Civil Society Alliances for Digital Empowerment

Co-funded by the European Union

SMEX

Civil Society Organizations' Engagement in Internet Governance Legal Frameworks: The Case of Cybercrime Laws

MENA Case Study

Updated December 2025

Acknowledgments

This study was conducted by SMEX, a non-profit that advocates for and advances human rights in digital spaces across West Asia and North Africa, as part of its work on the CADE project (Civil Society Alliances for Digital Empowerment), a project co-funded by the European Union. This project includes expert organizations from different regions. It aims to enhance the capacity of Civil Society organizations (CSOs) for effective advocacy in multilateral and multistakeholder internet governance (IG) processes, including cybercrime laws, tackled in this paper.

Author: Afnan Abu Yahia

SMEX's research and editorial teams worked collaboratively at every stage of this project, providing essential support in reviewing, refining, and strengthening the research. Special thanks are due to **Abed Kataya** for his critical role in supervising the research process and **Nathan Silber** for his valuable comments, which improved the quality of this paper.

Appreciation is also extended to the Diplo team, specifically **Stephanie Borg Psaila**, **Slavica Karajicic**, and **Kenneth Harry Msiska** from Forus, for their constant follow-up and thoughtful insights, as well as CSOs and activists in Jordan, Egypt, Tunisia, Iraq, KSA and Bahrain, who gave their valuable time to participate in the interview process of this study

This publication was co-funded by the European Union. Its contents are the sole responsibility of SMEX and do not necessarily reflect the views of the European Union.

.

Case Study Update

Since our initial MENA Case Study was published in 2025, the legal landscape across West Asia and North Africa (WANA) has continued to shift in ways that directly affect civil society's space for advocacy. In the countries covered in the case study, reforms to cybercrime and other laws regulating the online sphere have broadened state control over online speech and freedom of expression, often with extensive enforcement that disproportionately targets dissent, and ultimately hinders CSOs involvement in lawmaking. These same laws, adopted without civil society involvement,are constantly being used by state authorities to silence it, as illustrated by the following examples.

In 2024, Jordan persecuted people in more than 3,100 cases under the provisions of its amended cybercrime law of 2023, mostly for alleged online defamation. Authorities have additionally blocked a dozen local and foreign websites from operating in Jordan for "spreading media poison and attacking Jordan." Other abuses of the cybercrime law involved the arbitrary arrest of several dissidents, including Ayman Sandouka for a tweet he posted in 2023 criticizing Jordan's King for his government's relationship with Israel. This law had previously been used to prosecute people under the pretext that they were undermining national unity. In a continuous advocacy effort to amend the law, Jordan's National Center for Human Rights (المركز الوطني لحقوق الإنسان) publicly called for a comprehensive review and amendment of Jordan's Cybercrime Law in April-May 2025. Other organizations in the region, including SMEX and Access Now, had also previously sent an open letter to the King of Jordan urging him not to approve the Cybercrime Law in the first place.

In Tunisia, the 2022 Decree-Law 54 on cybercrime, still heavily used to persecute people in 2025, criminalizes *"spreading false news"* and grants the authorities broad surveillance powers, resulting in numerous prosecutions of journalists and critics. Authorities have leveraged this law in 2025 to detain and sentence multiple individuals for social media posts and public criticism, both online and offline, of government entities. According to Human Rights Watch, multiple previous and current government figures were also sentenced, including former President Moncef Marzouki, a critic of the current President Saied for "*undermining state security.*" Other dissidents were also prosecuted on different charges, all known for being critical of the current President. In 2025, Tunisian civil society groups, including the Syndicat National des Journalistes Tunisiens and the Tunisian League for Human Rights publicly called for the amendment or repeal of Decree-Law 54, urging the African Commission on Human and Peoples' Rights to address its misuse against journalists and free expression.

Egypt's broader criminal justice reforms, including a revised Criminal Procedure Code enacted in late 2024, further eroded due-process protections and empowered law enforcement agencies to detain and prosecute people who practice their right to freedom of expression online under provisions broadly referring to public order and morals. According to Human Rights Watch's 2026 World Report, Egypt has detained over 23 journalists for matters like Facebook posts criticizing some government policies. In a long awaited win for civil society after years of mounting pressure, Alaa Abdel Fattah, an activist who had been

held by the Egyptian authorities since 2014, was finally freed in 2025, having received a presidential pardon.

In Bahrain and Saudi Arabia, authorities continue to use an array of security and cyber-related statutes to monitor and suppress online dissent, detaining activists for social media posts and blocking content critical of the state. Multiple CSOs have also multiplied their media advocacy efforts denouncing the two countries' human rights abuses, including abuses of online freedom of expression. In 2025, Bahrain's government had also approved amendments to the Law on Press, Printing, and Publishing that allegedly aimed to regulate online publications and protect journalists. However, some CSOs also expressed their concerns surrounding these amendments, which they argued could further restrict freedom of expression.

In the WANA region, progress on reforming cybercrime regulations still remains limited, despite sustained advocacy by civil society to amend restrictive and oppressive legal frameworks. Despite that, CSOs across the region continue to organize and demand meaningful participation in shaping cybercrime legislation. This makes our analysis and case study all the more relevant in 2026, as civil society persists in exploring innovative and strategic pathways to ensure their perspectives and expertise are reflected in regulatory reform, particularly cybercrime laws.

Executive Summary

Civil Society Organizations (CSOs) play a crucial role in shaping digital infrastructure and internet governance, including cybercrime laws. Their role has become even more critical in the context of increasing crackdowns on freedom of expression and civic engagement. This case study explores how CSOs in the Arab region, particularly in Iraq, Egypt, Jordan, Tunisia, Bahrain, and Saudi Arabia, have engaged in the development of cybercrime legal frameworks.

Using a qualitative methodology, the study assesses the level of CSO involvement in these countries' drafting, enactment, and amendment of cybercrime laws, based on in-depth interviews with digital rights activists and organizations. The paper concludes that CSOs influence on cybercrime laws has been limited, despite their wide range of advocacy methods, including lobbying, awareness-raising, legal advocacy, coalition-building, direct action, international advocacy, and digital advocacy. It identifies the tools and techniques used by CSOs to influence the lawmaking process and analyzes the effectiveness of their efforts, highlighting both the challenges and successes encountered. Lastly, the paper contains recommendations to improve the engagement of civil society in cybercrime lawmaking and strengthening their advocacy strategies.

Introduction

According to the United Nations Office on Drugs and Crime,[1] cybercrime law "identifies standards of acceptable behaviour for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilitates cooperation between countries on cybercrime matters."

This definition highlights the importance of the law at addressing and combating the rise of digital crime in West Asia and North Africa, as stated in IBM's "Cost of a Data Breach" report[2]. However, cybercrime laws in West Asia and North Africa are frequently used by governments to suppress dissent, posing a threat to freedom of expression.[3] Many of cybercrime laws in West Asia and North Africa prohibit various forms of online speech using broad and unclear language that legitimize prosecuting human rights defenders who criticise governments and officials. According to the National Center for Human Rights report,[4] Jordan arrested 1,821 individuals in 2018 under its Cybercrime Law, most of them academics, media activists, online journalists, and other citizens, on charges of defamation, slander, and contempt that were brought against them by public figures.

Conversely, cybercrime laws in West Asia and North Africa raised other concerns over data privacy. Some laws allow surveillance data interception without safeguards, in addition to enabling internet service providers to process data without the need for judicial authorization or users' pre-consent. A policy paper published by Access Now in 2024[5] has stated that this kind of mass data collection and processing allows for precise conclusions to be inferred about people's daily habits and movements, their usual place of residence, their social connections, and other details.

