مجتمع التحقق العربي
Arabi Facts Hub

Annual Report on Information Disorder, Coordinated Digital Campaigns

and Trends in Digital Rights Violations in the Middle East and North Africa in 2024

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canadä

This work would not have been possible without the generous support of the International Development Research Centre (IDRC)

Executive Summary

This report marks the inaugural edition of the Annual Report by Arabi Facts Hub (AFH), dedicated to documenting and analyzing the state of information disorder, coordinated digital campaigns, and digital rights violations across the Middle East and North Africa (MENA) in 2024. As AFH's first comprehensive annual publication, it establishes a baseline for tracking the evolving challenges of misinformation, online repression, and digital manipulation in the region. By consolidating evidence from fact-checking networks, monitoring platforms, and legal analysis, the report highlights major trends and offers actionable recommendations for governments, civil society, and technology companies.

In this executive summary, we seek to provide the reader with a comprehensive overview of the report, including its methodology, sections, findings, and recommendations.

The report is structurally organized around three interconnected pillars: (1) Legislation, (2) information disorder and fact-checking trends, and (3) coordinated online campaigns. These dimensions are mutually reinforcing. Laws are increasingly used to silence dissent and shrink civic space, leaving a vacuum in which misinformation flourishes. Coordinated campaigns then exploit both repression and information disorder to manipulate narratives and advance political or geopolitical objectives. Together, these dynamics create a cycle that undermines digital rights and destabilizes public discourse in the region.

Restrictive Legislation

Across MENA, governments continue to misuse cybercrime and counterterrorism laws under vague charges such as "spreading false news" or "undermining state authority." Far from addressing security concerns, these laws serve as tools to criminalize legitimate online expression, target journalists and activists, and suppress civic freedoms. Case studies from Saudi Arabia, Egypt, Bahrain, the UAE, Iraq, Jordan, Tunisia, Morocco, and Mauritania illustrate how legal systems impose harsh penalties including imprisonment and heavy fines for social media activity. Such practices stand in clear conflict with international human rights standards and highlight the urgent need for legal reform to safeguard digital rights.

Information Disorder

In 2024, AFH and its partners monitored 5,402 topics across 23 fact-checking platforms in the Arab world. Content was categorized into five classifications: false, partially false, satirical, investigative, and unclassified, using a methodology aligned with global standards (Meta, Google). Strikingly, 90% of the monitored content was found false, including 185 AI-generated items, mostly political.

Key disinformation hotspots included Palestine (14% of regional disinformation), where the war on Gaza alone accounted for 18% of all fact-checked content 96% of which was false. Other themes included fabricated Red Sea shipping incidents, misleading claims on Egypt's economic performance, U.S. election-related rumors, and smear campaigns during the Paris Olympics. Visual content: images and videos, remained the most widely circulated, reflecting both the power and risks of easily manipulated media in environments with limited access to trusted information.

Coordinated Campaigns

AFH documented 42 coordinated campaigns in 2024, with more than half directly tied to conflict. The Gaza war was a central focus, accounting for 18 campaigns, while others related to Yemen, Sudan, Libya, and regional disputes. State-linked or state-affiliated networks: such as Saudi Arabia's Salmani Electronic Army, Egypt's Maestro, and Emirati-aligned accounts played significant roles in shaping narratives, promoting propaganda, and inflaming sectarian tensions.

These campaigns frequently targeted individuals and vulnerable groups, including journalists, women, refugees, and LGBTQ+ communities, relying on smear tactics, doctored content, and hate speech. Notably, social media platform especially Xfailed to curb inauthentic behavior despite clear violations of their policies, enabling harmful content to circulate unchecked.

Interlinkages Between the Three Pillars

In 2024, AFH and its partners monitored 5,402 topics across 23 fact-checking platforms in the Arab world. Content was categorized into five classifications: false, partially false, satirical, investigative, and unclassified, using a methodology aligned with global standards (Meta, Google). Strikingly, 90% of the monitored content was found false, including 185 AI-generated items, mostly political.

Key disinformation hotspots included Palestine (14% of regional disinformation), where the war on Gaza alone accounted for 18% of all fact-checked content 96% of which was false. Other themes included fabricated Red Sea shipping incidents, misleading claims on Egypt's economic performance, U.S. election-related rumors, and smear campaigns during the Paris Olympics. Visual content: images and videos, remained the most widely circulated, reflecting both the power and risks of easily manipulated media in environments with limited access to trusted information.

Key Findings

- Cybercrime and counterterrorism laws are systematically misused to silence dissent.
- Disinformation surged in 2024, with 90% of content fact-checked as false especially around Gaza, Yemen, Syria, U.S. elections, and economic issues.
- Coordinated campaigns by state-linked actors weaponized disinformation in conflicts and targeted activists, journalists, and vulnerable communities.
- Social media platforms failed to enforce their own policies, allowing harmful content to thrive.

Recommendations

To address these trends, AFH proposes targeted measures:

For Governments: Align legislation with international standards, protect online freedoms, end internet shutdowns, and release those imprisoned for digital expression.

For Civil Society: Expand documentation of violations, strengthen regional coalitions, train activists in digital security, and provide legal and psychological support to victims of online harassment.

For Technology Companies: Prioritize user safety, invest in transparent content moderation, disclose cooperation with governments, and dismantle coordinated inauthentic networks through independent assessments and locally informed teams.

Background

Our first annual report aims to identify and analyze trends in information disorder across the Middle East and North Africa (MENA) in 2024. Information disorder is defined as a broad category that includes: **misinformation** — false information shared without the intent to harm; **disinformation** — false information shared with the intent to cause harm; and **malinformation** — genuine information used in a way that inflicts harm. These three categories are collectively referred to as MDM, and the report uses both "information disorder" and **"MDM"** interchangeably. Similarly, **coordinated digital campaigns** refer to both authentic and fake or duplicate social media accounts that are created with the intent to manipulate audiences and amplify specific narratives — often ones that align with government agendas.

1. Digital Rights and Legal Frameworks in MENA

The report opens with a review of the evolution of digital rights in MENA over the past few years, including changes in cybercrime legislation and other laws used to regulate the digital space. Digital rights refer to the digital extensions of human rights — those exercised within online environments. The Alliance for Universal Digital Rights outlines nine digital principles to ensure the protection of human rights in the digital domain. These include: personal safety, protection of privacy, universal digital access, freedom of expression and association, as well as secure, stable, and resilient networks, and sound digital governance.

The report also presents research conducted on information disorder during the past year, through an extensive analysis of data collected from numerous fact-checking organizations operating across the region. This includes an examination of a number of coordinated digital campaigns launched in 2024.

The report concludes with a set of recommendations addressed to fact-checkers in the region, technology companies, governments, and international organizations, outlining proposed ways to confront information disorder and mitigate its impact on the digital rights of communities in the MENA region.

This report comes at a time when challenges to digital rights and freedom of expression in digital spaces are intensifying, as evidenced by the increasing use of legal measures by states to monitor citizens' internet use, suppress online dissent, and stifle the free flow of information. In fact, although technological advancement and digital transformations across the region have been linked to economic growth—particularly in the countries of the Gulf Cooperation Council (GCC) —as well as to the mobilization of communities during the democratic uprisings of 2011 and 2019, they have also been employed in the service of counter-revolutionary efforts in response to those very uprisings.

At an accelerating pace, digital transformation has been misused by many governments in the region to entrench what has come to be known as "digital authoritarianism"—the authoritarian adaptation to digital technology. This encompasses a wide range of practices, from blocking and disrupting access to the internet, to employing legal frameworks in support of surveillance and repression. In recent years, there has been a marked increase in the use of national security and counterterrorism laws to criminalize digital activity, justify internet censorship, block websites, and monitor individuals. For instance, Saudi Arabia has used its counterterrorism law to charge human rights activists with "committing" or "inciting" terrorism based on the content they publish online. This has also been the case in other countries across the region, leading to the targeting of political dissidents and civil society activists in efforts to punish and silence online opposition. .

In addition to the misuse of existing laws to police online activity, some countries in the region have recently introduced cybercrime legislation that criminalizes a broad spectrum of online content and grants governments expanded powers to surveil digital activity—further restricting the ability to exercise freedom of expression online.

2. Information Disorder and Coordinated Campaigns

The recent explosive events that lead to political escalation across the MENA region have intensified information disorder within Arabic online content. Governments throughout the region have employed systematic, coordinated inauthentic behavioral campaigns—composed of real, fake, and duplicate social media accounts—to deliberately push specific narratives during turbulent times. In this context, some governments in the Middle East and North Africa stand out as major actors behind information disorder, using bots, troll armies, and "sockpuppet" accounts to flood online spaces with pro-government narratives.

In 2019 Twitter—now known as X—unveiled the largest state-backed misinformation network it had ever discovered, originating from Saudi Arabia; the network involved 5,929 core accounts, which in turn controlled 88,000 accounts engaged in coordinated inauthentic behavior aimed at influencing the public. A previous AFH report documented campaigns that have spread in recent years: in Jordan, online campaigns influenced the controversial Cybercrime Law issued in August 2021; in Egypt, the killing of Nayera Ashraf sparked the creation of multiple Facebook groups and hashtags supporting the man accused of killing her and spreading conspiracy theories.

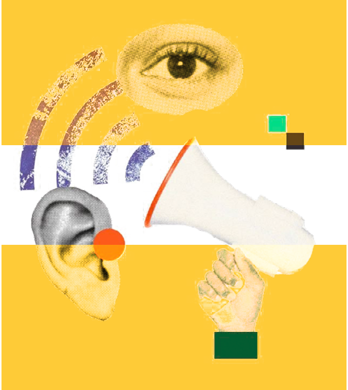
In 2024, coordinated campaigns related to the wars in Gaza, Lebanon, and Sudan proliferated. The genocide in Gaza in particular witnessed a surge of both direct and indirect campaigns. Direct campaigns include, for example, the coordinated Israeli attacks on Palestinian journalists in February 2024 or on UNRWA in March 2024. Indirect campaigns focus on Gaza but target regional parties. For instance, following the Israeli assault on Gaza, Saudi accounts quickly praised the Kingdom for recognizing Palestine, while Emirati accounts responded by highlighting and praising the UAE's positions instead.

The assassination of several prominent leaders during the war also triggered coordinated campaigns: the killing of Ismail Haniyeh, head of Hamas's political bureau, led to targeted campaigns accusing Shiites of orchestrating the assassination, met by counter-campaigns accusing Sunnis of involvement and collusion with Israel. Similarly, after the assassination of Hezbollah's Secretary-General Hassan Nasrallah, Saudi and Egyptian accounts launched mocking campaigns that included spreading disinformation about him.

The war in Sudan, which had already seen forms of digital repression including repeated internet shutdowns, inspired a series of coordinated digital campaigns involving the United Arab Emirates—either supporting its participation in the conflict or opposing it.

3. New Technological Drivers of Disinformation

Moreover, the rapid spread of generative artificial intelligence (AI) technologies has exacerbated the intensity of information disorder globally and within the Middle East and North Africa. These tools have facilitated the production of fabricated content—whether texts, images, audio recordings, or videos—posing an additional challenge to fact-checking efforts and combating disinformation.



Methodology

This report provides an overview of information disorder trends in the region in two ways: first, through a comprehensive analysis of data and investigations issued by a group of fact-checking organizations in the region; and second, through an analysis of coordinated inauthentic behavior campaigns based on the weekly analysis conducted by Arabi Facts Hub (AFH) in 2024, where the team selects one campaign weekly for detailed analysis and study.

