332/uae-minister-calls-for-end-to-internet-censorship.
362. Wallace, Jonathan. 1998. "What Censorware Means to Me." *The Ethical Spectacle* 4 (4). https://www.spectacle.org/cs/means.html.
363. Walters, Timothy N., and Lynne Masel Walters. 2002. "Cyberspace and the United Arab Emirates: Searching for Tunes in the Air." Georgetown University. August 2002. https://web.archive.org/web/20030220002011/http://nmit.georgetown.edu/papers/walterstl.htm.

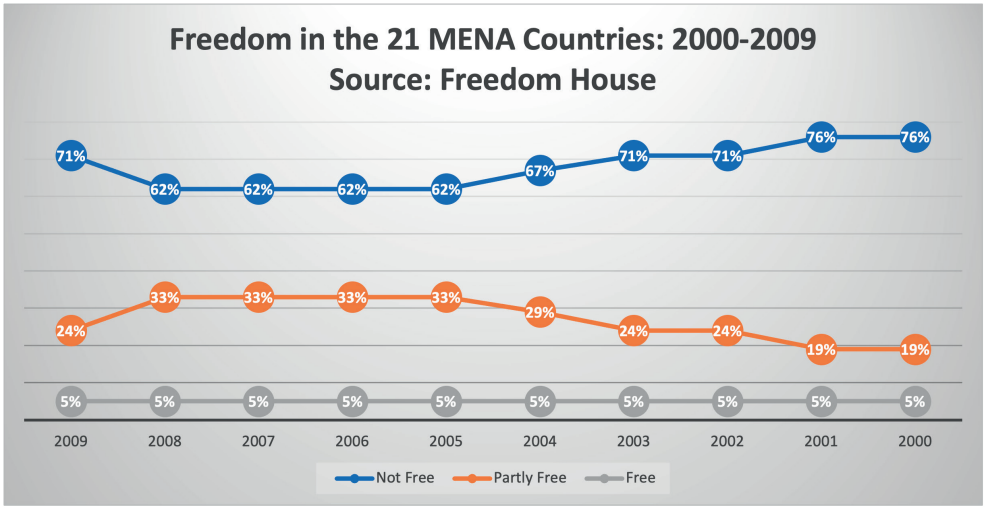
364. Wayne. n.d. “Waynes Proxy Censorship Avoidance Site - UAE, KSA and Others.” Accessed November 24, 2023. https://www.angelfire.com/wy/waynes/.
365. “Web Filtering Appliances Heat Up the Hardware vs. Software Debate.” 2005.
366. Wheeler, Deborah. 2001. “Islam, Technology and Community.” *The Journal for Education, Community and Values: Interface on the Internet*, October. https://web.archive.org/web/20020812152523/http://bcis.pacificu.edu/journal/2001/10/wheeler.php.
367. Wheeler, Deborah L. 2004. “The Internet in the Arab World: Digital Divides and Cultural Connections.” Royal Institute for Inter-Faith Studies. June 16, 2004. https://www.mafhoum.com/press8/internet.htm.
368. Whitaker, Brian. 2000. “Saudis Claim Victory in War for Control of Web.” Arab Media. May 11, 2000. https://web.archive.org/web/20020615033645/http://www.al-bab.com/media/articles/saudi000511.htm.
369. ———. 2003. “Censor Sensibility.” The Guardian. May 19, 2003. https://www.theguardian.com/technology/2003/may/19/comment.worlddispatch.
370. “Why Block by IP Address?” 2005. CitizenLab. February 14, 2005. https://web.archive.org/web/20050419225559/http://ice.citizenlab.org/?p=78.
371. “Yaaddaasht Haaye Shakhsi Ahmadi Nejhaad (Persian).” n.d. Accessed December 3, 2023. https://web.archive.org/web/20060814213854/http://www.ahmadinejad.ir/.
372. Ynet. 2006. “Muhammad’s Cartoons: The Storm Goes Online.” February 9, 2006. https://www.ynet.co.il/articles/1,7340,L-3213102,00.html.
373. Zaharov-Reutt, Alex. 2007. “Shock: Is YouTube Cooked in Turkey?” ITWire. March 8, 2007. https://web.archive.org/web/20090221001502/http://www.itwire.com/content/view/10258/53/.
374. Zaman alwasl. 2008. “Altadmir Walqatla.. Aftradyaan ... Dianan Muqalad (Arabic).” October 14, 2008. https://www.zamanalwsl.net/news/article/7254.
375. Zarqawi, Nihad. 2008. “Aikhtiraq Mawaqie Asarayiyliat Min Qibal Majmueat Hakirz Turkia (Arabic).” Banurama. January 12, 2008. https://web.archive.org/web/20080204121909/http://www.panet.co.il/online/articles/11/13/S-102339,11,13.html.