These regulations have been widely slammed by CSOs[6] that often face significant challenges in participating meaningfully in law issuance processes, even in areas that directly affect their operations. Cybercrime laws are a crucial regulatory aspect of internet governance[7] because they impose restrictions on human rights

---

[1] Law Society of South Africa, "CYBER LAW," April, 2023, https://www.lssa.org.za/wp-content/uploads/2023/04/Cyber-law.pdf

[2] IBM, *Cost of a Data Breach Report*, 2025, https://www.ibm.com/reports/data-breach

[3] Yahya Shqair, "Cybercrime Laws in Arab Countries: Focus on Jordan, Egypt and the UAE", Arab Reporters for Investigative Journalism (ARIJ) and the Friedrich Naumann Foundation for Freedom, May 10, 2020, https://en.arij.net/wp-content/uploads/sites/3/2019/12/Cyber-Crime-Laws-in-the-Arab-world-Policy-paper-by-ARIJ.pdf

[4] Rana Husseini, "NCHR report reveals Kingdom's human rights situation in 2018," Jordan Times, November 5, 2019, https://jordantimes.com/news/local/nchr-report-reveals-kingdoms-human-rights-situation-2018

[5] Access Now, "Analysis of cybercrime laws in the Arab region," November 27, 2024, https://www.accessnow.org/wp-content/uploads/2024/11/%D9%82%D9%88%D8%A7%D9%86%D9%8A

[6] Human Rights Watch, "Jordan: Scrap Draconian Cybercrimes Bill," July 24, 2023, https://www.hrw.org/news/2023/07/24/jordan-scrap-draconian-cybercrimes-bill

[7] United Nations Office on Drugs and Crime, "Internet governance," https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/internet-governance.html

activists and organizations, violating their freedom of expression, access to information, and right to privacy. Thus, it is vital to understand how CSOs in the selected Arab countries (Iraq, Egypt, Jordan, Tunisia, Bahrain, and Saudi Arabia) have engaged in their creation, modification, or opposition.

This case study aims to examine how CSOs have engaged in the development of cybercrime laws in the Arab region, following a qualitative methodology that assesses the level of engagement by CSOs in the drafting, issuance, and amendment of cybercrime laws in selected Arab countries, based on research interviews conducted with digital rights activists and organizations. The theoretical framework presents an overview of the cybercrime laws in the region, while the study's findings discuss CSO's engagement during the legal processes of enacting cybercrime laws. The findings also identify some advocacy methods that CSOs employ to impact policy-making.

Cybercrime Laws in West Asia and North Africa

Clear legal frameworks that govern online spaces are essential in protecting individuals' privacy and security.[8] Governments in WANA have sought to regulate new media through cybercrime laws that define crimes and penalties, alongside other laws, policies, and agreements governing online activity.[9]

The rise of the internet in West Asia and North Africa has created unprecedented opportunities to access information, express opinions, and participate in civic life.[10] Between 2010 and 2012, social media platforms played a critical role in facilitating communication among participants of political uprisings known as the "Arab Spring," despite ongoing criticisms about social media's role and influence in this key historical moment.[11]

On the contrary, the rise of information technology has also brought about concerns over illegal online practices such as money laundering, drug distribution, copyright infringement, software piracy, and gambling,[12] in addition to publishing harmful content, such as defamation, incitement to violence, hate

[8] Axiom Law, "Cyber Law: What You Need to Know", https://www.axiomlaw.com/guides/cyber-law#:~:text=It%20helps%20protect%20individuals%2C%20organizations,and%20safety%20on%20the%20internet

[9] UN Women, "Mapping of laws and services for online and ICT-facilitated violence against women and girls in Arab States", March, 2022, https://arabstates.unwomen.org/sites/default/files/2022-03/Mapping_report_laws_and_services.pdf

[10] Digital divide and open government in the Arab region, "Digital divide and open government in the Arab region", 2021, https://www.unescwa.org/sites/default/files/pubs/pdf/digital-divide-open-government-arab-region-english.pdf

[11] Yurdagul Meral, "THE ROLE OF SOCIAL MEDIA IN ARAB SPRING," Electronic Journal of New Media, January 2017, https://www.researchgate.net/publication/347832383_THE_ROLE_OF_SOCIAL_MEDIA_IN_ARAB_SPRING

[12] Mariam M. H. Alansari, "On Cyber Crimes and Cyber Security," Developments in Information Security and Cybernetic Wars, January 2019, https://www.researchgate.net/publication/331914032_On_Cyber_Crimes_and_Cyber_Security

speech, child sexual abuse and pornography, terrorism, and other forms of extreme violence.[13]

The need for specialized regulations that address cybercrime laws emerged due to the lack of enough frameworks concerning the technical nature of cybercrime and online platforms.[14] Out of 22 Arab countries, 13 countries have enacted legislation to deal with cybercrime, while the rest apply existing laws to these new crimes. However, most cybercrime laws in WANA countries have been written to control online content rather than protecting users' rights.

The first Arabic-speaking country to enact a cybercrime law was the UAE, in 2006.[15] This influenced other draft laws in the WANA region in terms of charges and penalties.[16] Saudi Arabia and Sudan's draft cybercrime laws followed one year later, but the majority of cybercrime laws in other countries were enacted around the so-called *"Arab Spring"*. States developed these laws to criminalize speech and restrict online platforms through which people mobilized themselves during the uprisings.[17]

These cybercrime laws repeatedly failed to meet basic principles stipulated in local constitutions and international human rights which protect freedom of expression. Still, they were used as a legitimate tool that repressed freedom of expression, and exploited people's data to criminalize them.[18] Even the Arab Convention on Combating Technology Offences, signed by most countries in WANA countries,[19] failed to balance between freedom of expression and public interest, including national security and standards of public morals.

Table (1) shows the chronological order by which cybercrime laws were enacted in West Asia and North Africa.

---

[13] Regner Sabillon, "Cybercrime and Cybercriminals: A Comprehensive Study", International Journal of Computer Networks and Communications Security, June 2016, https://www.researchgate.net/publication/304822458_Cybercrime_and_Cybercriminals_A_Comprehensive_Study

[14] Zunaira Sattar, "Challenges of Cybercrimes to Implementation of Legal Framework", 14th International Conference on Emerging Technologies (ICET), 2018, https://ieeexplore.ieee.org/document/8603645

[15] Yahya Shqair, "Cybercrime Laws in Arab Countries: Focus on Jordan, Egypt and the UAE", Arab Reporters for Investigative Journalism (ARIJ) and the Friedrich Naumann Foundation for Freedom, May 10, 2020, https://en.arij.net/wp-content/uploads/sites/3/2019/12/Cyber-Crime-Laws-in-the-Arab-world-Policy-paper-by-ARIJ.pdf

[16] Shahd Hammouri, "Borrowing is easier than thinking: Legal transplants and the case of the Jordanian constitutional court", https://www.academia.edu/30424512/Borrowing_is_easier_than_thinking_Legal_transplants_and_the_case_of_the_Jordanian_constitutional_court

[17] Ezzeldin Tahoun, "Cyber Crime in the Middle East: Analysis", May 2015, https://www.researchgate.net/publication/317648264_Cyber_Crime_in_the_Middle_East_Analysis

[18] Alyona Tsyplakova, "Theoretical And Legislative Characterization of Cybercrime In Arab Countries", International Scientific and Practical Forum, April 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4968861

[19] League of Arab States, "Arab Convention on Combating Information Technology Offences", 2021, https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