Our data analysis comprises a total of 5,402 verified investigations or fact-checked information, which collectively paint a picture of information disorder present in Arabic content. To achieve this, we reviewed data from January to December 2024 collected from 23 fact-checking organizations across the region. AFH organizes this data based on the contributing organization, the country involved, and the categories/topics. Due to the diversity of fact-checking outputs from various organizations, the monthly volume of data issued by these organizations—and thus for the countries concerned—is not uniform. Furthermore, while most fact-checking organizations operate independently, we had to include additional organizations potentially affiliated with government entities in some countries to represent these countries, due to the absence of independent civil society organizations.

Coordinated inauthentic behavior campaigns have gained increasing significance in MENA. Since late 2022, AFH has undertaken the task of analyzing this pattern of campaigns by publishing periodic reports in partnership with Daraj. During this period, the organization published approximately 70 reports documenting activity from both fake and real accounts dedicated to spreading coordinated inauthentic messaging, some of which contains hate speech and racism, while a large portion includes disinformation.

Coordinated inauthentic behavior campaigns are defined as a deceptive communication tactic that uses a mix of real, fake, and duplicate social media accounts to form an inauthentic network across social platforms, steering users toward a specific ideological direction. This definition excludes non-digital coordinated campaigns launched by traditional media to support or attack a certain party, as well as commercial/political digital campaigns targeting individuals or groups based on their data and preferences. It also excludes coordinated commercial and advertising digital campaigns aimed at influencing consumer behavior toward a particular product.

The main criteria we use to identify relevant cases include:

- The presence of a coordinated digital campaign that spreads repetitive and organized messages in support of specific parties or groups and/or attacks another party or group;
- The campaign is launched through social media platforms, particularly X (formerly known as Twitter), Facebook, and Telegram;
- The campaign aims to influence public opinion;
- Exposing the campaign serves the public interest, beyond the interests of the targeted individual or entity.

This annual report covers the content of 42 coordinated digital campaigns analyzed by AFH in 2024. The analysis is organized into multiple research themes aligned with the campaigns' topics—such as military or political conflicts, refugee issues, minority rights, gender-related matters, among other things.

Campaigns are categorized based on the country or countries where the campaign was implemented, in addition to identifying the country or entity likely responsible for orchestrating it. In some cases, a campaign may originate in one country (or a group of countries) while being implemented in a context that is geographically distinct from its source.

Legislation in Arab Countries: Weaponizing Law Against Digital Rights

Digital rights are defined as the natural extension of human rights into the digital space. They guarantee every individual the right to access and share information freely and securely. These rights include the right to privacy and the protection of personal data, the right to express opinions freely without fear of surveillance or persecution, the right to access the internet and communication services, as well as the right to equality and non-discrimination in accessing technology and knowledge.[1]

Although many Arab states have enacted laws addressing cybercrime, these laws have often been misused to suppress online freedom of expression.[2] Counterterrorism laws have also been employed in some countries to restrict digital rights and freedoms, including the imposition of harsher penalties related to the use of social media platforms.

This section of the report highlights the most relevant legislation enacted in Arab countries and presents examples of how such laws have been used to suppress freedom of expression in general—and digital rights in particular.

[1] Kathleen Azali, «Coconet: What are digital rights?» Association for Progressive Communications, last modified July 9, 2024,

[2] «Learn about the classification of Arab countries in the 2024 Freedom Index (infographic),» Arabi 21, last modified March 3, 2024

Criminalizing Digital Rights

In Saudi Arabia, counterterrorism laws are systematically used as tools to restrict and violate digital rights. In recent years, a number of human rights activists have been charged with committing “terrorist crimes” based on Articles 43 and 44 of the Counterterrorism Law—reflecting a growing trend of legal provisions being deployed to prosecute digital activity related to rights advocacy or freedoms.

A notable example of this digital repression is the case of Saudi activist Manal Al-Otaibi, who was arrested in November 2022 on charges related to “terrorism” and “undermining security,” after posting a series of videos that some described as “offensive to religion and societal values.” In January 2024, she was sentenced to 11 years in prison—a verdict that sparked widespread outrage. Amnesty International stated in a report that the ruling fell short of international standards of justice, pointing to a lack of transparency and fairness in legal proceedings—highlighting a deeper crisis in the treatment of human rights and freedom of expression in the Kingdom.[3]

In Egypt, the 2015 Counterterrorism Law continues to heavily restrict digital activity. Some of its articles are used to criminalize the dissemination of news or information deemed “misleading” or threatening to “national security.” In 2018, President Abdel Fattah El-Sisi ratified the Cybercrime Law, which grants authorities broad powers to erode user privacy and monitor online behavior. Parliament also passed a Media Law giving the government authority to monitor any social media account with more than 5,000 followers.

These laws have been used to justify website blocking and target human rights defenders and political dissidents. A prominent example is Yehia Hussein Abdel Hadi, founder of the Civil Democratic Movement, who faced multiple charges including “spreading false news” and “disturbing public order.”[4] He spent three years in prison before receiving a presidential pardon in 2022. However, he was re-arrested in 2024 after publishing a Facebook article titled “How Long Will the Army Remain Silent?”, and faced new charges such as “joining a terrorist group,” “misusing social media,” and “spreading rumors and false news.”

In Bahrain, counterterrorism and cybercrime laws are actively used as surveillance tools to restrict freedom of expression and digital activism.[5] The Counterterrorism Law penalizes those convicted of publishing information considered “misleading” or threatening to “national security.” According to Americans for Democracy & Human Rights in Bahrain (ADHRB), these laws have been used to target human rights defenders and dissidents who express their opinions online.[6]

These examples from across the MENA region reflect how criminal laws are, at times, arbitrarily applied—not to protect the digital space, but rather to suppress rights activists, dissidents, and opposition voices.

[3] Urgent action: Manahel Al-Otaibi sentenced to 11 years in prison» Amnesty International, last modified May 22, 2024

[4] Eyptian opposition figure Yahya Hussein Abdel Hadi detained after being kidnapped from the street,» Al Araby, last modified August 1, 2024,

[5] Security and protection,» The Government of the Kingdom of Bahrain, accessed January 26, 2025,

[6] «Restricted Freedom … The Bahraini Government’s failure to Implement Transitional Justice for Released Individuals,» Americans for Democracy & Human Rights in Bahrain, last modified July 1, 2024,

Cybercrime Laws

Cybercrime laws in the region are often used as tools to silence critics, activists, and human rights defenders. Additionally, they are frequently invoked as a pretext to restrict journalistic work. Many of these laws share a common trait: the use of vague and overly broad terminology—such as “undermining the state,” “inciting sectarianism or discord,” “threatening national security or independence,” and “violating public morals”—all of which allow the law to be weaponized against dissent.

For example, the UAE’s Cybercrime Law criminalizes a wide range of digital activities, including publishing or sharing content deemed offensive or contrary to Islamic values.[7] It also penalizes any unauthorized use of personal data or information, granting authorities broad powers to monitor digital activity. The law imposes severe penalties, including lengthy prison sentences and heavy fines.

Iraq’s proposed cybercrime law recommends harsh penalties for anyone who publishes content deemed offensive to the country’s “supreme economic, political, military, or security interests.” These penalties include life imprisonment and fines of up to 50 million Iraqi dinars (approximately 38,000 USD). Such legislation has raised concerns about its potential use to restrict digital freedoms and punish dissenting voices, thereby threatening to shrink the already limited space for public discourse and civic engagement.[8]

In Jordan, the Cybercrime Law contains vague provisions that are open to arbitrary interpretation, enabling the targeting of dissenting voices and the suppression of freedom of expression, according to Amnesty International. [9] The law focuses on combating “rumors” and “false news,” penalizing the publication of information deemed misleading or harmful to “public or private interests.” This has raised human rights concerns about its potential misuse to restrict legitimate criticism and curtail free expression.[10]

Notable cases under the law include the arrest of lawyer Moataz Awad due to social media posts, charged with “inciting sectarian strife,” and fined 5,000 Jordanian dinars (approximately 7,000 US dollars).[11] Similarly, journalist Heba Abu Taha was sentenced to one year in prison for an article criticizing Jordan’s role in exporting goods to Israel amid the ongoing Israeli war on the Gaza Strip.[12] These cases amplify the concerns of human rights organizations about the exploitation and weaponization of the law to silence critical voices and restrict digital freedoms.

In Tunisia, Electronic Crimes decree No. 54 of 2022 is used as a tool to restrict civil liberties and suppress the work of human rights organizations, according to Amnesty International. [13] The decree particularly targets organizations working on migrant and refugee rights, contributing to a significant decline in civil society activity. It also imposes harsh penalties on any expression deemed insulting to authorities or inciting discord, raising widespread human rights concerns.

[7] «Decree-Law on Combatting Rumors and Cybercrimes,» The Government of the United Arab Emirates, accessed January 26, 2025,

[8] “Iraq: Two Draft Laws Threaten the Right to Freedom of Expression and Peaceful Assembly”, Amnesty International, July 18, 2023,

[9] «Jordan: New cybercrime law stifles freedom of expression,» Amnesty International, last modified August 13, 2024

[10] «Jordan: Protests in response to the issuance of «draconian» cybercrime law,» Business & Human Rights Resource Centre, last modified July 29, 2023,

[11] Jordan: A Year of Repression – Renewed Calls to Repeal the Cybercrime Law, Article 19, last modified September 13, 2024,

[12] A Year in Prison for a Jordanian Journalist Who Published an Investigation on Jordan’s Export of Goods to Israel During the Gaza War, Mc-doualiya, last modified June 17. 2024,

[13] Tunisia: Authorities Escalate Clampdown on Media, Freedom of Expression, Amnesty International, last modified May 30, 2024

According to the foundation Digital Action, dozens of activists and bloggers have been targeted under this decree.[14] Recently, nearly sixty individuals have been detained or summoned due to their social media posts, reflecting the expanding scope of censorship and restrictions on freedom of expression in Tunisia.

In March 2020, the Moroccan government introduced a draft law to regulate social media, sparking widespread controversy due to its potential to restrict freedom of expression. Activists dubbed it the "gag law." Article 16, in particular, faced criticism for its vague definition of "fake news," which opens the door to arbitrary interpretations and the criminalization of criticism of the authorities. In 2023, the Minister of Justice announced harsher penalties for those spreading fake news under the new draft penal code, further heightening concerns over restrictions on free expression. On March 3, 2025, a Casablanca court sentenced prominent activist Fouad Abdelmoumni in absentia to six months in prison and fined him 2,000 dirhams (about USD 208) over a Facebook post. [15]

In Mauritania, the enactment of the "Information Manipulation" and "Protection of National Symbols" laws has been used to restrict freedom of opinion under the pretext of combating "fake news." For instance, blogger Abdelrahman Ould Wedaddy was summoned in September 2024 by the National Gendarmerie's (police) cybercrime unit after broadcasting a Facebook livestream in which he criticized the drug trade.

The Omani government uses Article 19 of the Cybercrime Law as a legal tool to prosecute individuals who publish content deemed to incite sectarianism or disturb public order. In April 2024, Omani authorities summoned activist Said Jaddad over a series of posts on his account on X.[16] At the same time, the Omani Centre for Human Rights reported that Dr. Ahmed Masoud Al-Ma'shani and Tareq Said Mahad Al-Omari faced similar charges, accused of posting content that incites religious and sectarian strife.[17]

It is evident that many countries in the MENA region have used cybercrime-related laws as a tool to restrict freedom of opinion and expression. This has had serious repercussions for journalists and activists who voice opinions that diverge from those of the authorities. Although these laws claim to aim at combating disinformation and protecting public security, they are often used, in practice, to curtail digital freedoms, suppress dissent, and impose media censorship.