376. Zenklo, Khaled. 2003. "Suria 'Tahasiru' Albarid Alalkitruniu Warasayiluh (Arabic)." Alhayaa. November 13, 2003. https://web.archive.org/web/20040704160554/http://www.mafhoum.com/press6/169T42.htm.
377. Zittrain, Jonathan, and Benjamin Edelman. 2002. "Documentation of Internet Filtering in Saudi Arabia." Berkman Center for Internet & Society. September 12, 2002. https://cyber.harvard.edu/filtering/saudiarabia/.
378. Zittrain, Jonathan, and John Palfrey. n.d. "Internet Filtering: The Politics and Mechanisms of Control." In , 1–28. Accessed November 23, 2023. http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-2.pdf.
379. Zuckerman, Ethan. 2005. "A Technical Guide to Anonymous Blogging – a Very Early Draft." Global Voices. April 13, 2005. https://globalvoices.org/2005/04/13/a-technical-guide-to-anonymous-blogging-a-very-early-draft/.

Appendix A1 – Freedom House, "Freedom in the World Index" - States (Freedom House 2023)

Country	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	Total
Algeria	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Bahrain	NF	NF	PF	PF	PF	PF	PF	PF	PF	NF	30% NF, 70% PF
Egypt	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Iran	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Iraq	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Israel	Free	Free	Free	Free	Free	Free	Free	Free	Free	Free	100% Free
Israeli-Occupied Territories	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Jordan	PF	PF	PF	PF	PF	PF	PF	PF	PF	PF	100% PF
Kuwait	PF	PF	PF	PF	PF	PF	PF	PF	PF	PF	100% PF
Lebanon	NF	NF	NF	NF	NF	PF	PF	PF	PF	PF	50%NF, 50%PF
Libya	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Morocco	PF	PF	PF	PF	PF	PF	PF	PF	PF	PF	100% PF
Oman	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Qatar	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Saudi Arabia	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Sudan	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Syria	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Tunisia	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Turkey	PF	PF	PF	PF	PF	PF	PF	PF	PF	PF	100% PF
United Arab Emirates	NF	NF	NF	NF	NF	NF	NF	NF	NF	NF	100% NF
Yemen	NF	NF	NF	NF	PF	PF	PF	PF	PF	NF	50%NF, 50%PF
Not Free	16 (76%)	16 (76%)	15 (71%)	15 (71%)	14 (67%)	13 (62%)	13 (62%)	13 (62%)	13 (62%)	15 (71%)	**14.3 (68%)**
Partially Free	4 (19%)	4 (19%)	5 (24%)	5 (24%)	6 (29%)	7 (33%)	7 (33%)	7 (33%)	7 (33%)	5 (24%)	**5.7 (27%)**
Free	1 (5%)	1 (5%)	1 (5%)	1 (5%)	1 (5%)	1 (5%)	1 (5%)	1 (5%)	1 (5%)	1 (5%)	**1 (5%)**