No.	Country	Year of issuance	Official name	English translation	Link
1	UAE	2006[20]	مرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات	Federal Decree-Law No. (5) of 2012 on Combating Cybercrimes	Link
2	Saudi Arabia	2007	نظام مكافحة الجريمة الالكترونية م/١٧، ١٤٢٨/٣/٨ ه	Anti-Cyber Crime Law, Royal Decree No. M/17, 26 March 2007	Link
3	Sudan	2007[21]	قانون مكافحة جرائم المعلوماتية	Law to Combat Information Crimes 2007	Link
4	Algeria	2009	القانون رقم 09 - 04 المؤرخ في 05 أوت سنة 2009	Law No. 09-04 of 14 Chaabane 1430	Link
5	Jordan	2010[22]	قانون الجرائم الإلكترونية رقم 17 لسنة 2023	Cybercrime Law, Law No. 17 of 2023	Link
6	Oman	2011	مرسوم سلطاني رقم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات	Royal Decree No 12/2011 issuing the Cyber Crime Law	Link
7	Syria	2012[23]	قانون الجرائم المعلوماتية رقم 20 للعام 2022	Cybercrime Law No. 20 of 2022	Link
8	Bahrain	2014	قانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات	Law No. (60) of 2014 on Information Technology Crimes	Link
9	Qatar	2014	قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجريمة الإلكترونية	Law No. (14) of 2014 Promulgating the Cybercrime Prevention Law	Link
10	Kuwait	2015	قانون رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات	Law No. (63) for the year 2015 on Combating Information Technology Crimes	Link
11	Mauritania	2016	القانون رقم 007-2016 بشأن الجرائم الإلكترونية	Law No. 2016-007 on Cybercrime	Link
12	Egypt	2018	قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018	Law No. 175 of 2018 on Combating Information Technology Crimes	Link
13	Palestine	2018	قانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية	Law No. (10) of 2018 on Cybercrimes	Link

[20] Amended three times in 2012, 2016, 2018
[21] Amended in 2018
[22] Amended three times in 2015, 2019, 2023
[23] Amended once in 2022

According to a policy paper conducted by the Arab Reporters for Investigative Journalism (ARIJ) and the Friedrich Naumann Foundation for Freedom (FnF),[24] cybercrime laws in many WANA countries agree on criminalizing the following points:

- Illegal access to any information system or network to change data or information
- Disabling any website or electronic service
- Violation of the privacy and protection of correspondence and communications of individuals
- Dissemination of child pornography
- Forging of an electronic signature
- Seizure of money (or credit card data) using fraudulent methods
- Human trafficking
- Drug trafficking
- Money laundering
- Gambling
- Terrorism and the promotion or financing of terrorist ideologies
- Dissemination of information on how to manufacture incendiary or explosive devices
- Obtaining confidential government information

Most of the laws have used general terms with no clear definition of what constitutes *indecent* material; it can, therefore, be used to criminalize many types of content published on the internet.[25] In a number of countries, such legislation on cybercrime includes provisions on criminalising the "dissemination of false information," "offensive messages," "spreading of rumours," "character assassination via social media," "solicitation to commit lechery," "condoning sins," and other conducts leveraging cybercrime laws to suppress digital rights.

For example, according to Human Rights Watch, **Tunisian** authorities have sentenced at least 20 journalists, lawyers, students, and other critics for their public statements online or in the media under a 2022 cybercrime decree.[26] In these cases, authorities relied on Article 24 that provides for imprisonment of five years and a fine of TND50,000 (about USD16,000) for whoever publishes content with the aim of violating the rights of others, harming public security or national defence, spreading terror among the population, or inciting hate speech.[27]

This also highlights the heavy fines and punishments that such provisions stipulate for non-criminal charges, resulting in self-censorship and selective

[24] Yahya Shqair, "Cybercrime Laws in Arab Countries: Focus on Jordan, Egypt and the UAE," Arab Reporters for Investigative Journalism (ARIJ) and the Friedrich Naumann Foundation for Freedom, May 10, 2020, https://en.arij.net/wp-content/uploads/sites/3/2019/12/Cyber-Crime-Laws-in-the-Arab-world-Policy-paper-by-ARIJ.pdf

[25] Joyce Hakmeh, "Cybercrime Legislation in the GCC Countries: Fit for Purpose?", International Security Department, July 2018, https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh-final.pdf

[26] Human Rights Watch, "Tunisia: Cybercrime Decree Used Against Critics", December 19, 2023, https://www.hrw.org/news/2023/12/19/tunisia-cybercrime-decree-used-against-critics

[27] ARTICLE 19, "Tunisia: Decree-law No 54 of 2022", January 2023, https://www.article19.org/wp-content/uploads/2023/03/Analysis-of-decree-law-54-English.pdf

justice.[28] For example, in 2022, **Saudi Arabia** sentenced a woman, Salma al-Shehab, to 34 years in prison over her Twitter activity,[29] after Saudi Arabia's special terrorist court convicted her of "causing public unrest and destabilising civil and national security" under the terrorism act.[30] Cybercrime laws allow for legal referrals to other regulations when charges are stated in more than one law, which also leaves room for relative judicial interpretation and the interference of political bodies.[31]

Cybercrime laws have also allowed public prosecutors or courts to "remove, block, stop, disable, register or intercept the data path, or prevent access to it, or temporarily ban the user or publisher" of websites, social media platforms, or people in charge of public online accounts.[32] **Egypt** practices broad censorship of the internet and enables executive authorities to block websites since 2017, even before their cybercrime law was issued. However, the number of blocked sites in Egypt had reached at least 500 by June 2018. Article 7 of the law gives the investigative authority the power to order a website blocked whenever it deems the content to constitute a crime or a threat to security, or a danger to national security or the economy.[33]

Such jurisdictions also enable authorities to arbitrarily ban social media platforms as a whole, in spite of its impact on users, including influencers, small business owners, and journalists, who use platforms for a living. Article 37 (a) of **Jordan's** 2023 Cybercrime Law requires any social media platform outside Jordan, with more than 100,000 subscribers in Jordan, to establish an office inside Jordan, to deal with any requests and notices issued by the competent Jordanian judicial and official authorities. Otherwise, platforms will incur a ban or a reduction in the bandwidth of internet traffic.[34]

Despite the local contexts of each country in terms of political circumstances and economic conditions, cybercrime laws in West Asia and North Africa have many restrictions and violations in common. Governments viewed the century's revolution in information and communication technologies (ICT) as a challenge to their authority that could threaten their reigns and potentially lead to political

[28] Selective justice refers to a system in which when a crime is committed in a country or region, the judicial authorities will make different treatment according to its specific. circumstances.
[29] Amnesty International, "Saudi Arabia: Further information: Release woman sentenced to 27 years for tweets: Salma al- Shehab", April 3, 2023, https://www.amnesty.org/en/documents/mde23/6643/2023/en/
[30] A Saudi court reduced the prison sentence of Saudi prisoner of conscience Salma al-Shehab from 27 years to four years, with an additional four years suspended.
[31] The Higher Population Council and Share-Net Jordan, "Legal Analysis of the Cybercrime Law of 2023 and the Penal Code of 1960 and its Amendments", 2024, https://www.hpc.org.jo/sites/default/files/mlkhs_syst_stshr_qnwny_m_glf_3_11_2024.pdf
[32] The National Centre for Human Rights, "Outputs and Recommendations Related to the Cybercrime Law No. (17) of 2023", 2024, https://www.nchr.org.jo/media/31ap0ass/%D9%85%D9%84%D8%AE%D8%B5-%D8%AA%D9%86%D9%81%D9%8A%D8%B0%D9%8A-
[33] Access Now, "Egyptian Parliament approves Cybercrime Law legalizing blocking of websites and full surveillance of Egyptians", January 2023, https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites-and-full-surveillance-of-egyptians/
[34] JOSA, "Full Text in English of the Cybercrime Law of 2023", August 2023, https://www.josa.ngo/publications/33

transformation. Civil society actors have had varying experiences trying to engage with how these laws are created, modified, and opposed, given the different legislative processes and factors influencing them in each country.