[14] Tunisia Country Briefing, Digital Action, last modified October 30, 2024

[15] Morocco: Activist Sentenced Over Peaceful Expression, HRW, last modified Mar 27, 2025

[16] «Royal Decree No. 12/2011 issuing the Law on Combatting Information Technology Crimes,» Decree Oman, last modified February 6, 2011

[17] «Latest developments in the case of detainees in Dhofar Governorate,» The Omani Center for Human Rights & Democracy, accessed January 26, 2025,

Information Disorder in the Middle East and North Africa in 2024

AFH relies on a specific methodology for classifying fact-checking content. This methodology was carefully developed after examining the classification approaches used by platforms like Meta and Google, and ensuring alignment with those platforms' standards. Below are the AFH classifications and what each one signifies:

False: This category includes claims that are entirely unfounded, whether they are fabricated or simply inaccurate.

Partially False: This applies to content containing some factual errors that contribute to misinformation, including misleading framing, selective context, or incorrect context.

Satirical: This includes content intended for satire, exaggeration, or criticism, especially when it comes from platforms not clearly labeled as satirical or from lesser-known satire sources.

Reports (Investigations): This category covers all content produced by fact-checking platforms that aim to shed light on specific controversial issues, with the goal of spreading verified, reliable information and helping audiences avoid falling for disinformation.

Unclassified: These are materials that fact-checking partners have not labeled as verified content. No specific classification was assigned by the partners.

Fact-checking in 2024

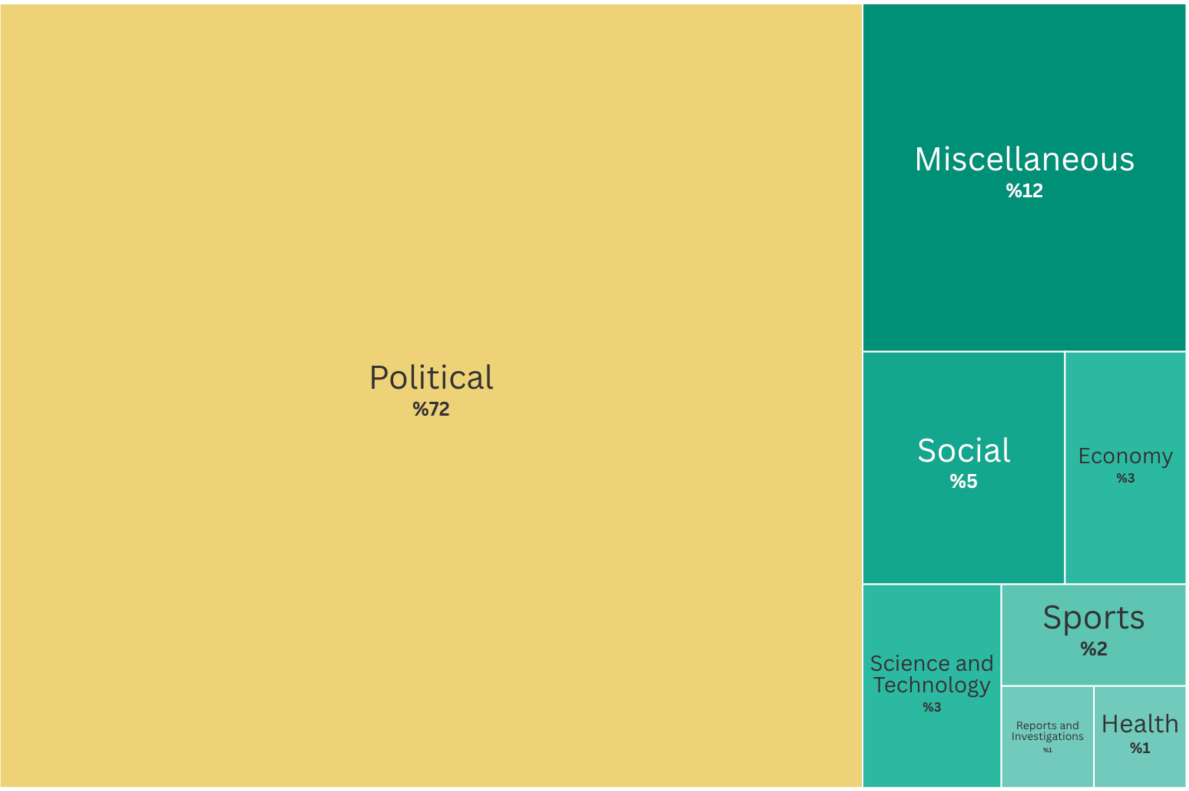
Over the course of one year, AFH monitored a total of 5,402 pieces of content, collected from 23 fact-checking organizations across the Arab world. According to AFH's classification system (outlined above), 90% of the monitored content was labeled as "False," including items generated by artificial intelligence (AI). Approximately 185 AI-generated items were identified and fact-checked by the 23 platforms. Of these, about 41% were visual content, particularly images and videos.

61% of the AI-generated content focused on political topics, while 19% fell under entertainment, and 15% dealt with science and technology.

Another 5% of the content was classified as "Partially False," while 4% of the output consisted of original reports and investigations produced by fact-checking platforms—not simply verifications of existing third-party content. Satirical content made up less than 1% of the total.

Political content accounted for 72% of the disinformation fact-checked by the 23 platforms, followed by entertainment and miscellaneous content—classified as “miscellaneous”—at 12%, and social topics at only 5%. Other topics, including economy, science and technology, sports, health, and original reports and investigations, made up the remaining 10% combined, with varying proportions as illustrated in the chart below.

72%
of Fact-Checked Material Is Political Topics



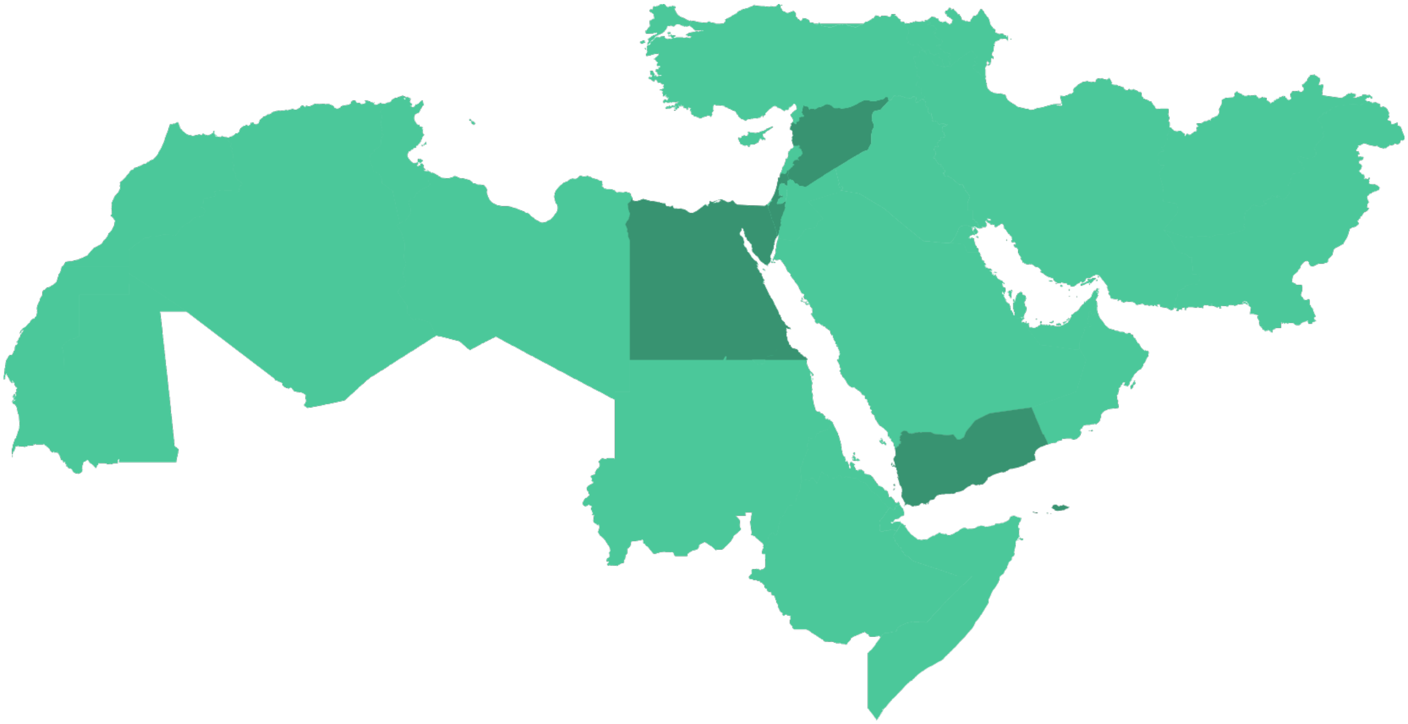
In terms of country-based distribution, Palestine was the most targeted by fact-checking content, accounting for 14% of the total. This is primarily due to the surge in disinformation that accompanied the recent war on Gaza—from October 7, 2023, until the time of this report's preparation—which prompted fact-checking platforms across various Arab countries to establish dedicated monitoring units.

Yemen followed with 12%, largely due to disinformation surrounding Houthi attacks on ships in the Mediterranean Sea and the link to Israel, the United States, and the Palestinian cause. Syria came third with 11%, especially during the final month of the year, following the fall of Bashar al-Assad's regime, which triggered a wave of conflicting narratives.

Egypt ranked fourth with 8% of the fact-checked content, followed by Lebanon, Iraq, Saudi Arabia, Sudan, Israel, and Libya, each ranging between 7% and 4%, in descending order. The United States and Iran were in the middle of the list with 3% each, due to rumors surrounding the death of the Iranian president, the assassination of Ismail Haniyeh, and other events related to the ongoing war on Gaza.

Non-Arab Asian countries, such as Singapore and Tajikistan, appeared at the bottom of the list.

Palestine was the Country with the Most Disinformation, Followed by Yemen and Syria

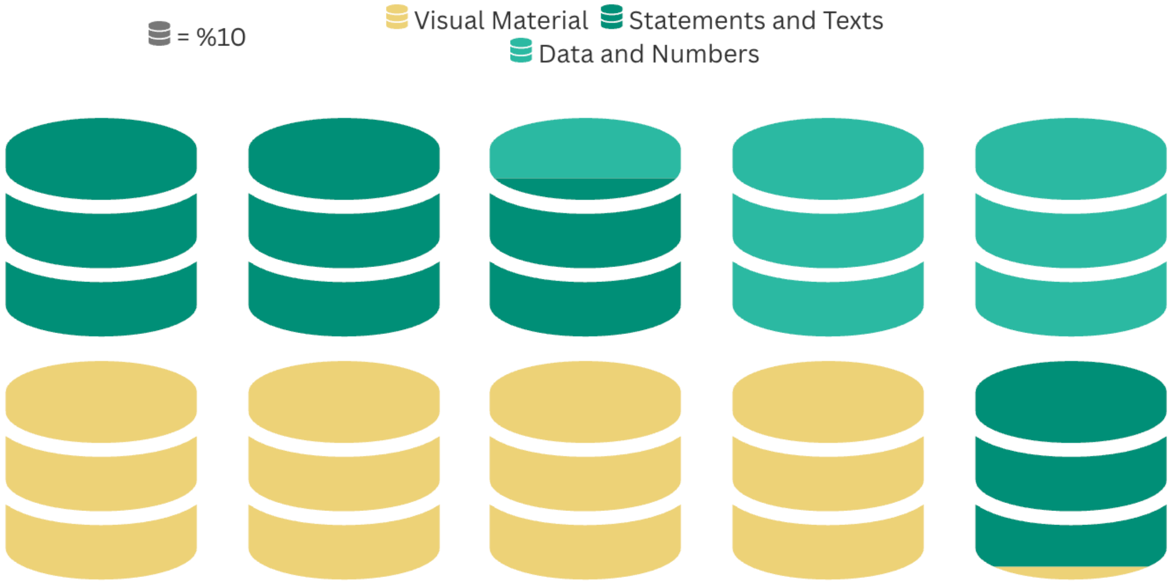


The majority of the content verified by fact-checking organizations in the Arab world consisted of visual materials—including videos, images, and maps—making up 41% of all verified content. These were followed by statements and texts, which include journalistic and media content as well as social media posts, accounting for 35% of the total. Data and figures came in last, comprising 22%, likely due to the challenges of accessing official information and statistics in the Arab world and broader Middle East. This difficulty is linked to the absence of legislation guaranteeing the right to access information in most countries of the region, as well as the technical expertise required to process and analyze open-source data sets.