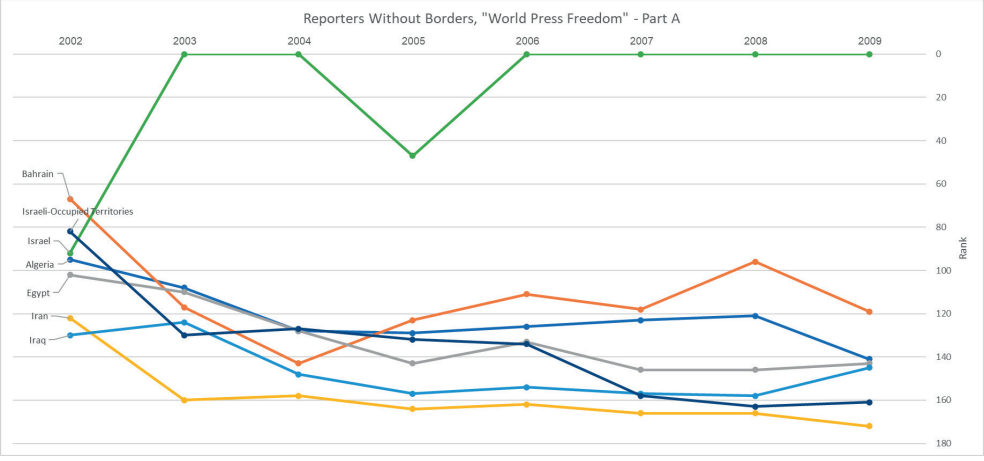
Appendix A2 – Freedom House, "Freedom in the World Index" - Trends 'Freedom in the World' (n 359).



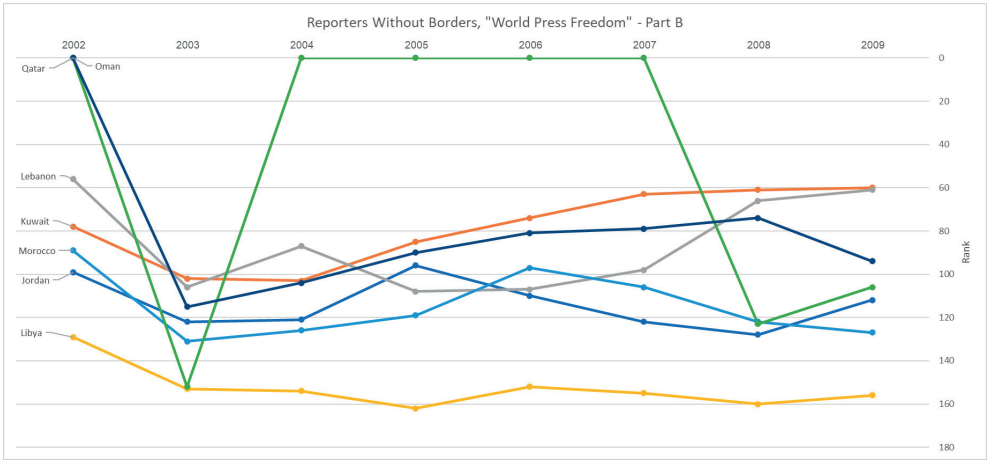
Appendix B1 – Reporters Without Borders, "World Press Freedom"(Reporters Without Borders, n.d.-c)

Country	2002	2003	2004	2005	2006	2007	2008	2009
Algeria	95	108	128	129	126	123	121	141
Bahrain	67	117	143	123	111	118	96	119
Egypt	102	110	128	143	133	146	146	143
Iran	122	160	158	164	162	166	166	172
Iraq	130	124	148	157	154	157	158	145
Israel	92	-	-	47	-	-	-	-
Israeli-Occupied Territories	82	130	127	132	134	158	163	161
Jordan	99	122	121	96	110	122	128	112
Kuwait	78	102	103	85	74	63	61	60
Lebanon	56	106	87	108	107	98	66	61
Libya	129	153	154	162	152	155	160	156
Morocco	89	131	126	119	97	106	122	127
Oman	-	152	-	-	-	-	123	106
Qatar	-	115	104	90	81	79	74	94
Saudi Arabia	125	156	159	154	161	148	161	163
Sudan	105	142	132	133	139	140	135	148
Syria	126	155	155	145	153	154	159	165
Tunisia	128	149	152	147	148	145	143	154
Turkey	100	115	113	98	100	101	102	122
United Arab Emirates	-	122	137	100	77	65	69	86
Yemen	103	136	135	136	150	143	155	167
Total Countries	139	166	167	167	168	169	173	175