Methodology

- This case study employs a qualitative research methodology to assess the level of engagement by CSOs in the drafting, issuance, and amendment of cybercrime laws in selected Arab countries: Iraq, Egypt, Jordan, Tunisia, Bahrain, and Saudi Arabia. The research draws on three primary data sources: **Desk Research**, which analyzes existing cybercrime laws, policy documents, and reports on CSO engagement in legal processes in the WANA region;

- **Key Informant Interviews**, involving semi-structured interviews with CSO leaders, legal experts, policymakers, and representatives from the targeted WANA countries.The study samples at least one representative country from each sub-region within WANA – the Gulf, the Levant, Egypt, and the Maghreb – interviewing CSO representatives directly involved in cybercrime law processes, policymakers, and stakeholders in relevant internet governance frameworks. These interviewees are: Haidar Hamzouz from the Iraqi INSM organization, Mohamad Altaher from the Egyptian digital rights organization Masaar, Yara Alrafie from the Jordan Open Source Association (JOSA), Tunisian human rights activist Yousra Al-Khadrawi, Ali Abdulemam from Red Line 4 Gulf, and an expert from GCHR (Gulf Centre for Human Rights), who preferred to stay anonymous.

- **Case Study Guide**, the CADE Regional Case Study Guide, which provides a framework for data collection and analysis to ensure consistency across the countries in the sample.

The study adopts social change theory to categorize different advocacy types, methods, and tools used by CSOs, positing that social change often follows a patterned, rather than an arbitrary, course. Data collection methods include secondary data analysis (e.g., government documents, law amendments, and CSO publications) and an interview guide focused on engagement strategies and challenges.

Findings and Discussion

Assessing CSOs engagement in the legal process of issuing cybercrime laws

The legislative authority carries out specific constitutional duties, such as creating laws, approving the budget, overseeing the executive branch, and holding it accountable through questioning and investigation. Additionally, it reflects the

views of the citizens, addressing different issues and aspects of life.[35] In West Asia and North Africa, the process of lawmaking involves many technical and procedural details, yet it is typically linked to **parliamentary bodies**. One of the core functions of the parliament or the national assembly, which usually consists of chambers or houses, is to issue and/or pass laws; thus, the ability to modify or influence laws often depends on the effectiveness of this body and its engagement with societies.[36]

In **Jordan**, for example, a draft law is submitted by the government to the House of Representatives, or vice versa. Draft laws always end up in the hands of the House of Representatives, where they are included in the agenda for discussion and deliberation, and are open to suggestions from relevant committees. The House of Representatives, and the Senate engage in a voting process according to specific guidelines. Later, any draft law approved by both of them will be submitted to the king for ratification and publication in the official gazette, unless stated otherwise.[37]

Following this procedure, several versions of the Cybercrime Law in **Jordan** have been approved, and in practice, these steps generally apply to several other countries in WANA, such as Lebanon, Iraq, and Tunisia.[38] A digital rights expert at the Gulf Centre for Human Rights (GCHR) also added that: "Oftentimes, an executive institution would be created prior or shortly after these laws are enforced, such as the specialized police cybercrime units. In some cases, there would be special courts created for cybercrime cases."

Nevertheless, some countries have restricted the legislative powers of their parliaments. Ali Abdulemam from Red Line 4 Gulf, a digital rights organization, states that the **Bahraini** parliament does not have the right to propose or draft laws, as its role is limited to approving the legislation that comes from the royal court or reviewing it to provide comments according to internal regulations. This applies to the Bahraini Cybercrime Law, which was enacted in 2014[39].

These limited powers of the House of Representatives give monopoly powers for the legislative process by governmental or presidential entities, such as ministries or the royal court, which also reduces the level of democratic participation in lawmaking. Legislative powers are not only concentrated in specific bodies, but also in certain figures.

---

[35] New Horizons in Public Policy series, "Public Policy in the Arab World: Responding to Uprisings, Pandemic, and War", 2024, https://www.e-elgar.com/shop/gbp/public-policy-in-the-arab-world-9781035312689.html

[36] United Nations Economic and Social Commission for Western Asia, "ENHANCING CIVIL SOCIETY PARTICIPATION IN PUBLIC POLICY", https://www.unescwa.org/sites/default/files/pubs/pdf/sdd-10-tp1.pdf

[37] Jordanian House of Representatives, "Stages of the legislative process", https://representatives.jo/Ar/Pages/%D9%85%D8%B1%D8%A7%D8%AD%D9%84_%D8%B9%D9%85%D9%84%D9%8A%D8%A9_%

[38] Hania Sobhy, "Civil Society and Public Policy Formation: Strategies from Morocco and Egypt", Arab Reform Initiative, July 2017, https://s3.eu-central-1.amazonaws.com/storage.arab-reform.net/ari/2017/07/10173603/arab_reform_initiative_201707-Civil_Society_and_Public_Policy_Formation_English.pdf

[39] Wafa Ben-Hassine and Dima Samaro, "Restricting cybersecurity, violating human rights: cybercrime laws in MENA region," OpenGlobalRights, January 10, 2019, https://www.openglobalrights.org/restricting-cybersecurity-violating-human-rights/

The legislative process in **Tunisia** is carried out by the president himself. President Kais Saied is able to propose, enact, and ratify laws without consulting the relevant authorities or involving the people in their decisions, thus bypassing the activation of a democratic legislative process.[40]

According to Tunisian human rights activist Yousra Al-Khadrawi, the legislative process in Tunisia used to be carried out in a participatory manner after the 2011 uprising. Various sectors of civil society, unions, and parties directly affected by the law would meet with parliamentarians in hearing sessions to discuss laws and take into account the proposals submitted, whether the legislative initiative came from the government or from the parliament itself.

For example, in 2016, AlBawsala, a Tunisian human rights organization, along with other digital rights organizations like Access Now, participated in the biometric identity bill through public hearings.[41] However, this democratic process disappeared in 2021, after the Tunisian president dissolved the parliament. Tunisia shifted to a more unilateral and non-transparent approach to passing laws without involving any parties and excluding civil society.[42] This resulted in the enactment of the 2021 draft Cybercrime Law through the People's Assembly without consultations or the inclusion of civil society.

The absence of democratic bodies allows for the passage of repressive legislation, but their presence would not necessarily guarantee improvements in draft versions, especially when parliaments align with oppressive regimes and serve their interests. Mohamed Al-Taher from Masaar, a group of lawyers and technologists in **Egypt**, said that popular and civil participation in lawmaking is almost non-existent, as laws come from the state and are passed directly through the House of Representatives without any societal dialogue.[43]

“The process of enacting laws in Egypt is very procedural, and this was evident when the House of Representatives approved the draft Cybercrime Law in a meeting without any objections,” he said.