41%

of Fact-Checked Material was Visual Material, Including Photographs, Videos, and Maps

followed by statements, texts, numbers, and data



The disinformation landscape in MENA was saturated in 2024; however, six key themes stood out, according to data analysis conducted by the AFH.

The War On Gaza

On January 2, 2024, the Egyptian fact-checking platform Matsada2sh verified a video accompanying a post that claimed: “A high-level martyr operation... Freedom fighters seized a Zionist armored vehicle for camouflage, rigged it with explosives, and detonated it near several tanks.” According to the fact-checking result, the video was old — specifically from seven years ago in Iraq — and had no relation to the war in Gaza.[18]

Fact-checking materials related to the war in Gaza — which broke out on October 7, 2023 — accounted for 18% of the AFH’s database over the past year, totaling 976 fact-checks.

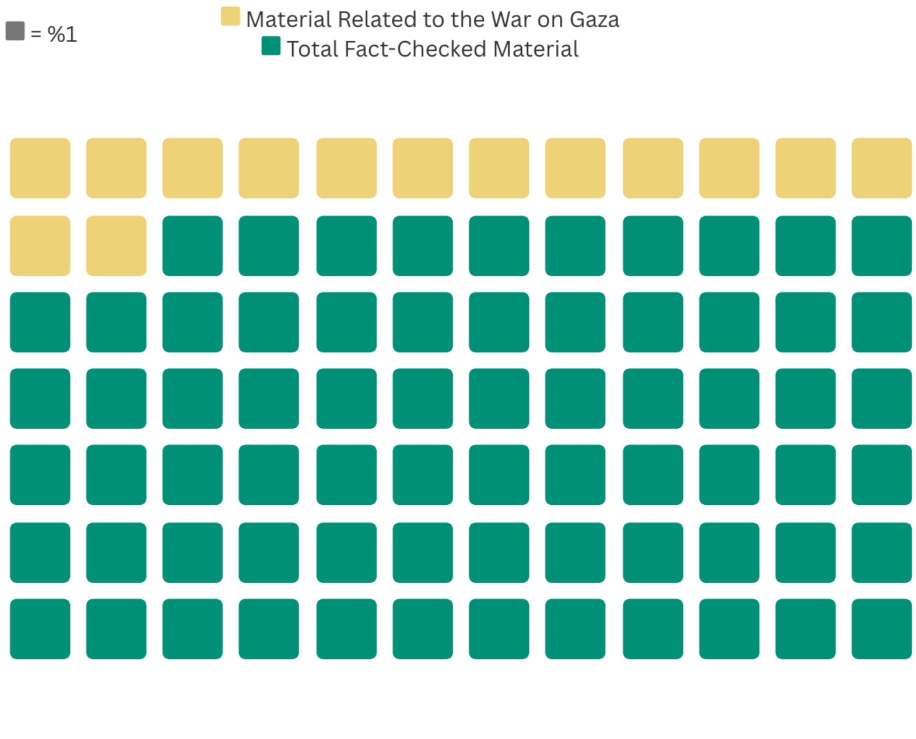
96% of Gaza war-related entries in the database were classified as “False,” while 4% were categorized as either “Partially False” or “Investigations.”

Approximately 55% of fact-checked content consisted of visual materials, including videos, images, and maps—most of which were outdated or captured in different geographical locations and contexts.

Statements and texts ranked second, accounting for 25%, including posts on social media platforms, particularly from Arabic-language Israeli accounts. Data and figures related to the war came in third among the Gaza war-related fact-checked materials, comprising around 21% of the total.

18%

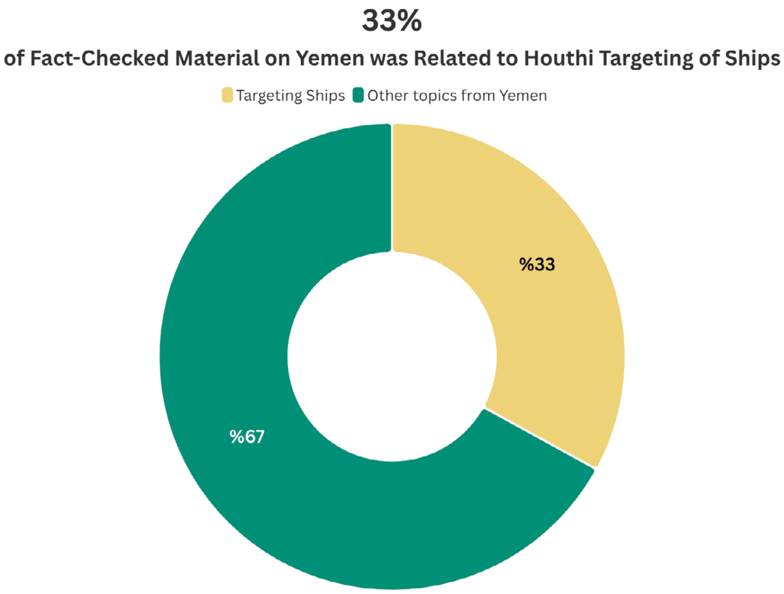
of the Database of Fact-Checked Material was about the War in Gaza



[18] “This video is old and from Iraq; it has no connection to the war in Gaza”, Matsda2sh, last modified January 2, 2024,

Houthis Targeting Ships in the Red Sea

On February 20, 2024, the Yemeni platform "Sadeq" fact-checked two video clips accompanied by the caption: "Two videos showing the sinking of the British ship 'RUBYMAR', which the Houthis claimed to have targeted in the Gulf of Aden." However, verification revealed that "the first video actually showed the sinking of the Turkish cargo vessel 'ATLANTIK CONFIDENCE' off the coast of Masirah Island, Oman, on April 3, 2013. The second clip showed the Brazilian Navy sinking the bulk carrier 'STELLAR BANNER' off the coast of Maranhão, northeastern Brazil, in June 2020." [19]



33%

of Fact-Checked Material on Yemen was Related to Houthi Targeting of Ships

Amid the ongoing Israeli war on Gaza, news circulated alleging that the Houthis had targeted ships in the Red Sea as a response to Israeli actions during the conflict. In fact, 33% of misleading content related to Yemen revolved around such claims of Houthi attacks on vessels of various nationalities in the Red Sea.

Some of this content consisted of old footage, such as images or videos from unrelated incidents and locations, while others were sourced from video games or generated using artificial intelligence. All of these materials were classified as "False" according to AFH methodology.

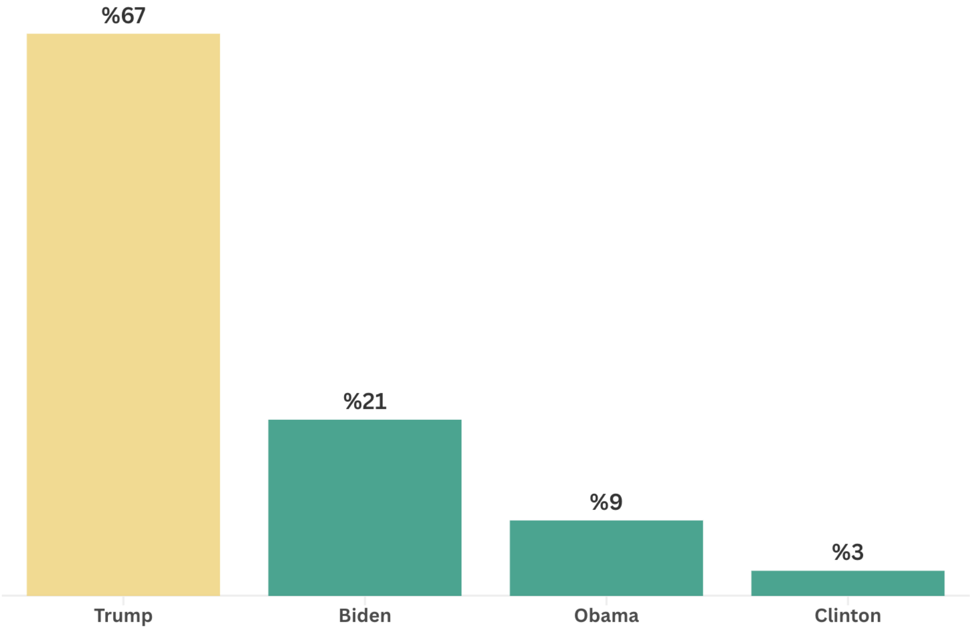
[19] The Two Video Clips Are Not of the Sinking of the British Ship "RUBYMAR", Sidqyem, Last modified January 8, 2024,

U.S. Elections

On July 14, 2024, accounts on the X circulated a quote allegedly made by former U.S. President Joe Biden just hours before the attempted assassination of Donald Trump. The quote claimed: "I will teach Donald Trump a lesson he'll never forget and he'll never run again," implying Biden's involvement in the assassination attempt. The fact-checking platform Misbar investigated the claim and found it to be false. In reality, in January 2024, President Joe Biden, during a rally with his supporters, condemned the abortion ban that endangers the health of pregnant women and placed the blame on Donald Trump.[20]

67%

of Fact-Checked Material On the U.S. Elections Were About Trump



Ironically in the middle of all of this political turmoil, 2024 was dubbed "the Year of Democracy" due to the number of elections held in many countries around the world—most notably in the United States, which saw a significant amount of disinformation, even before the final candidates were confirmed. AFH recorded a total of 141 political fact-checks related to the United States, 33 of which were about the U.S. elections—roughly 23%.

The most prominent claims focused on then-presidential candidate Donald Trump, accounting for 67% of the content—particularly the rumor about his alleged assassination attempt, which was fact-checked by multiple platforms. Following Trump in number of fact-checked claims were former U.S. Presidents Joe Biden and Barack Obama, as well as Hillary Clinton, while no fact-checks addressed candidate Kamala Harris. According to AFH methodology, all the materials fact-checked regarding the U.S. elections were classified as "False."

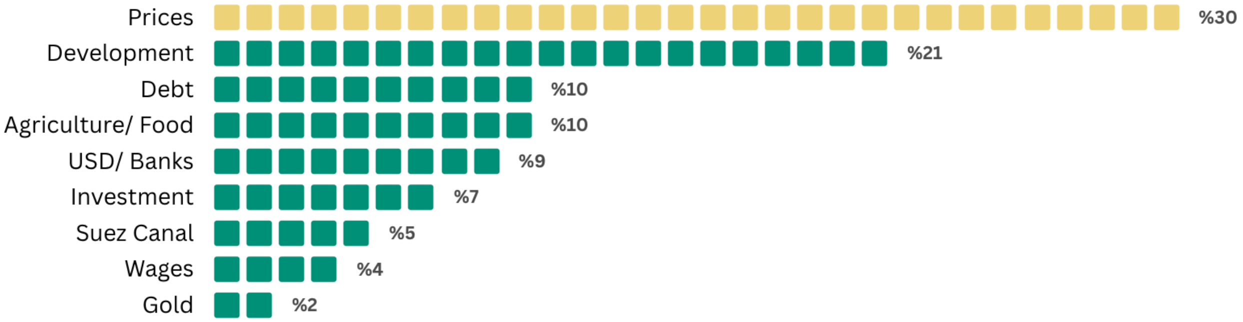
[20] "Joe Biden did not threaten Trump hours before the assassination attempt.", Misbar, Last modified July 4, 2024,

The Egyptian Economy

On January 3, 2024, Egyptian Prime Minister Mostafa Madbouly stated during a press conference that “electricity subsidies have now reached 90 billion Egyptian pounds.” However, the Egyptian fact-checking platform Matsada2sh revealed that this claim is inaccurate, as the Egyptian government stopped subsidizing electricity four years ago. According to Egypt’s general budget data, electricity subsidies were zero from the 2019/2020 fiscal year through to 2023/2024.[21]

30%

of Disinformation Material on the Egyptian Economy was Related to Prices



The economy was a dominant topic, especially amid the renewed devaluation of the Egyptian pound, the issue of foreign debt, and developments surrounding the Ras El Hekma deal.