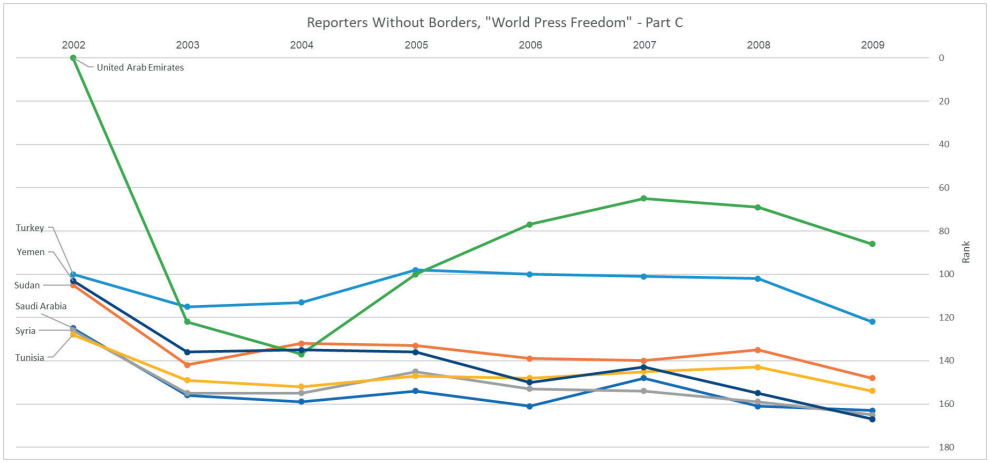
Appendix B2 – Reporters Without Borders, "World Press Freedom" – Part A



Appendix B3 – Reporters Without Borders, "World Press Freedom" – Part B



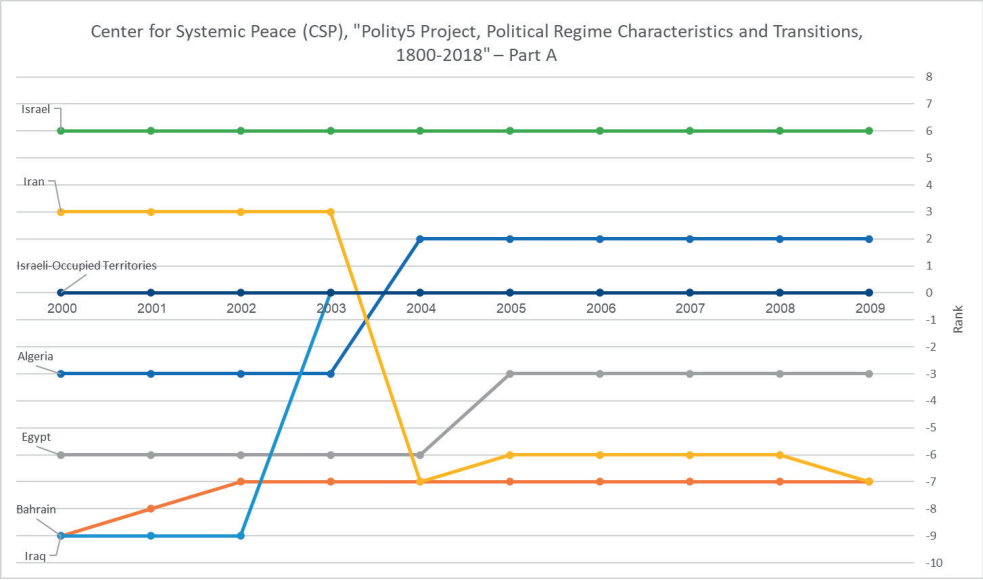
Appendix B4 – Reporters Without Borders, "World Press Freedom" – Part C