Additionally, Abdulemam stated that the Bahraini parliament cannot be seen as a legitimate representative of the people or a body with full powers, legislative capacity, or independence capable of challenging the state, although in theory, its members are elected.[44] This means that the passage of a law through the local

[40] Reuters, "Tunisian crisis escalates as president dissolves parliament", Arab Reform Initiative, March 2022,
https://www.theguardian.com/world/2022/mar/31/tunisian-crisis-escalates-as-president-dissolves-parliament
[41] Access Now, "Eight years in the making: Tunisia’s controversial Biometric ID and Passport Bills risk rights", March 2024,
https://www.accessnow.org/press-release/tunisia-biometric-id-passport-bills-passed/
[42] Eric Gobe, "Kais Saied’s Tunisia: A “New Republic”
with Old Authoritarian Tactics", Geographical Overview,
https://www.iemed.org/wp-content/uploads/2024/04/Saieds-Tunisia-Authoritarian-Tactics-Gobe-IEMedYearbook2024.pdf
[43] Mohamed S. E. Abdel Wahab, "An Overview of the Egyptian Legal System and Legal Research",
New York University School of Law,
https://www.nyulawglobal.org/globalex/egypt1.html#:~:text=The%20Egyptian%20legal%20system%20is,of%20Egyptian%20jurists%20in%20France.
[44] Ali Sawi, "State of Parliament in the Arab States", Cairo University, December 3, 2018,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3294968

legal process shaped and drafted by the state does not guarantee that the law is legitimate, especially since these official channels are unjust. In such cases, governments or the ruling family do not need to bypass the official legal process to pass laws because the existing paths are sufficient for their purposes.

There were some members of the Jordanian parliament who opposed the 2023 version of the Cybercrime Law and voted against it.[45] However, the limited time between the draft proposal and its enactment prevented civil society from effectively being able to communicate with members of the parliament and coordinate efforts to object to the law. Yara Alrafie from the digital rights organization Jordan Open Source Association (JOSA), said that the final version of the law was issued by royal decree, which carries a sense of urgency or priority. While legal, it deprived civil society of the opportunity to participate, be included in consultations, or apply pressure on the government.

On other occasions, public pressure, political lobbying, and civic engagement have prevented the passing of Jordan's draft cybercrime law in 2018, despite an arguably more repressive version having passed later in 2023.[46] In the case of Iraq, Hayder Hamzoz, founder and CEO of the Iraqi Network for Social Media (INSM), a digital rights activist network, stated that CSOs in Iraq try to take advantage of political disagreements between ministries over the law's implementation to prevent the approval of the currently proposed version in the House of Representatives, in order to gain more time to propose amendments to improve draft laws.

In conclusion, all experts and activists who were interviewed stated that the space available for civil society in the Arab region to influence the legislative process, including the cybercrime law, is limited to narrow margins surrounded by many challenges. Authorities resort to exploiting security, political, health, and economic conditions to impose martial law and exceptional circumstances that allow for the passage of repressive laws.

Methods and tools used by CSOs

Advocacy is defined as "the pursuit of influencing outcome – including policy and resource allocation decisions within political, economic, and social systems and institutions – that directly affect people's lives."[47] Advocacy is taking an increasingly important place in the role of CSOs, which monitor government

[45] Aljazeera, "Rights groups, opposition slam proposed cyber crime law in Jordan", July 2023, https://www.aljazeera.com/news/2023/7/28/rights-groups-opposition-slam-proposed-cyber-crime-law-in-jordan

[46] 7iber, "Cybercrime Law: Protecting Public Figures and Suppressing Cyberspace", July 2023, https://www.7iber.com/politics-economics/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%84%D8%B3%D9%86%D8%A9-2023/

[47] Ger Roebeling and Jan de Vries, "Advocacy and Policy Influencing for Social Change", Technical Assistance for Civil Society organizations – TACSO, July 2011,https://resource.actionsee.org/app/uploads/2018/05/doc_manual_5.pdf

policies, actions and hold the government accountable.[48] They are commonly described as the fourth power within a state, reflecting a belief in the significant influence in driving legislative change.

In the case of the internet governance legal framework, including cybercrime laws, CSOs in the Arab region have implemented different methods and approaches to impact the process of issuing laws. This part of the paper maps the different types of advocacy which CSOs have used or tried to use to impact the enactment of laws. According to interviews, CSOs have implemented activities and tools that fall under these approaches of advocacy: lobbying, raising awareness, legal advocacy, coalition-building, direct action advocacy, international advocacy and digital or online advocacy.

These advocacy approaches will be explained accordingly, drawing on concrete examples and insights of organizations and activists.

Lobbying

It is common to use the terms *lobbying* and *advocacy* interchangeably, but there is an important difference between them. Lobbying indicates a position on specific legislative change.[49] All lobbying is advocacy, but not all advocacy is lobbying. Advocacy generally refers to *arguing* in favor of (or against) a cause or idea. A few examples of lobbying could be drawn from the experience of CSOs in the Arab region, challenging cybercrime laws in their countries.

These examples are defined as direct lobbying, which attempts to influence new or existing legislation via communication with a member of the legislative body or other government representative who has a say in the legislation.[50] However, grassroots lobbying is rarely implemented, as it requires mobilizing the public around a legislative issue in the long term while utilizing different resources and tools.

AlKhadrawi states that hearings and consultations at the Tunisian Parliament were one of the lobbying techniques that Tunisian CSOs have relied on to have a significant impact in improving draft laws. However, these public consultations stopped after 2021, when the draft law was approved amid exceptional circumstances. However, interventions in public hearings conducted by the parliament are not advocacy campaigns by themselves, but they could be if they were part of a broader action plan that clarifies objectives and steps.

---

[48] Rana Abdel Aziz Al-Khamash, "The Role of Civil Society organizations in Policy Reforms in the Education Sector in Jordan", Centre for Lebanese Studies, 2024, https://lebanesestudies.com/wp-content/uploads/2024/09/Jordan_eng.pdf

[49] Lobbyit, "Advocacy vs. Lobbying: Understanding the Difference", https://lobbyit.com/advocacy-vs-lobbying-understanding-difference/

[50] Bloomberg Government, "Grassroots Lobbying vs. Direct Lobbying — What's the Difference?", Public Affairs Strategies, May 13, 2024, https://about.bgov.com/insights/public-affairs-strategies/grassroots-lobbying-vs-direct-lobbying-whats-the-difference/#:~:text=Grassroots%20lobbying%20relies%20on%20the,Collecting%20signatures%20on%20a%20petition

In the case of Iraq, CSOs have held several hearings with the Iraqi parliament to provide feedback on the draft cybercrime law of 2011. Haidar Hamzouz, a member of the Iraqi INSM organization said that their efforts have delayed the law's passage so far, allowing for more time to amend it. The organizations participated in these hearings, alongside committee members representing various ministries, to discuss its provisions and explain the legal challenges. "Some official bodies lacked a proper understanding of the technical terms in the draft law, which digital rights organizations were trying to clarify and explain," according to Hamzouz.

Jordanian CSOs also had a similar experience regarding the lack of understanding technical terms, despite that organizations were sharing contributions and comments with political parties and PMs without being invited to attend sessions or initiate meetings with stakeholders. Alrafie says that some of the Jordanian MPs did not understand the meaning of many technical terms like "ISPs," "VPN" or "IP address." JOSA has published a policy paper mapping technical bugs related to the scope and definitions of the law, and the paper was publicly published and shared with the Parliament.[51]

When asked, only two out of seven interviewees stated that their organizations have been engaged in different forms of public consultations as a lobbying technique to impact cybercrime laws. In addition, both interviewees mentioned that this method was the most effective way to engage with policymakers and track their positions on the law, as they interact with people, explain their opinions, and win more people to their side.

Raising awareness

Awareness-raising is a form of advocacy, and can be directed at a variety of audiences, including policymakers, government officials, and the general public. Awareness-raising is "a process that seeks to inform and educate people about a topic or issue with the intention of influencing their attitudes, behaviours and beliefs towards the achievement of a defined purpose or goal."[52] According to interviews, all CSOs across West Asia and North Africa implemented awareness-raising activities in their pursuit to advocate against repressive cybercrime laws, as these activities helped them know the reality of the situation before changing it, and conduct a rapid assessment of the situation.