AFH recorded around 111 fact-checked claims related to Egypt’s economy. Approximately 30% of these addressed rising prices or shortages of goods in Egyptian markets—such as medicines—and inflation-related crises. Another 21% covered development issues in both their negative and positive aspects, including unemployment, energy, and national projects. Topics related to foreign debt, loans, grants, and their impact on Egypt’s economy ranked third, making up 10% of the total, equal to the share of issues concerning agriculture and food security.

[21] On Electricity and Debt: Inaccurate Statements by Mostafa Madbouly, Matsda2sh, Last modified January 3, 2024,

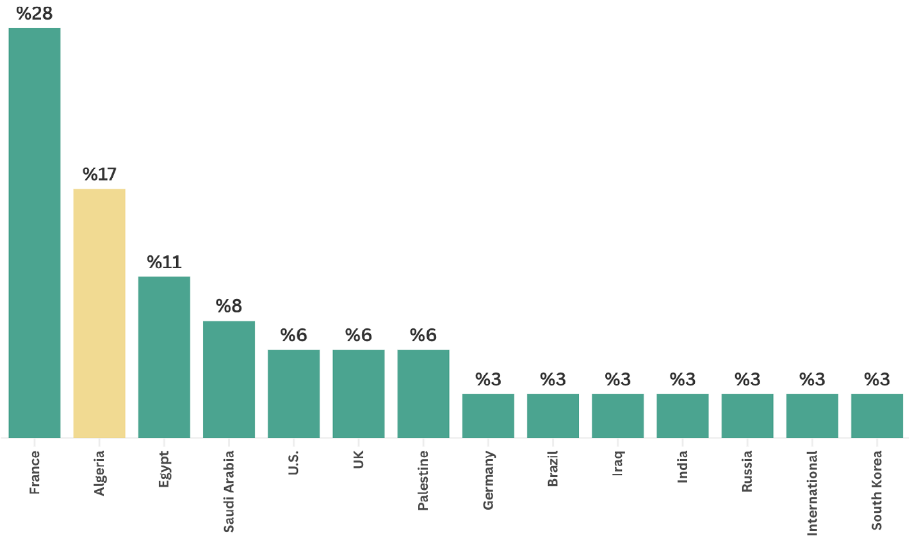
The Paris Olympics

On October 6, 2024, social media accounts and sports news websites circulated a claim alleging that “the World Boxing Organization (WBO) had permanently banned Algerian boxer Imane Khelif from professional boxing and stripped her of her titles after test results showed elevated testosterone levels.” However, the Syrian fact-checking platform Ta’akkad revealed that the claim was fabricated. The Algerian Olympic and Sports Committee officially responded to the allegation, describing it as “nothing more than a deliberate smear campaign against Algeria, clearly sourced and intended to undermine the outstanding success of the Olympic champion.”[22]

17%

of Fact-Checked Material on the Paris Olympics Was About Algeria

In relation to Algerian boxer Imane Khelif



Sports were not immune to misinformation in 2024 either—especially in relation to a global event like the Paris Olympics, which also carried political, social, and gender-related dimensions.

AFH monitored 36 pieces produced by fact-checking platforms related to the Paris Olympics. Of these, 10 pieces addressed topics directly related to France, while Algeria ranked second with around 6 pieces, primarily due to the case of Algerian boxer Imane Khelif. An additional 4 pieces focused on Egypt.

[22] “What is the truth behind Imane Khelif being banned from boxing and stripped of her titles?”, verify-sy (Ta’kkad), last modified October 6, 2024,

Coordinated Online Campaigns in 2024: Indicators and Key Actors

"Coordinated inauthentic behavior" is a manipulative communication method that uses a mixture of original, fake, and duplicate social media accounts to weave a hostile network operating across digital platforms.[23]

This definition closely reflects the core approach of AFH, as it excludes coordinated but non-digital campaigns launched by traditional media in favor of or against a particular party. It also excludes online campaigns targeting specific individuals or groups based on data analysis and preferences, which are then used to send political or commercial messages—such as those seen during the 2016 U.S. elections.[24] Likewise, it does not include coordinated commercial or promotional campaigns that aim to influence consumer behavior or steer them toward a particular product.

In most cases, coordinated online campaigns originate from fake accounts that are programmed and managed by a particular entity. These accounts are used to drive interaction with specific hashtags and mobilize support or opposition in favor of or against a given actor.

The forms of such campaigns vary. Some are operated by bots that perform pre-programmed tasks, while others are run by individuals or organized groups. In some cases, real accounts also participate in directed campaigns. All of these seek to influence public opinion through non-organic means. As these campaigns evolve, accounts increasingly rely on artificial intelligence to generate images and publish varied content that conceals their nature—making detection more difficult.

In response to this evolution, AFH adopted advanced tools and techniques, such as Meltwater and CrowdTangle (before Meta discontinued it), as well as AI content detection technologies. This report focuses on the statistical analysis of the campaigns observed throughout the year in order to identify trends and provide recommendations, without detailing the methodology—which can be found in our article published on IJNet.[25]

[23] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10060790/#:~:text=Coordinated%20inauthentic%20behavior%20(CIB)%20is,across%20multiple%20social%20media%20platforms

[24] https://www.techtarget.com/searchcio/definition/microtargeting

[25] Methodology and Tools for Detecting Inauthentic Online Campaigns, IJNet, last modified August 7, 2024,

It is important to note that this report highlights a select number of online campaigns and inauthentic behavior in the region during 2024, without claiming to cover all such campaigns. This is due to the difficulty of comprehensive statistical tracking and the shifting priorities driven by rapidly unfolding events—chief among them the war on Gaza and its regional repercussions.

War was a prominent subject in the studied online campaigns. The region has seen many conflicts recently, including those in Yemen, Libya, Sudan, and Gaza, which started in October 2023 and later involved Lebanon in September 2024, followed by renewed tensions in Syria in early December. War-related subjects were dominant, with 26 of the 42 campaigns focused on conflict. The war in Gaza and its continuing impact accounted for the majority, at 18 campaigns.

Some of the campaigns tracked during the ongoing Gaza war were direct, such as the one led by Israeli accounts targeting two Al Jazeera journalists after they were hit by a drone strike in February 2024. This campaign continued and escalated in October when the Israeli army issued a statement accusing journalists in Gaza of affiliation with Hamas. Another major campaign targeted UNRWA in late March 2024.

On the other hand, a series of indirect campaigns was also observed—those addressing the Gaza issue in a more convoluted way by targeting regional actors involved in the conflict, whether militarily or diplomatically. Examples include a campaign launched by fake accounts promoting Iraqi militia attacks on Israel, a smear campaign against Jordanian protests opposing the war on Gaza, and another targeting Iraqi militia reactions to Jordan's wartime decisions.

Online campaigns targeting supporters of Hezbollah also intensified early on, as the group ramped up its military skirmishes with Israel, which eventually escalated into a full-scale war in September 2024. One victim of these campaigns was Lebanese nun Maya Ziyadeh, who faced online harassment after expressing support for fighters in southern Lebanon and calling for "prayers for the South."

Away from the battlefields in Gaza, coordinated online campaigns also extended into the realm of diplomacy. Saudi-affiliated accounts were quick to claim credit for the recognition of Palestine by several countries, attributing it to the Kingdom's diplomatic efforts. In response, Emirati accounts cast doubt on this narrative, asserting that the recognition was actually due to initiatives by the United Arab Emirates.

In a rare and striking incident, the announcement of the identity of a killed Israeli combatant sparked a wave of digital skirmishes between Algeria and Morocco. Disinformation circulated by Algerian accounts claimed the soldier was of Moroccan origin, prompting a counterclaim from Moroccan users alleging he was Algerian. Fact-checking later confirmed both claims to be false.

Gradually, Lebanon was drawn into this web of digital conflict. The kickoff came with the launch of the "Shia Against the War" campaign, which our analysis identified as a coordinated effort involving Saudi and Emirati actors, along with Lebanese non-Shia accounts falsely claiming that all Shia opposed the war with Israel. While it is true that some members of the Shia community voiced opposition, many others publicly supported Hezbollah's stance and its backing of Gaza. External political involvement lent the campaign a clear tone of propaganda.[26]

These campaigns took on a more openly deceptive and inflammatory character following the assassination of Ismail Haniyeh, head of Hamas's political bureau, in Tehran in July 2024. Gulfi and Egyptian accounts were prominent in pushing the narrative that Haniyeh had previously orchestrated terrorist attacks in Egypt after the ousting of former president Mohamed Morsi of the Muslim Brotherhood.[27] Following Haniyeh's killing, a sectarian, coordinated campaign emerged accusing Shia groups of being behind the assassination. This, in turn, triggered a retaliatory campaign by Shia-affiliated accounts accusing Sunnis of "allying with Israel."

What stood out in the coordinated online campaigns related to the war in Gaza—whether directly or indirectly—was the deep division between forces providing military support to Gaza, such as Hezbollah in Lebanon and Iraqi militias, and others favoring diplomatic paths, like Egypt and Jordan. These campaigns also reflected internal divisions within individual countries. In Lebanon, for instance, anti-Hezbollah narratives clashed with pro-Hezbollah ones, while in Jordan, popular pro-Gaza protests became a target of smear campaigns.

What made these campaigns particularly noteworthy was their heavy reliance on disinformation. It wasn't just about promoting a specific narrative on social media; it also involved the deliberate spread of falsehoods embedded within those narratives—as seen in the reactions to the assassination of Ismail Haniyeh.

A pattern in these campaigns is their repetition during moments of regional conflict. Following Haniyeh's assassination, hashtags expressing glee over his death trended widely, with participation from coordinated and fake accounts, predominantly based in Saudi Arabia and Egypt. Some of these accounts also spread disinformation.[28] A similar campaign followed the assassination of Hezbollah's Secretary-General, Hassan Nasrallah, where Saudi and Egyptian accounts again launched celebratory and misleading posts about his life and role.[29]

Also noteworthy is the intersection of war with sectarian tensions and gender-based violence, as clearly seen in the campaign titled "[Food] Basket Jihad." This campaign targeted displaced women from southern Lebanon, accusing them of receiving food aid in exchange for sexual favors. It spread disinformation and circulated doctored videos, fueling hate speech and abuse against these women.[30]

[26] Lebanon: "Shia Against the War" Campaign with Saudi and Emirati Participation, Daraj, August 2, 2024

[27] Egyptian and Saudi Campaigns Gloating in the Death of Haniyeh, Daraj, August 2, 2024,

[28] Egyptian and Saudi Campaigns Gloating in the Death of Haniyeh, Daraj, August 2, 2024,

[29] Saudi and Egyptian accounts launch a coordinated disinformation and gloating campaign over Nasrallah's death, Daraj, last modified October 4, 2024,

[30] [Food] Basket Jihad: A Coordinated Hate Campaign Against Displaced Lebanese Women, Daraj, last modified November 2, 2024

Less Intense Conflicts

Other conflicts in the Middle East also unfolded on digital battlegrounds. While these conflicts may appear separate, they share common patterns and tactics—most notably, coordinated campaigns driven by external actors, the dissemination of disinformation, and the exacerbation of sectarian and political divisions.