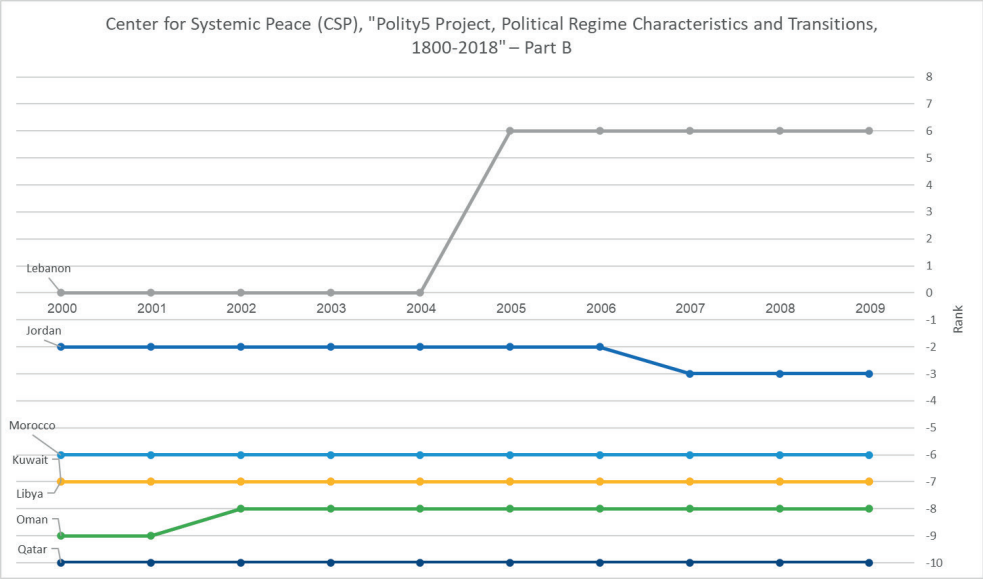
Appendix C1 – Center for Systemic Peace (CSP), "Polity5 Project, Political Regime Characteristics and Transitions, 1800-2018"(Center for Systemic Peace (CSP), n.d.)

	2009	2008	2007	2006	2005	2004	2003	2002	2001	2000
Algeria	2	2	2	2	2	2	-3	-3	-3	-3
Bahrain	-7	-7	-7	-7	-7	-7	-7	-7	-8	-9
Egypt	-3	-3	-3	-3	-3	-6	-6	-6	-6	-6
Iran	-7	-6	-6	-6	-6	-7	3	3	3	3
Iraq	NA	NA	NA	NA	NA	NA	NA	-9	-9	-9
Israel	6	6	6	6	6	6	6	6	6	6
Israeli-Occupied Territories	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Jordan	-3	-3	-3	-2	-2	-2	-2	-2	-2	-2
Kuwait	-7	-7	-7	-7	-7	-7	-7	-7	-7	-7
Lebanon	6	6	6	6	6	NA	NA	NA	NA	NA
Libya	-7	-7	-7	-7	-7	-7	-7	-7	-7	-7
Morocco	-6	-6	-6	-6	-6	-6	-6	-6	-6	-6
Oman	-8	-8	-8	-8	-8	-8	-8	-8	-9	-9
Qatar	-10	-10	-10	-10	-10	-10	-10	-10	-10	-10
Saudi Arabia	-10	-10	-10	-10	-10	-10	-10	-10	-10	-10
Sudan	-3	-3	-3	-3	-3	-6	-6	-6	-6	-6
Syria	-6	-6	-6	-6	-6	-6	-6	-6	-6	-6
Tunisia	-4	-4	-4	-4	-4	-4	-4	-4	-3	-3
Turkey	7	7	7	7	7	7	7	7	7	7
United Arab Emirates	-8	-8	-8	-8	-8	-8	-8	-8	-8	-8
Yemen	-2	-2	-2	-2	-2	-2	-2	-2	-2	-2