CSOs' awareness-raising activities mainly took place online, including publishing research papers, coordinating with media outlets, carrying out online campaigns and implementing influencer marketing, as concluded from the interviews. Only two organizations have conducted offline security sessions as a form of activity to raise awareness around the law and offer relevant security tips. These workshops and training sessions have mostly targeted journalists, human rights defenders, and politicians, who are the most prone to being arrested.

---

[51] Jordan Open Source Association (JOSA), "The new Cybercrime Draft Law has many technical issues," July 2023, https://x.com/jo_osa/status/1683214148648222721

[52] SDG ACCOUNTABILITY and TAP Network, "Raising Awareness through Public Outreach Campaigns", https://sdgaccountability.org/wp-content/uploads/2019/05/Raising-Awareness.pdf

The anonymous expert from GCHR also mentioned that their organization has advocated against vague and broad provisions of the law, by conducting research reports analysing cybercrime laws in the Gulf region. These reports are essential for raising awareness and conducting research-based advocacy. According to the expert, findings from these reports have been used in various advocacy efforts, including to the the United Nations Human Rights Council (UNHRC) and the European Union (EU), and to issue appeals or joint statements to repeal the criminalization of digital rights.

CSOs in Egypt had also engaged similarly with the cybercrime law, Masaar's Mohamad Altaher said that most Egyptian CSOs have something to criticize the law with, but the closed political situation has made talking about it the maximum effort they can make. Altaher's organization has published different articles, statements and social media posts highlighting the concerns on some problematic clauses in the law in an attempt to provide a policy analysis source for researchers and journalists who are interested in reporting on the issue[53].

Similar online campaigns have also been launched in Jordan. Alrafie says that their organization also reached out to social media influencers and digital creators to advocate for their cause and raise awareness on the issue, as influencers are one of the top social segments who are negatively impacted by Egypt's Cybercrime Law's restrictions on platforms where they publish their content and generate profit. The hashtag #اسحبوا_قانون_الجرائم_الإلكترونية (#Withdraw_the_Cybercrime_Law) topped the list of trending hashtags on social media in Jordan in July 2023.

Online campaigns can mobilize the power of public opinion in support of an issue and thereby influence the political will of decision-makers. However, awareness-raising can mean different things in different circumstances, indicating a wide variety of experiences, and it's difficult to assess the impact of these activities, especially when they're not attached to measurable goals. Although the use of digital advocacy has been promoted for successful campaigns, most interviewees stated that awareness-raising activities by themselves did not lead to concrete action on the ground, as many research papers on advocacy have concluded.[54]

Coalition-building

Coalition-building is "the process by which parties (individuals, organizations, or nations) come together to form an alliance or partnering of groups in order to achieve a common purpose or to engage in joint activity."[55] By working together, coalition members can increase and expand their influence, and make a stronger case for policy change among different audiences. Research on advocacy has concluded that coalition-building creates more effective strategies and can

[53] SMEX, "Egyptian Parliament Passes Cybercrimes Law to Legitimize its Efforts to Curb Free Speech," June 18, 2018, https://smex.org/egypt-passes-cybercrimes-law-to-legitimize-its-efforts-to-curb-free-speech/
[54] Ann Christiano & Annie Neimand, "Stop Raising Awareness Already," Stanford Social Innovation Review, 2017, https://ssir.org/articles/entry/stop_raising_awareness_already#
[55] Business Advocacy Network, "Building coalitions & alliances", Irwin Grayson Associates, 2020, https://www.businessadvocacy.net/dloads/fs/fsBuildingCoalitions.pdf

empower marginalized groups. The diversity within coalitions broadens their reach, allowing for tailored messaging to different policymakers.[56] Additionally, coalitions raise visibility, garner media attention, and build political clout, increasing the chances of success in securing policy change.

In addition to raising awareness, coalition-building is the top advocacy method used by CSOs in the WANA region to advocate for better cybercrime laws. In each country, organizations have utilized efforts to share a unified position on the law, increased visibility and collective action, and built a solidarity network. AlKhadrawi says that more than five Tunisian organizations and unions[57] have called on authorities to withdraw the cybercrime decree "as it contradicts the goals of the [2011] revolution … and contains threats against anyone who initiates an opinion contrary to the authority," according to the statement.[58]

Later statements from CSOs condemned the law and urged the president to withdraw it with immediate effect. For instance, one statement stated: "the undersigned human rights associations and organizations have expressed their deep alarm regarding specific provisions of the law and their flagrant contravention of the Tunisian Constitution and the International Covenant on Civil and Political Rights, which Tunisia has ratified."[59] Similar statements were signed by different segments of the civil society, including grassroots movements, local organizations, regional and international NGOs, and activists.

Haidar Hamzouz from INSM also said that joint statements and online petitions help to direct the focus of all stakeholders on the unresolved issues and make better use of the expert's time and evidence. He also added that coalition-building activities could take different forms, such as joining digital rights conferences concerning the situation in the Arab region. According to him, these events enable communication and networking between organizations, and constitute a free space where they reflect on their techniques and approaches to hold government and big tech companies accountable.

According to author Sam Grant, while coalition building can be powerful, it also presents several challenges. Differences in priorities, values, and strategies among diverse members can lead to conflicts and slow decision-making. Aligning goals can be difficult, especially when coalition members represent varying sectors with different agendas. Managing power dynamics is another hurdle, as larger or more influential groups may dominate discussions, potentially sidelining smaller or marginalised members. Additionally, coordinating efforts and maintaining clear

---

[56] Catherine Brown, "Coalition-Building: Why it Matters and How to Start", National College Attainment Network, March 27, 2023, https://www.ncan.org/news/635812/Coalition-Building-Why-it-Matters-and-How-to-Start.htm#:~:text=Strength%20in%20numbers%3A%20A%20coalition,policy%20change%20among%20different%20audiences.

[57] The UGTT labour union, the Tunisian Order of Lawyers, the Tunisian Federation of Journal Directors, the National Syndicate of Tunisian Journalists, and the Tunisian League for Human Rights issued a joint statement against the legal proclamation.

[58] The New Arab, "Tunisian groups call for withdrawal of 'threatening' cybercrime decree", December 2022, https://www.newarab.com/news/tunisian-groups-call-withdrawal-cybercrime-decree

[59] Access Now, "Tunisia: President must scrap decree-law undermining free expression and the press", January 2023, https://www.accessnow.org/press-release/decree-law-54-tunisia/

communication across multiple organizations can be complex and time-consuming.[60]

Direct action advocacy

Direct action is defined as "a form of action where people use their power to directly achieve political goals."[61] Unlike indirect methods like voting or lobbying politicians, people taking direct action aim to meet their goals through their own activity, rather than the actions of others. Direct action may include activities (often nonviolent), targeting people, groups, institutions, actions, or property whose participants deem objectionable. Nonviolent direct action may include civil disobedience, sit-ins, strikes, and counter-economics.

Some WANA capitals have witnessed protests and demonstrations that demanded the withdrawal of laws restricting digital rights, citing concerns over its potential repercussions on society.[62] In Amman, hundreds of citizens took to the streets and chanted slogans denouncing restrictions on freedom of expression in front of the national assembly and downtown, according to Alrafie. More protests followed when the law was used against online activities demonstrating pro-Palestine views after October 2023, and to punish individuals with harsh sentences of up to five years.[63]

Alrafie said the CSOs have actively participated in coordination with political parties – mostly informally. However, organizations had limited powers in calling for these protests due to security concerns. Similarly, AlKhadrawi added that Tunisian authorities have suppressed several demonstrations calling for the abolition or amendment of the law, some of which have seen activists arrested, which has fostered self-censorship and limited the ability of organizations to participate in direct action advocacy.

Other countries have not witnessed any protests against the law due to different reasons. The political and human rights protest movement in Egypt has been very limited since 2011 due to repressive and arbitrary measures taken by its government. Altaher said that the crackdown on freedom of expression after the Arab Spring has reached unparalleled levels in Egypt's recent history, making it as dangerous as ever to organise protests or even criticise the government.