In Yemen, for instance, two notable online campaigns emerged in which Emirati-affiliated actors played a prominent role, particularly in their support of the Southern Transitional Council (STC) in its confrontation with the Yemeni government.

In Sudan, Emirati influence was similarly evident through its backing of the Rapid Support Forces (RSF), reflected in coordinated online campaigns promoting narratives that favored the RSF, as part of broader efforts to shape public opinion in favor of the UAE's allies in the conflict.[31]

In Yemen, a coordinated online campaign was launched against Sheikh Ali Salem Al-Huraizi, head of the Mahra Sons Sit-in Committee, after he criticized the STC. This led to the circulation of high-quality videos and graphics containing criticisms of Al-Huraizi, which were widely disseminated among accounts supportive of the UAE.[32]

In Sudan, we observed that some of the accounts involved in the campaign criticizing Al-Huraizi also participated in another campaign defending UAE interests in Sudan and promoting its role in supporting the country. Meanwhile, those running the campaign criticized the Sudanese army for relying on Iran for its weapons.

This campaign was met with a coordinated counter-campaign supporting the Sudanese army, accusing the UAE of being involved in funding and arming the RSF to keep the war going. Pro-army accounts launched hashtags such as #الإمارات_تقتل_السودانيين (UAE Kills The Sudanese), #الإمارات_ترعى_الإرهاب (UAE Sponsors Terrorism), and #الإمارات_تسلح_ميليشيا_الدعم_السريع (UAE Arms Rapid Support Forces). [33]

Given the UAE's common involvement in both the Yemeni and Sudanese conflicts, Yemeni accounts opposing the UAE became active, such as that of journalist Anis Mansour, promoting hashtags associated with the campaign.

The same dynamic applied to Egypt's intervention in the Libyan conflict, which resurfaced after Egypt hosted the interim government's head in eastern Libya, Osama Hamad, prompting criticism from the existing Government of National Unity in Tripoli.[34]

[31] The Nairobi Declaration: Behind Abdalla Hamdok's Propaganda Campaign, Daraj, Last modified June 12, 2024

[32] Ali Al Huraizi: Yemeni Leader Praises Houthis and Provokes Electronic Trolls, Daraj, last modified April 18, 2024

[33] The Digital Conflict in Sudan: Accounts Supportive of the Army Overlook Its Violations and Seek to Impose Its Narrative, Daraj, Last modified July 8, 2024

[34] "Coordinated Egyptian Campaigns in Response to Libyan Foreign Ministry Criticism", Daraj, Last modified August 23, 2024

The division in Libya, and Egypt's support for the eastern government also cast a shadow over social media, with coordinated online campaigns under the hashtag #الشعب_المصري_يدعم_وحدة_ليبيا (The Egyptian People Support Libyan Unity) predominantly backing the political and military forces in the east while attacking Abdul Hamid Dbeibeh's transitional government in Tripoli.

Shia forces linked to Iran intervened in the Syrian military conflict by launching an online campaign in early December to counter the advances of armed factions. This campaign included incitement related to the use of barrel bombs, which the Syrian regime had previously deployed in the early years of the war, causing many civilian casualties. Meanwhile, from Turkey, a coordinated campaign supported online activity on Syrian accounts targeting the Syrian Democratic Forces (SDF) and inciting hostility against the Kurds.

Politics and Internal Strife

In second place come the coordinated campaigns with a political tone—particularly those linked to elections. We documented six coordinated online campaigns, three of which were related to elections in Algeria, Tunisia, and Jordan. Unlike armed conflicts, political contests like elections did not witness interference from regional powers seeking to influence their outcomes.

Intersecting factors played a role in shaping these coordinated electoral campaigns. In Algeria, for instance, the elections were accompanied by gender-based discrimination targeting female candidates. These candidates were subjected to organized online attacks aimed at discrediting their participation based on their gender. Hate speech was heavily employed in these campaigns, reinforcing discriminatory stereotypes against women in the political arena as online assaults escalated in an effort to obstruct their effective participation in the electoral process.[35]

The third notable feature of coordinated online campaigns in the context of elections is their persistent reliance on disinformation. For instance, one campaign targeting a candidate from Jordan's Islamic Action Front circulated a misleading video that had been taken out of context, falsely portraying the candidate as assaulting a local business.[36] In Tunisia, social media pages and groups devoted considerable space to spreading false claims about President Kais Saied's opponents. In response, other pages circulated fake news alleging that Saied had been summoned by the International Criminal Court on charges of "political persecution"—a claim that was entirely untrue.[37]

The Tunisian elections also marked the first instance of a network of Facebook pages supporting presidential candidate Ayachi Zammel deploying paid political ads to bolster his campaign. However, Meta removed many of these ads, citing violations of its advertising standards, including the failure to disclose the sponsor or properly label the posts as paid content. This raised questions about transparency and accountability in digital campaigning during elections.[38]

As for other politically driven campaigns, one originated in Egypt in response to criticism by the grandson of the late President Hosni Mubarak. He had compared the current economic hardships facing citizens under the present regime with conditions during his grandfather's rule. This prompted the launch of a coordinated digital campaign involving both fake and genuine pro-government accounts. The campaign sought to counter the criticism by attacking the state of affairs under the late president's leadership, effectively attempting to justify the current situation.[39]

Government-led campaigns against the opposition in Saudi Arabia have remained active. Alongside Egypt and Iraq, Saudi Arabia accounts for the largest share of coordinated digital campaigns, often waged through a network of pro-government accounts supporting the Saudi Crown Prince. One such politically charged campaign targeted Saudi dissident Salem Al Qahtani, a former air force officer who defected and voiced his opposition to what he described as "shielding those in power under a veneer of selective religious rhetoric."[40] He also spoke about the deteriorating conditions of military personnel and underperformers, while noting that "hundreds of millions are being burned on parties that offer no real value." Pro-government accounts responded to Al Qahtani by accusing him of being "mentally unstable" and a "drug addict," in an attempt to discredit him.

[35] "They Weren't Made for This": Algerian Female Presidential Candidates Face a Coordinated Discrimination Campaign Online, Daraj, Last modified July 29, 2024,

[36] Jordan: Pro-Government Accounts Lead Smear Campaign Against Wissam Rabihat, Candidate of the Islamic Action Front, Daraj, Last modified September 21, 2024

[37] "Foreign Funding of Protests" and "Kais Before the ICC": The Tunisian Power Struggle Spills into Cyberspace, Daraj, Last modified October 1, 2024,

[38] "Foreign Funding of Protests" and "Kais Before the ICC": The Tunisian Power Struggle Spills into Cyberspace, Daraj, Last modified October 1, 2024

[39] A Comparison Between Two Eras Sparks Fierce Campaign Between Supporters of Sisi and those of Mubarak, Daraj, Lastmodified Febraury 7, 2024

[40] "Salem Al Qahtani: "Defection" of an Officer Sparks Coordinated Campaign Against the Saudi Opposition", Daraj, Last modified March 22, 2024,

In Egypt, a large-scale campaign targeted political activist Ahmed Douma and former presidential candidate Hamdeen Sabahi following their criticism of reports about the docking of the ship Kathrin, which was allegedly carrying weapons destined for Israel. The campaign used inflammatory rhetoric calling for the arrest of anyone opposing the ship's docking, aiming to discredit the opponents and accuse them of spreading rumors.[41]

A common thread among many coordinated online campaigns is the use of hate speech and incitement against opponents. This rhetoric has been deployed against Algerian female candidates, critics of President Kais Saied, as well as in the electoral battle in Jordan, and against the Saudi dissident Salem Al Qahtani. The purpose of this discourse was to tarnish the reputations of the targeted individuals and to mobilize public sentiment against them, reflecting the exploitation of technology to deepen political and social divisions.

This also raises questions about the effectiveness of the policies of social media platforms in combating hate speech, as outlined in their published codes of ethics and community standards.

[40] «سالم القحطاني.. «انشقاق» ضابط يثير حملة منسّقة ضد المعارضة السعوديّة”, Daraj, Last modified March 22, 2024,

[41] «السفينة «كاثرين» في مصر… حملة ضد المُنتقدين وتحقيقات بتهمة «نشر الشائعات»», Daraj, Last modified November 19, 2024

Most Vulnerable Groups

Minorities, migrants, refugees, and the LGBTQ+ community are frequent targets of coordinated online campaigns, especially those promoting hate speech against them. These campaigns are supported by disinformation aimed at tarnishing the image of these groups and turning public opinion against them. Arabi Facts Hub has identified three coordinated digital campaigns linked to gender and sexual identity, all accompanied by hate speech and false content.

The United Nations defines hate speech as any form of communication—whether verbal, written, or behavioral—that attacks or uses pejorative or discriminatory language against an individual or group based on their identity, such as religion, ethnicity, nationality, race, color, descent, gender, or other identity factors; in a manner that poses a threat to social peace.

The Internet Governance Forum defines gender-based misinformation as a type of misinformation that targets individuals based on their gender and exploits stereotypical gender narratives to achieve political, social, or economic objectives.[42]

Gender-based disinformation often overlaps with technology-based gender violence, which refers to violence occurring through digital and technological media, targeting individuals based on their gender. This type of violence includes using technology to commit acts involving harm or defamation, causing damage to individuals because of their gender

The first of these campaigns targeted Egyptian student Nayera El Zoghby, known as the "Arish Girl." El Zoghby was subjected to a smear campaign after her death in 2024. The campaign aimed to tarnish her reputation by alleging that she had engaged in a relationship outside of marriage, in an attempt to weaken public sympathy for her and direct moral accusations at her.[43] The campaign circulated disinformation claiming that "the girl had committed suicide," prompting the Public Prosecution to issue a warning against "spreading false information" regarding the incident, after permitting an autopsy of the student's body.

We also observed the intersection of gender-based disinformation with political issues, as previously noted in our discussion of the discriminatory online campaign targeting female candidates in Algeria's 2024 presidential elections. Analysis of the campaign indicates a deliberate effort to smear the candidates and discriminate against them based on their gender. The campaign promoted the notion that leadership and political office are not suitable for women, and that men are more qualified for such roles—regardless of the women's qualifications, capabilities, or electoral platforms.

.

[42] «Best Practice Forum on Gender and Digital Rights» IGF, 2021,

[43] Campaign against the "Arish Girl" Led by Egyptian Accounts Affiliated with the Regime, Daraj, Last modified March 19, 2024,

Iraq ranked among the top countries witnessing coordinated online campaigns related to gender issues. These were led by Shiite political forces that launched hate campaigns against the LGBTQ+ community. The campaigns aimed to defame and incite hatred toward the community in an effort to support the passage of a law criminalizing same-sex relationships. A coordinated online campaign, supported by Shiite factions, also emerged to endorse proposed amendments to Iraq's Personal Status Law, while smearing opponents of these changes. The campaign used AI-generated images to fabricate scenes of supposed demonstrations backing the amendments, in an attempt to bolster public support for the legal changes.[44]

In addition to incitement and the spread of disinformation in such campaigns using artificial intelligence, a network of fake accounts with low follower counts has been observed actively resharing content and amplifying activity on hashtags. These accounts aim to mislead public opinion by creating a false impression of popular support, thereby generating a fabricated perception of the scale of endorsement or opposition to certain issues, and ultimately contributing to the manipulation of public opinion.