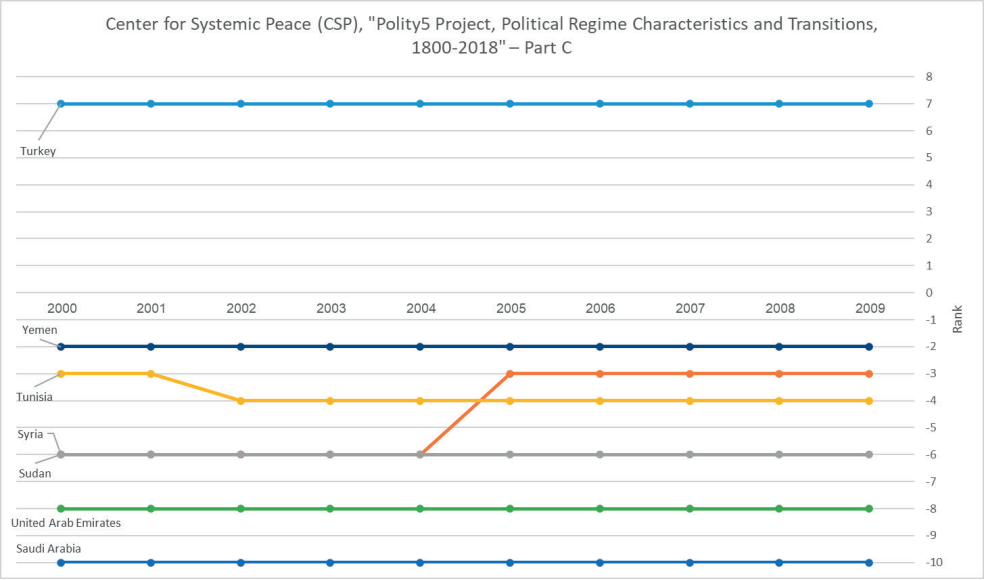
Appendix C2 – Center for Systemic Peace (CSP), "Polity5 Project, Political Regime Characteristics and Transitions, 1800-2018" – Part A



Appendix C3 – Center for Systemic Peace (CSP), "Polity5 Project, Political Regime Characteristics and Transitions, 1800-2018" – Part B



Appendix C4 – Center for Systemic Peace (CSP), "Polity5 Project, Political Regime Characteristics and Transitions, 1800-2018" – Part C



REVIEWS

Ilin Savov Ph.D.

Digital technologies proliferated rapidly in the late 20th and early 21st centuries, revolutionizing how people interact with the outside world, communicate, and obtain information. Particularly the Internet has shown to be a potent instrument for democratizing information access, promoting international connections, and amplifying a variety of viewpoints beyond national boundaries.

Ideals like freedom of expression, creativity, and openness are embodied by the Internet, a symbol of the information revolution. On the other hand, the Middle East and North Africa (MENA) region is frequently associated with bureaucratic institutions and traditionalism, which can impede the exercise of free expression and human rights. But these broad generalizations fall short of encapsulating the complexity of the region. The Internet has been crucial in influencing narratives in the MENA area, where historical legacies, religious traditions, and political difficulties collide.

Based of my experience on the field of defense of national security knowledge workers would greatly benefit from the insights and tools that are produced by ongoing academic study. Dr. Tal Pavel recently published book, "The Internet in the Middle East and North Africa: A Study of Usage, Threats and Restrictions during the First Decade of the 21st Century" is an excellent illustration of this kind of study and a successful strategy for promoting both immediate use and more study on the field of communications.

The goal of the scientific book is to give a thorough understanding of the technology advancements, cultural dynamics, historical background, and governance issues that have influenced the development of the digital ecosystem in the Middle East and North Africa. This book attempts to provide a comprehensive knowledge of the opportunities, hazards, and ramifications of the digital revolution in

one of the most dynamic and diverse regions of the globe by exploring the intricacies and subtleties of Internet usage in the MENA region.

Science is a never-ending quest for knowledge, and it will never stop learning by depending on research that has provided as much as has been possible at some point in certain circumstances. In this regard, I believe it is about intriguing subjects and works, and the book`s publication will serve as a catalyst for the academic community`s further efforts.

As a result, I advise for publication of the scientific book that will be a great benefit for university teachers, researchers, students and practitioners.

George-Marius Șinca Ph.D.