Additionally, Abdulemam stated that Bahrain's cybercrime laws were passed amid a "phase of constitutional reform" and intense security events that occupied headlines. These local conditions and disturbing decisions, such as terrorism law amendments which allows for nationality withdrawal, have shifted attention from the cybercrime law. As digital rights are often visualised as secondary,

---

[60] Sam Grant, "Barriers to Coalition Building", Tribal Oriented Policing Strategies, https://ncjtc-static.fvtc.edu/Resources/RS00002733.pdf
[61] Seeds For Change, "What is direct action?", 2022, https://www.seedsforchange.org.uk/downloads/directaction.pdf
[62] ARTICLE 19, "Jordan: Marking a year of oppression, fresh calls to scrap Cybercrime Law", September 13, 2024, https://www.article19.org/resources/jordan-fresh-calls-to-scrap-cybercrime-law/
[63] Human Rights Watch, "Jordan: Arrests, Harassment of Pro-Palestine Protesters", February 6, 2024, https://www.hrw.org/news/2024/02/06/jordan-arrests-harassment-pro-palestine-protesters

governments tend to take advantage of political conditions to pass repressive regulations.

Legal advocacy

Legal advocacy occurs when lawyers represent a client in a court or tribunal. This means they can do and say things on their client's behalf[64]. Legal advocacy includes educating and assisting victims to understand the justice system; assisting victims in evaluating the advantages and disadvantages of participating in legal processes; and facilitating victims' access and participation in legal systems.

Legal advocacy is often perceived as public policy advocacy. However, the former concerns justice systems, and the latter address the regulations themselves[65]. However, Legal advocacy activities could help resist violations in the legal framework. When Arab CSOs realised their limited impact on the cybercrime drafts and legal amendment process, some of them shifted their resources to represent victims of the law to minimize charges and secure fair trials and a strong defence.

Legal assistance or aid organizations are a whole sub-group of civil society entities that exist to support accused activists and journalists, document human rights violations, and produce statistics on arrests and cases. Altaher says that this approach could be effective when you can trust the independence of judiciary procedures. But when the system is vague and relative, the effectiveness of legal efforts are minimised.

In one example, Ali Abdelemam stated that legal representations helped some activists win their cases, including ones filed outside the country. One notable example is when the High Court in London convicted the ruling Al Khalifa regime in Bahrain in a case of spying on dissidents in 2023. In this case, the exiled Bahraini activist Yousef Al-Jamri pursued legal action against Bahrain's government after discovering that his phone was being spied on using the Israeli Pegasus spyware in 2019.

Security assistance services function in parallel with legal aid programmes, as activists face risks of surveillance, harassment, or physical threats. Regular security checks, such as encrypting communications, securing social media accounts, and using VPNs protect valuable data, communications, or contacts that could be exploited by authorities or malicious actors if not properly secured. When arrested, security measures can help protect sensitive digital information and prevent further risks to personal safety and privacy.

---

[64] Solicitors Regulation Authority, "What is legal advocacy?", October 2022, https://www.sra.org.uk/consumers/instructing/legal-advocacy/legal-advocacy/#:~:text=Legal%20advocacy%20is%20when%20lawyers,to%20a%20court%20or%20tribunal

[65] Sask Culture, "Advocacy & Changing Public Policy", April 21, 2024, https://www.saskculture.ca/programs/organizational-support/organizational-resources/advocacy-changing-public-policy

International advocacy

International advocacy targets a worldwide audience and national policymakers involved in international processes.[66] It could bring change in international agreements about a specific issue or call on international stakeholders to pressure local regulators during policy-making and shaping processes. International advocacy could intersect with networking and coalition-building advocacy, as well as legal advocacy, as international organizations take part in alliances and local or regional organizations use international legal systems to impact the drafting and enforcement of laws.

According to case study interviews, different forms of international advocacy have been widely adopted by WANA-based CSOs in the case of cybercrime law. Abdelemam says that this approach is essential for national organizations based abroad, especially when the local civil society scene lacks independent organizations and watchdogs. Arab human rights organizations and activists, based abroad, mostly in Europe, are still exposed to attacks and surveillance, but they provide an alternative perspective for lobbying as well.

The anonymous expert states that the GCHR has submitted reports to mechanisms such as the Office of the UN High Commissioner for Human Rights (OHCHR). For example, one of the GCHR's reports has supported OHCHR advocacy in Geneva, as actors can refer to these country-specific insights and evidence. This approach helped them collaborate within and beyond the region which opened new spaces for advocacy, such as investors and businesses. "While documentation can be challenging in certain contexts, it has been the most effective to demonstrate concrete consequences of cybercrimes laws and their abuse," Nardine said.

The level of Arab governments' responsiveness to international recommendations related to freedom of opinion and expression is very low, Altaher said, as he took part in two Universal Periodic Review (UPR) rounds in Egypt without witnessing any changes in the law. Despite that, international advocacy is perceived differently in Iraq. INSM's Hamzouz expressed that the engagement of international organizations in national advocacy campaigns has facilitated their communication with official stakeholders: "It counts when international organizations show up at hearing sessions and consultations besides local and regional digital and human rights organizations, as the government fears international accountability and sanctions."

Exploring successes and challenges

Arab organizations have managed to achieve a few goals in their advocacy against repressive cybercrime laws in the region using different approaches, methods, and tools. In some countries, civil society organizations were able to modify unjust laws, which is the ultimate goal of most of the campaigns. In the case of Iraq's cybercrimes law, which has not been issued yet, Hamzouz said that

[66] CHOICE for Youth and Sexuality, "UN Advocacy", 2024, https://www.choiceforyouth.org/resource/youth-led-advocacy/un-advocacy#:~:text=International%20advocacy%20targets%20a%20worldwide,agreements%20about%20a%20specific%20issue.

CSOs' recommendations and comments during regular consultations and follow-ups led to the modification of some loose terminologies in law articles and the phrasing in some others to be more accurate.

According to Hamzouz, one of the most significant successes of these efforts is that they managed to change the name of the law. The old version of Iraq's cybercrime law criminalizes the medium itself rather than the harmful actions that could occur as a result. Official committees have considered an alternative wording for the title that is more objective. Hamzouz also explained that, had their efforts continued, the law's passage and implementation could have been postponed until it aligned with the principles set out in the Iraqi constitution.

However, other existing regulatory frameworks, like the Penal Code and Publications Law, could be used to prosecute journalists and issue sentences against them. In addition, passing amendments to a law's provisions might not always be considered a success. In 2023, the Senate approved amendments to Jordan's Cybercrime Law, reducing fines for some charges and allowing the judiciary to choose among fines, imprisonment, or both penalties for crimes such as spreading false news, defamation, slander, or contempt.

Alrafie stated that the amendments did not alter the law's core, as no radical changes to its articles were considered, but the broad charges were left intact. "Even if the fine is reduced from JOD 50,000 to JOD 20,000, it is still an enormous sum. No one can afford such fines for a Facebook post in a country where the minimum wage is only JOD 290 per month (around USD 3,500 annually), she noted. She added that these cosmetic amendments allow governments to claim cooperation with civil society without enacting any real policy change.

In most WANA countries, CSO advocacy against cybercrime has little impact on the drafts. Interviewees on average evaluated the effectiveness of their engagement at 3 out of 10, despite their engagement rates reaching 7 out of 10. Nardine said "It is difficult to assess the efficacy of our effort. These regimes often have strong ties and interest in solidifying their tight grip on power. Resources at their disposal outweigh our capacity to do the remedial, advocacy, and documentary work we do."