Ranked second among the most vulnerable groups targeted by coordinated online campaigns are refugees and migrants. These groups were especially targeted in Egypt, where disinformation campaigns were launched concerning the number of Sudanese and Syrian refugees—particularly after the influx of Sudanese nationals into Egypt following the outbreak of war in Sudan in April 2023.

AFH analyzed three campaigns targeting Syrian and Sudanese refugees. One of these campaigns was launched under the hashtag "Report a Refugee" and involved a coordinated effort against refugees in Egypt. It included language and expressions laden with hate speech—some of which dehumanized refugees or diminished their worth, while others directly incited hostility toward them. This campaign specifically targeted Sudanese refugees, spreading misleading videos of fabricated deportation operations of Sudanese individuals from Egypt. [45]

This campaign was preceded by another that called for the boycott of Syrian-owned businesses in Egypt, alongside the recirculation of news claiming that some Syrian restaurants were shut down for allegedly using expired meat. A network of fake accounts actively promoted this narrative, pushing it into the list of trending topics in Egypt. The campaign was launched by Egyptian accounts supportive of the regime, which had previously attacked critics of the government and participated in official events by invitation from government entities.

The same accounts became active again when the Egyptian Parliament gave initial approval to the draft law on Asylum, launching eight hashtags inciting hostility against refugees and promoting claims that refugees are responsible for Egypt's economic crisis and the rising cost of living—especially housing rents.

In conclusion, the coordinated campaigns targeting the most vulnerable groups consistently show a deliberate effort to spread disinformation and hate speech, supported by networks of fake accounts to amplify their messaging. These campaigns also intersect with politics, at times originating from accounts affiliated with sectarian political forces, and at other times from accounts aligned with or supportive of the government.

[44] Iraq: Shiite Forces Launch Online Campaign in Support of Child Marriage Law, Daraj, Last modified September 11, 2024

[45] "Report A Refugee": A Wave of Incitement Against Refugees Led by Proponents of the Egyptian Regime", Daraj, Last modified July 22, 2024,

Account Network Analysis

This section is divided into two parts: the first addresses the countries most frequently targeted by coordinated digital campaigns, while the second outlines the countries from which these campaigns were launched.

Our data analysis indicates that Egypt was the most targeted country, with a total of ten campaigns. It is followed by Saudi Arabia, which witnessed four campaigns—equal to the numbers seen in Lebanon and Palestine. Iraq followed with three campaigns, then Sudan and Jordan with two each.

Also worth noting is the emergence of regionally themed campaigns—those launched simultaneously from multiple countries in response to regional events, such as the Iranian attacks on Israel, or the deaths of Ismail Haniyeh, the head of Hamas's political bureau, and Hassan Nasrallah, the secretary-general of Hezbollah.

Egyptian accounts launched 13 campaigns, placing Egypt at the top of the list of countries where accounts are most actively involved in coordinated digital campaigns. It is followed by Saudi Arabia with a total of ten campaigns. Iraq ranks third with nine campaigns, followed by the UAE with participation in eight campaigns, and Lebanon, which took part in six coordinated online campaigns.

It is notable that the number of campaigns originating from countries such as Egypt, Saudi Arabia, the UAE, and Iraq exceeds the number of campaigns focused on the internal affairs of these same countries. This is because many of the coordinated online campaigns launched from these states engage with regional issues and reflect the interests of their respective governments, often acting in defense of those interests.

Egyptian-launched campaigns were particularly prominent during the war on Gaza—especially in reaction to events such as the deaths of Ismail Haniyeh and Hassan Nasrallah, and rumors about Hamas being expelled from Qatar. These campaigns were not limited to Gaza; they also extended to Sudan, supporting Egypt's stance against the Rapid Support Forces and in favor of the Sudanese army.

A similar trend applies to Saudi Arabia, whose digital networks engaged with anti-war protests in Jordan and promoted narratives about Saudi Arabia's role in achieving international recognition for Palestine. These campaigns often took on a sectarian tone, such as those titled "Shiites Against the War" and "Shiites Assassinated Haniyeh." Pro-Saudi networks celebrated the deaths of Haniyeh and Nasrallah and circulated claims that Hamas had been expelled from Qatar.

The country where this pattern is most evident is the UAE. Although it was not the target of any coordinated online campaigns, its digital networks launched multiple campaigns in defense of Emirati interests in regional conflicts—particularly in Palestine, Yemen, and Sudan.

Organized Online Armies

The countries actively engaged in coordinated online campaigns have a network of accounts that frequently launch or participate in such efforts. Within each country, there are specific accounts that can be described as “whistleblowers”—the ones initiating the campaigns. In addition, there are other accounts—usually with fewer followers—that contribute to the campaigns by engaging through likes, reposts, replies, or quote tweets.

Some accounts on X (formerly Twitter) explicitly label themselves with names that reflect their affiliations or ideological leanings, such as “The Salmani Electronic Army” and “Saudi Digital Hawks.” Similarly, on Facebook, accounts have grouped under names like “The Egyptian Coalition for Social Media”—a group whose administrators have reportedly attended official events such as The Egyptian Family Iftar and the World Youth Forum.

In Egypt, the most prominent account on X is known as El Masri, also referred to as “The Maestro.” This account is known for regularly launching digital campaigns, particularly those targeting refugees. Our research revealed that “The Maestro’s” real name is Bassem Bakhit, and he resides in the Ain Shams district of Cairo.

To bypass the platform’s policies, he frequently changes his account handle and maintains multiple accounts on X. The Maestro openly encourages the use of hashtags and explains their intended purpose. Some of the hashtags he has promoted include direct incitement, such as the hashtag #بلغ_عن_لاجئ (Report A Refugee), where he called on users to “assist the Ministry of Interior in locating refugees or undocumented residents, and to determine whether their status has been rectified or if they should be deported.”[46]

The Salmani Electronic Army is active in defending Saudi Arabia’s interests. It typically adopts an aggressive tone and incites against critics of the Saudi regime. This group has hundreds of members and functions as a pressure group that operates in coordination with Saudi figures in the digital space. It also employs a vast network of fake accounts. In addition to its campaigns, the collective includes various units tasked with different roles such as hacking operations and account takeovers.

Amid escalating political tensions in the region and the rise of narratives critical of Saudi Arabia and supportive of Iran-aligned forces, sub-groups have emerged within the Salmani Electronic Army — notably the “Saudi Digital Hawks”. This subgroup is active on X, operating through accounts estimated to include around 16,000 members. It is managed by the account of Salman bin Hathleen, a long-time participant in Saudi propaganda campaigns, with more than 517,000 followers.

Across the Gulf countries, there are also several accounts that begin with the name “Radʿ” (meaning “deterrence”), such as “Radʿ Saudi” and “Radʿ Abu Dhabi.” The “Radʿ Saudi” account describes itself as a social media influencer — a label commonly adopted by Saudi and Yemeni accounts to reflect their online activity — and uses a banner identical to that of the “Saudi Digital Hawks” group. The “Radʿ Abu Dhabi” account conducts or joins coordinated online campaigns in support of the official policies of the United Arab Emirates (UAE).

[46] A Campaign Against “Naturalizing Refugees”... What is the Story?, Daraj, Last modified May 25, 2023

UAE digital campaigns are frequently in coordination with networks of accounts defending Emirati interests in conflict zones. These accounts collaborate and alternate participation across campaigns. For instance, the production style of the "Hamdok" campaign resembles that of another campaign targeting Ali Salem Al-Huraizi, a leader in Yemen's Al Mahrah governorate. Accounts supportive of the UAE, such as the anonymous "Batool Al Khair" and the "Ijaz Yemeni Network" — managed from Egypt, the UAE, and Yemen — were involved in both campaigns.

Other social media platforms also take part in the Sudanese conflict and identify themselves as Sudanese, such as the website "Barq Al Sudan". Data from its YouTube account indicates it is operated from the UAE, and its content promotes Emirati propaganda, using phrases such as "The Benevolence of the Emirates" and "Zayed's Genius." The site's social media accounts have long been involved in campaigns defending the UAE's interests in Sudan. [47]

On the other side, Iran-aligned digital collectives are prominent—such as the electronic networks of the Popular Mobilization Forces (PMF) in Iraq, the digital collectives supporting the Houthi movement in Yemen, and those backing Hezbollah in Lebanon. These groups rely on networks of fake accounts, which have previously been used to launch coordinated campaigns. One such campaign targeted Jordan, and was initiated by accounts supportive of the Iraqi PMF, accusing Jordan of bombing Iraq and supporting the U.S. and Israel, following American airstrikes in Iraq earlier this year.

Some posts in this campaign included the term "Hashdawi", a word used in a similar way to "social influencer"—a label often adopted by Saudi electronic groups in their online activities. [48]

Just as Egyptian digital groups operate across platforms—often using Facebook to launch their campaigns— Iran-aligned groups tend to use Telegram to create their own channels, such as the "Maydan Mannaset Al-E'lam Al-Muqawim" (Resistance Media Platform) channel, from which they launch propaganda campaigns in support of the PMF.

The name of this channel resembles another Telegram channel, "Multaqa Al-E'lam Al-Muqawim – CIMIA", which is linked to Hezbollah's digital operations. It regularly launches campaigns expressing the party's views and stances—including smear campaigns and trolling efforts.

This media hub also operates multiple social media accounts that engage simultaneously when campaigns are launched. For instance, it spearheaded a solidarity campaign for Lebanese nun Maya Ziyadeh, who faced backlash after publicly expressing support for Hezbollah's military operations against Israel in southern Lebanon.[49]

There are also multiple Telegram channels based on geographic regions. For example, the Tasnim Center for Resistance Media in the Bekaa region regularly rebroadcasts content from the main channel CIMIA, and assists in disseminating campaign materials.

[47] Coordinated Online Campaigns Targeting Sudan, Daraj, Last modified October 16, 2024

[48] Iraqi Militia Accounts: "Jordan Will Pay", Daraj, Last modified February 14, 2024

[49] Lebanese Nun Maya Ziyadeh's Call to Prayer for the South Sparks Wave of Incitement and Another of Solidarity, Daraj, Last modified April 2, 2024,

The Nasim Center is linked to a network of fake accounts that publish the same content. Indicators suggest that this network is automated, as evidenced by the similarity of posts, low follower counts, high posting frequency, and a consistent focus on regional issues related to Hezbollah and Iran.

This does not mean that campaigns reflecting the interests of Iran-aligned forces are entirely automated. Hezbollah campaigns, for instance, receive support from prominent figures such as Jawad Nasrallah, the son of Hezbollah's former Secretary-General Hassan Nasrallah, and Hussein Mortada, the director of the Sonar Media Center.

In Iraq, certain accounts have played a mobilizing role in coordinated campaigns, including that of journalist Zohair Al Qassem, a frequent guest on PMF-aligned media platforms, and Ahmed Abdul-Sada, whom Iraqi news outlets have accused of inciting violence against intellectual Hisham al-Hashimi, who was assassinated in July 2020. Abdul-Sada also relayed threats from the Fatah Alliance—affiliated with the PMF—to launch drone and ballistic missile attacks against the UAE in protest of the October 2021 election results.

Violation of Social Media Platform Policies

X's policies prohibit manipulation and spam content. The platform states: "You may not use X's services in a manner intended to artificially amplify or suppress information." [50]

The platform's policies also ban "inauthentic engagements that attempt to make accounts or content appear more popular or active than they actually are," as well as "coordinated activity that seeks to manipulate conversations artificially through the use of multiple accounts, fake accounts, automation, and/or scripting." [51]

Previously, Twitter shut down around 6,000 accounts believed to be supported by Saudi authorities for spreading government narratives. Despite this, we found that X continues to host extensive activity by the Salmani Electronic Army cluster and its associated fake accounts that actively support the Saudi regime, as previously explained. Likewise, a network of fake accounts tied to pro-Iranian forces operates in Iraq—backed by the PMF—and supported in Lebanon by Hezbollah-affiliated accounts.