In a historical perspective, the author is describing granularly the digital revolution that appeared in the Middle East and North Africa since the very beginning, since the Internet arrived in the MENA region in the early 1990's and the immediate period of time in the following decade. In the same time, the statistical comparison made between MENA and Western countries is very exact, describing in an objective perspective the process of growth and the moment of cyber maturity for different countries and regions based on cultural and geographical opportunities and limitations.

The author's is going further in researching inductively the progress of internet as a resource in the area, by highlighting the infrastructure development, governmental e-Services, e-Commerce and Leadership Involvement.

The resources used in this research, as are the international organisms and organizations empowers the results by giving a verified perspective on the topic of internet usage, threats and restrictions during the first decade of the 21st century in Middle East and North Africa. This book remains as a empiric global analysis of the usage of the internet; here we can observe the segregations of the internet in four areas, as follows: governmental entities, public institutions, public organizations and civil society where the communications came first as restrictive as it was possible, later after the year 2000, the access was granted for almost everyone with fewer restrictions or limitations.

In conclusion, the SWOT analysis is speaking by itself about the Internet's unique characteristics presented a double-edged sword for governments, demanding a severe and cautious approach - as a communication tool, it offered a range of strengths, weaknesses, opportunities, and threats.

Even if the book through the research is offering a good understanding of the Internet's complex role in the Middle East and North Africa, one of the studies that could be related, as a compared study, is an analysis of Internet's role in MENA and Europe in the same period of time.

The motivation of the author's regarding the future research directions is very well chosen – self-censorship on websites is one of nowadays struggle around the globe as is the content analysis. Other possible directions as are the gender, language, and culture, citizen engagement are oriented towards the wellbeing or towards society that is a real challenge.

The most interesting future research that appears written down are the infrastructure and technology, and off course government utilization.

Regarding the bibliography, we could see a diversity of sources, that strengthens the fact that the documentation and the research process was laborious and very well done.

Krunoslav Antoliš Ph. D.

The book provides a comprehensive and well-structured exploration of the Internet's historical development, socio-political implications, and challenges across the MENA region. While it has numerous strengths, including its balanced perspective and relevance to the context, there are areas where improvements in clarity, consistency, and focus could elevate the overall narrative. A more streamlined approach, coupled with visual aids and forward-looking insights, would enhance its accessibility anal relevance, making it an indispensable resource for understanding the region's digital transformation.

The Internet in the Middle East and North Africa is a valuable contribution to the field, offering a nuanced and insightful analysis of the Internet's impact on governance, society, and economy in the MENA region. By broadening the scope, strengthening empirical support, streamlining content, and enhancing readability, the book can become an even more impactful resource for scholars, policymakers, and general readers. Implementing these recommendations will ensure that the book remains relevant, accessible, anal influential in understanding the region's digital transformation.

Michel A. Calvo Ph. D.

This Book, "The Internet in the Middle East and North Africa (MENA): A Study of Usage, Threats and Restrictions", written by Dr. Tal Pavel, provides a comprehensive analysis of Internet adoption and control in the MENA region during 2000-2009. This pivotal period saw extraordinary growth in Internet use, with the region experiencing a 1,648% increase compared to the global average of 380%.

The author examines the Internet development in this region, how the Internet became a tool for political dissent, social activism, and religious discourse, often challenging traditional power structures. He also details how various groups, from political oppositions to terrorist organizations, used the Internet.

It analyses how governments, societies, and individuals navigated the opportunities and challenges presented by this technology. Governments used monitoring, blocking, and filtering techniques and/or engaged in international information warfare, targeting websites critical of their regimes and potentially deploying malicious software. Various actors, individuals and entrepreneurs, emerged to challenge these limitations and restrictions. Technical infrastructure developed unevenly across the region, reflecting economic disparities and political priorities. Social impacts varied by country but consistently challenged traditional communication patterns and cultural norms.

This important study provides a comprehensive regional analysis and details the strong historical context necessary to understand the Internet development in the Middle East and North Africa that challenges us all.

ALMA MATER
EUROPAEA
UNIVERSITY

en.almamater.si