Civil society advocacy has achieved isolated successes in cases where activists were prosecuted. According to Abdelemam, legal assistance and popular pressure have secured the release of some activists, reduced sentences, or substituted imprisonment with community service obligations. Yet the impact of these victories remains limited, varying according to national conditions and political openings. Such efforts provide case-by-case support but do not produce change at the level of the law itself.

According to Altaher, CSOs in Egypt can claim one outstanding success from their advocacy, which is "making the law notorious." In his opinion, CSOs' social media work, statements, research, reports, and petitions have created a negative image of the cybercrime law, both locally and internationally, which increased awareness of the human rights violations its implementation would commit, especially when the law applied to real-life cases involving activists and influencers.

All interviewees stated that impactful public policies required a supporting political will in the first place. In other words, if authorities are not welcoming CSO contributions and creating mechanisms where civil society can engage, changing regulations would be very difficult and advocacy efforts won't be effective. According to the interviewees, activists and organizations identified a lack of political will and hostile government responses to their demands as a top challenge. "It's not that CSOs cannot lead change, but it's how the system is designed to ignore their contribution and restrict it," said Abdelemam.

Organizations also face persistent challenges, including insufficient technical expertise, scarce resources, limited understanding of the policy-making process, weak evidence to persuade policymakers, self-censorship, and poor inter-organizational coordination. These obstacles are reflected in practice, as each advocacy method encounters specific restrictions shaped by context.

In general, interviewees considered that adapting advocacy methods and activities should be part of a detailed long-term collaborative strategy, but when activities are performed out of context as a response or a reaction to policies, or misinterpreted as goals rather than methods, organizations' efforts become random and temporary. Alrafie says that CSO campaigns, including alliances, lack sustainability, grassroots advocacy, and evaluation of the needs of local communities, needed to ensure that these are considered when setting priorities and shaping policies.

Conclusion

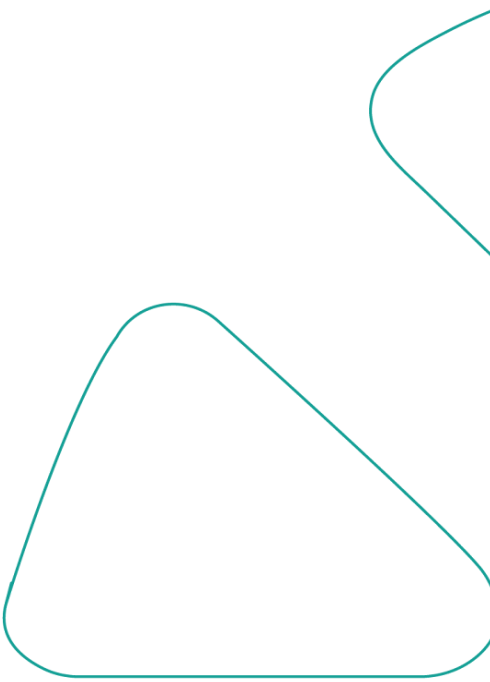
CSOs often seek to influence government policies, programmes, and strategies through consultations, discussions, and public hearings, often representing diverse stakeholders. Yet, this paper found that Arab CSO efforts to influence cybercrime legislation have a limited impact on policy. Every expert and activist interviewed stressed that the space available for civil society to influence the lawmaking in the Arab region, including on cybercrime laws, is limited to "narrow margins surrounded by many challenges." Regimes frequently exploit security, political, health, and economic crises to justify martial law or exceptional measures that enable the swift passage of restrictive legislation.

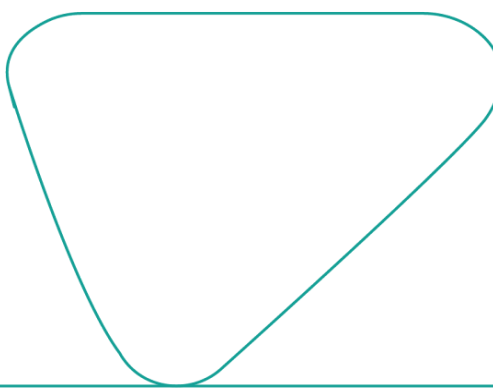
CSOs in the Arab region have employed a wide range of advocacy methods to push for improved drafts and adherence to human rights standards. These methods include lobbying, awareness-raising, legal advocacy, coalition-building, direct action, international advocacy, and digital or online campaigns. Raising awareness and coalition-building were the most commonly used approaches, while lobbying was the least implemented, even though interviewees noted it was the most effective way to influence legislation. Participants assessed the average effectiveness of their engagement at 3 out of 10, despite indicating that their engagement levels were sometimes higher.

Advocacy tools identified in the study include statements, training, workshops, petitions, research, meetings, conferences, media reports, international submissions, court trials, and more. In both their offline and online forms. These tools were either implemented as a response to policies or as part of an action plan. Interviewees insisted that adapting advocacy methods and activities should

be part of a detailed long-term collaborative strategy used to maximise achievements and lead to sustainable change.

This study also explored the different successes and challenges of CSOs in their policy-shaping efforts on cybercrime law. While various CSOs have managed to amend some articles of law, the maximum achievement of other CSOs was limited to publishing statements and raising awareness on the human rights violations of a certain law. Margins of change vary between countries depending on political, economic, and social factors, and they are also governed by multiple challenges. Organizations have identified the lack of political will and hostile responses from the government as main challenges to their attempts to influence public policy, alongside other difficulties, such as insufficient technical expertise, limited resources, self-censorship, other existing repressive laws, and poor coordination between organizations.





Recommendations

- **Authorities** should demonstrate a commitment to improving the drafting and enforcement of cybercrime laws by incorporating recommendations, reviews, and concerns from CSOs regarding the implications of such laws in the Arab region.

- **Governments** should establish or activate official channels for CSOs to engage in lawmaking processes, recognising the importance of their input. These channels could include consultations and public hearings designed to gather and consider opinions, concerns, and suggestions.

- **CSOs** should diversify their advocacy methods to effectively engage in the lawmaking process. This includes utilising direct and grassroots lobbying, which was identified as one of the most effective yet underutilised strategies. While CSOs have heavily relied on raising awareness, coalition building, and international advocacy, these approaches have had limited impact on the creation, modification, or opposition of laws, according to interviewees.

- **CSOs** should integrate advocacy methods and tools into broader action plans and strategies, rather than solely reacting to policies as they emerge. Interviewees noted that lacking a clear strategy of change limits the effectiveness of CSO activities. This approach positions activities as goals in themselves, rather than as means to achieve broader impacts, which can undermine the sustainability of their efforts.

- **CSOs** should invest in understanding the legislative processes in their countries, which will enhance their ability to engage meaningfully. Some CSOs lack the capacity to understand how the legal system operates, which has hindered their ability to effectively engage with it. A deeper understanding of the legislative process should also take into account the political and economic factors that influence it, helping CSOs identify potential opportunities and breakthroughs for advocacy.

- **International NGO engagement with national CSO campaigns**, whether as partners or donors, should prioritise contextual needs, ensuring that local communities are considered when setting priorities and shaping recommendations. In many cases, CSO opposition to repressive laws attempted to mirror donors' policies and perform activities for purposes of ticking off boxes. Limited dialogue between CSOs and international NGOs on advocacy strategies and methods leads to fragmented campaigns that lack value and relevance within local communities.

- **CSOs and international NGOs** should engage in ongoing monitoring, documentation, and analysis of cybercrime laws and their implications for human and digital rights. While civic engagement is typically highest during the drafting and issuance of laws, advocacy efforts often decline shortly afterwards, even though the threats posed by such laws persist. Continuous efforts are needed to maintain pressure on the long-term implications of these laws.