Some accounts have routinely evaded X's policies, particularly "whistleblower" figures such as Bassem Bakhit, known as El Maestro. Each time the platform restricted his access, he quickly returned using variations of similarly named accounts. If one account was suspended, he would reappear with another or change the account's handle. Bassem operates multiple accounts with different handles, including: @bassembekhet1 – @basemelmassry3 – @bassemelmassry.

Although X claims to prohibit hate speech and forbid incitement or dehumanizing insinuations, including the use of hateful imagery and symbols—as it claims to protect marginalized groups by banning "inciteful behavior targeting individuals or groups belonging to protected categories"—there have been documented campaigns inciting hatred against minorities, marginalized communities, LGBTQ+ individuals, and refugees. This shows that the company has failed to make the necessary efforts or invest sufficient resources to protect these groups from harmful content across its platforms, which often translates into real-world harm.

For example, during the "Report A Refugee" campaign in Egypt, numerous phrases and expressions classified as hate speech were published, ranging from demeaning refugees and dehumanizing them—comparing them to animals or invaders—to explicit incitement, including calls for violence like "crush them." Smear campaigns also targeted women opposing amendments to Iraq's personal status law, as well as female presidential candidates in Algeria. Yet X took no action against these campaigns.

Some of these coordinated online campaigns included disinformation. Despite such content violating the policies of platforms like X and Facebook, it continued to spread unchecked. X took no meaningful action except attaching disclaimers—only after the Arabi Facts Hub revealed a coordinated campaign targeting Wissam Rabihat, a candidate from the Islamic Action Front Party in Jordan.

[50] https://help.x.com/en/rules-and-policies/platform-manipulation
[51] https://help.x.com/en/rules-and-policies/platform-manipulation

Outcomes

Many governments in the Middle East and North Africa employ cybercrime and anti-terrorism laws to restrict citizens' digital rights, exploiting these laws to suppress opponents, journalists, and activists under broad charges such as "spreading false news" or "undermining state authority." This report reviews examples from Saudi Arabia, Egypt, Bahrain, the UAE, Iraq, Jordan, Tunisia, Morocco, and Mauritania to illustrate how these laws are arbitrarily used to criminalize legitimate digital activity. Severe penalties, including imprisonment and heavy fines, are imposed, and individuals face prosecution for social media posts. The observed cases demonstrate that these laws are not primarily aimed at protecting security or combating disinformation but serve as tools for controlling public discourse, shrinking civic spaces, and suppressing freedom of expression. These practices raise serious human rights concerns as they conflict with international human rights standards and underscore the urgent need for comprehensive review of these laws to ensure digital rights protection.

In 2024, there was a notable increase in disinformation across the MENA region. AFH and its partners classified content into categories such as false, partially false, satirical, investigative, and unspecified. In 2024, AFH monitored 5,402 topics from 23 fact-checking platforms in the Arab world, classifying 90% as "false," including 185 AI-generated items, mostly political. Visual content (images and videos) was the most circulated at 41%, followed by texts and statements, and lastly data and numbers, due to difficulty accessing official information.

Political topics dominated 72% of disinformation, followed by miscellaneous at 12%, social issues at 5%, and other topics such as economy, health, and technology. Palestine was the most targeted at 14%, followed by Yemen and Syria, due to major political events—especially the war on Gaza, which alone accounted for 18% of fact-checked content, 96% of which was deemed false.

Other prominent topics included the Houthi targeting of ships, which accounted for 33% of Yemen-related content, mostly fake or AI-generated, often using old videos or gaming footage as purported recent events. In the United States, rumors about elections, Trump, and Biden were widespread, all classified as disinformation. In Egypt, economic issues were prominent, such as government statements on electricity subsidies proven inaccurate. Other claims involved unemployment, foreign debt, with 30% relating to commodity shortages and price increases. Lastly, some false claims targeted the Paris Olympics, like the fabricated story about Algerian athlete Imane Khalif, part of a smear campaign.

The report's final section highlights the use of coordinated online campaigns as political and social weapons amid weak investment in user protection on social media platforms. The vast majority of monitored campaigns focused on military conflicts, especially the war in Gaza, targeting individuals such as Al Jazeera journalists, UNRWA staff, and even religious figures like Sister Maya Ziyadeh in Lebanon. Some campaigns involved regional actors supporting Gaza or opposing Hezbollah, fueling sectarian feuds and inciting campaigns among parties. The use of AI and fabricated materials further complicated monitoring.

These campaigns extended beyond Gaza to conflicts in Yemen, Sudan, and Libya, where regional powers like the UAE played a significant role in directing campaigns supporting their political and military allies. In Yemen, Sheikh Ali Al Huraizi faced a smear campaign; in Sudan, reciprocal campaigns erupted between supporters of the army and Rapid Support Forces. Libya's political divides were mirrored on social media, with campaigns promoting Egypt-backed eastern Libya against the Tripoli government. In Syria and Turkey, inciting campaigns targeted Kurds and the SDF, with calls for severe bombardment using barrel bombs.

Campaigns related to elections in Algeria, Tunisia, and Jordan emerged, using hate speech and disinformation to discredit candidates, especially women. Other campaigns targeted political opponents such as Salem Al Qahtani in Saudi Arabia and Ahmed Douma in Egypt, with hate speech frequently employed.

Direct incitement against marginalized groups, such as refugees and LGBTQ+ communities, was observed, including calls for violence and disinformation, with ineffective social media platform responses—as seen with the "" of Nayerra El Zoghbi, Algerian election candidates, and anti-LGBTQ+ campaigns in Iraq. These campaigns remain key tools serving state political interests and shaping public opinion on sensitive regional issues, amid a clear lack of serious protection by social media companies.

Data indicates these campaigns are often on a regional level, involving accounts from multiple countries responding to major events like the Gaza war or political assassinations. The campaigns show coordinated involvement from account networks managed within known groups, such as Saudi Arabia's Salmani Electronic Army, Egypt's Maestro, and coalitions supporting the UAE, Popular Mobilization Forces, and Hezbollah in Iraq and Lebanon.

These accounts have an organized character, acting as propaganda arms for the states or groups they represent by launching hashtags, inciting, and spreading similar content via fake accounts. Platforms like X play a negative role by allowing this harmful content despite its clear violation of X's policies on content manipulation.

Recommendations

Although work on this report began at the end of 2024—prior to major policy changes by major companies such as Meta, including the termination of its fact-checking program and the loosening of hate speech policies (particularly regarding women, LGBTQ+ communities, and migrants)—it has become clear that these platforms have long served as fertile ground for incitement against these groups, especially in the MENA region. Furthermore, some regimes in the region have systematically exploited these platforms to smear human rights defenders and journalists and to orchestrate coordinated online campaigns against them, ultimately restricting their work.

The failure of platforms like Meta and X, among others, to take decisive action to protect individuals and communities from digital harm—whether directly or indirectly caused by these platforms—makes them complicit in such harm.

The indicators presented in this report reveal an alarming rise in digital rights violations, directly threatening online freedoms. These violations, which stem from varied and increasingly complex sources, demand an urgent and comprehensive response. As such, this section presents a set of practical, targeted recommendations aimed at enhancing cybersecurity and protecting citizens' digital rights in the face of mounting threats, with a focus on the roles of governments, civil society organizations, and technology companies.

Practical Recommendations for Governments and Policymakers

Governments in the MENA region are involved in systematic digital rights violations, whether through enacting troubling legislation that is weaponized to suppress freedom of expression or through the misuse of social media platforms to disseminate state-sponsored narratives via coordinated campaigns that include incitement or defamation against political opponents, or to interfere in the affairs of other regional countries. In this context, this report recommends that governments:

1. **Support Human Rights in the Digital Sphere:** Governments must uphold human rights broadly and specifically in the digital space by protecting users' rights, including their right to privacy, freedom of expression, and access to information.

2. **Align with International Standards:** Ensure that local laws and their implementation align with international human rights standards, including guaranteeing free and open access to the internet.

3. **Prevent Internet Restrictions:** Refrain from imposing internet shutdowns or blocking websites, and enact laws that protect citizens' digital rights from infringement.

4. **International Pressure for Reforms and Releases:** Foreign governments should publicly call for the immediate release of individuals imprisoned for online expression or dissent and push for the repeal of unjust cybercrime laws.

5. **Reform Cybercrime Legislation:** External governments should press MENA states to revise cybercrime laws in accordance with international human rights standards and halt the misuse of anti-terrorism and other laws to suppress legitimate expression.

6. **Condition Foreign Aid on Rights Protections:** Governments providing aid to MENA states should impose human rights and digital rights conditions on that assistance.

Practical Recommendations for Civil Society

Document and Report Violations: Continue and expand efforts to monitor and document digital rights violations in the Arab region, and produce regular reports on the state of digital rights.

Advocacy Campaigns: Intensify advocacy efforts on digital rights issues at local, regional, and international levels to increase pressure on both governments and tech companies to respect and invest in protecting citizens' digital rights.

Cybersecurity Training: Organize intensive training programs for activists and human rights defenders in digital security and privacy protection.

Invest in Infrastructure: Invest in building independent digital infrastructure for civil society organizations to strengthen their resilience and protect them from recurring violations by companies in the absence of regulatory safeguards.

Build Alliances: Strengthen coalitions and partnerships to build a powerful digital rights movement in the region.

Provide Legal and Psychological Support: Offer legal and psychological assistance to activists, journalists, human rights defenders, women, LGBTQ+ individuals, migrants, and others in the region who have been victims of digital violations.

Raise Public Awareness: Launch large-scale awareness campaigns on the importance of digital rights protection.

Practical Recommendations for Tech Companies

1. **Prioritize User Protection:** Companies must prioritize user protection—especially for those systematically targeted by governments in the region, such as activists, dissidents, human rights defenders, journalists, women, and LGBTQ+ individuals.

2. **Invest in Content Moderation:** Companies should increase investment in content moderation programs and ensure their sustainability instead of phasing them out, as Meta recently did. These programs must be effective and transparent in monitoring harmful and discriminatory content.

3. **Transparency and Government Collaboration Disclosure:** Companies must publish detailed reports disclosing financial and human resources dedicated to user protection, and publicly reveal the nature of their cooperation with regional governments, including requests received and how they respond.

4. **Provide Tools to Civil Society and Researchers:** Companies should commit to offering tools that enable researchers and civil society to access and analyze platform data for independent studies—rather than eliminating tools like CrowdTangle, which Meta discontinued in 2024.

5. **Conduct Independent Human Rights Assessments:** Companies must carry out independent and public human rights impact assessments to ensure their operations do not harm marginalized communities in conflict zones. These evaluations should be conducted regularly to ensure compliance with international human rights standards.

6. **Expose Misleading Networks and Accounts:** Companies must significantly invest in identifying and dismantling networks and accounts that systematically promote misleading or defamatory narratives through coordinated campaigns. They should allocate trained and locally aware staff to investigate and publicly report on these networks. Strengthening specialized teams is critical to ensuring companies can effectively counter such operations with transparency and integrity.

Conclusion

This inaugural report demonstrates that information disorder in MENA is not merely a problem of false content but a structural challenge shaped by repressive laws, unchecked disinformation, and coordinated manipulation. Tackling these issues requires sustained collaboration between governments, civil society, and technology companies. AFH’s annual monitoring will continue to provide evidence and analysis to strengthen advocacy and promote digital rights in the MENA region.

مجتمع التحقق العربي

Arabi Facts Hub

2024 Annual Report