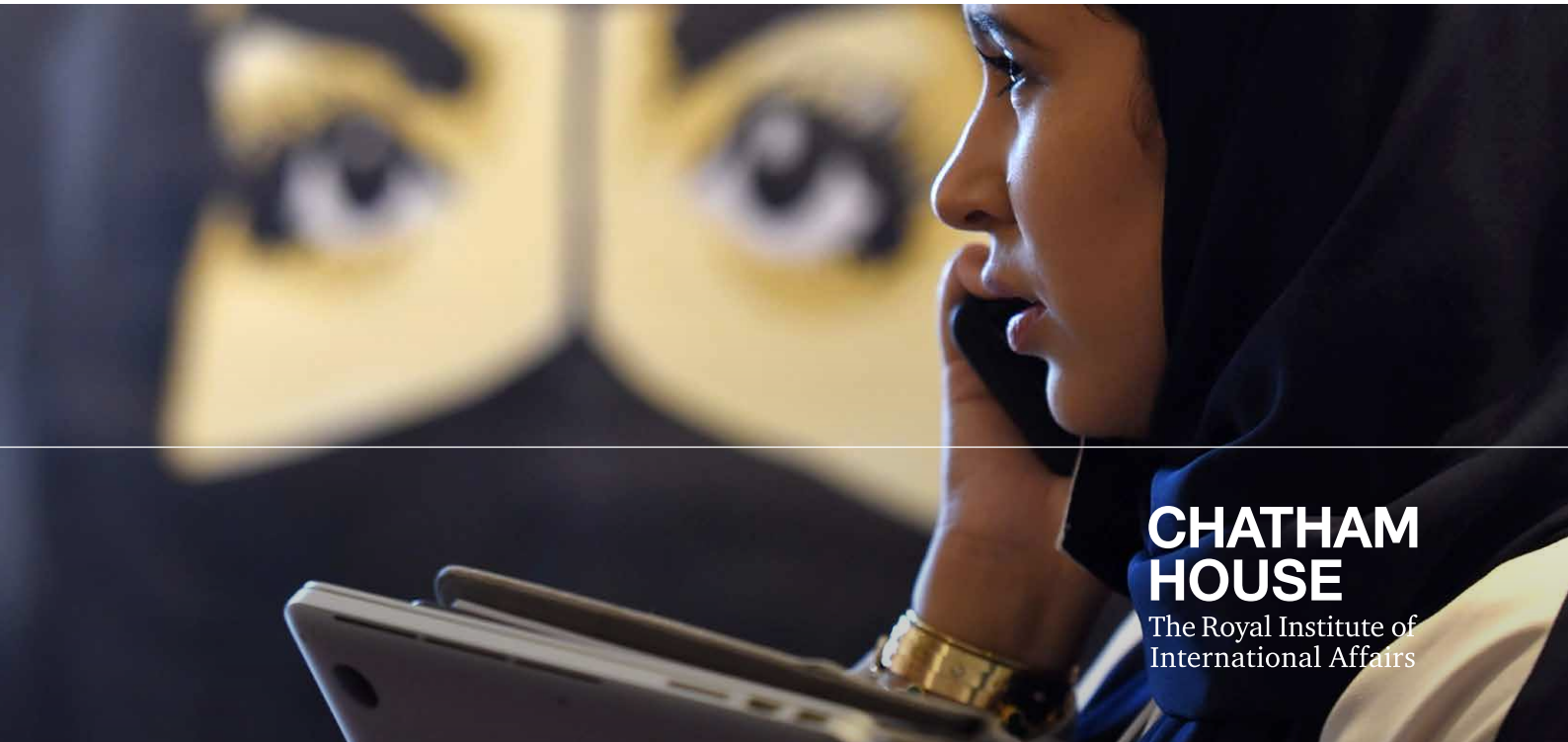
Research Paper

Joyce Hakmeh
International Security Department | July 2018

Cybercrime Legislation in the GCC Countries

Fit for Purpose?



CHATHAM HOUSE
The Royal Institute of International Affairs

Contents

Summary

- Most GCC countries have enacted or updated their cybercrime laws as part of their efforts to address the increasing threat of cybercrime. However, most of these focus on limiting freedom of expression and at the same time omit key elements needed to combat cybercrime as this would be understood under most legal frameworks.
- GCC cybercrime legal frameworks depart from international practice on cybercrime legislation in both structure and content.
- Regarding their structure, cybercrime legal frameworks in the GCC are focused on substantive criminal law that criminalizes offences considered to be cybercrimes. However, in prosecutions and investigations, most GCC countries still apply traditional texts to cybercrime cases that are mostly oblivious to the nature of these cases. This impedes the success of these efforts and therefore the overall impact of fighting cybercrime.
- Regarding their content, all GCC countries, except for Bahrain, have introduced as part of their cybercrime laws provisions that criminalize a wide-spectrum of content, using vaguely worded provisions that create the potential for confusion and abuse.
- The GCC countries have historically restricted traditional forms of speech, and have latterly sought to do the same with online speech as well. This was arguably accelerated by the events of the Arab uprisings and the 'cultural revolution' that was brought forward by social media.
- Through their cybercrime laws, the GCC countries have sought to get a stronger grip on social media, and to stymie the potential for spillover via online platforms of political unrest from other Arab countries.
- Several human rights defenders and activists, as well as other social media users, have been prosecuted under these laws, deported or jailed for online comments, for blogging or for posting pictures aimed at social, religious or political ends. Some people have been detained for publishing humorous and satirical online content.
- Given their text and scope of application, most cybercrime laws of the GCC countries could put in jeopardy the right to free speech and are at odds with international human rights law, standards and safeguards. Furthermore, their current structure, combined with a lack in other laws that address the specificities of cybercrime, makes them an inadequate tool for fighting cybercrime.
- Revision of these cybercrime laws is urgently required, and is essential for better security, for a better society and for better civil liberties.
- GCC governments would benefit extensively from joining international forums on cybercrime – such as the Budapest Convention – as this would help them in harmonizing and updating their laws, in enhancing their cybercrime investigative techniques, and in increasing international cooperation between them and with other countries.

Introduction

Over the past few years, most member countries of the Gulf Cooperation Council (GCC)[1] – Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE – have enacted or updated existing cybercrime laws as part of their efforts to address what is acknowledged as a growing security threat.[2] Although cybersecurity technology remains the primary investment in countering cybercrime, there is an increasing awareness among the region's policymakers of the important role of legislative frameworks in preventing and in combating cybercrime. However, most GCC cybercrime legal frameworks are still an incomplete step. They do not elaborate on elements – such as the procedural powers, electronic evidence, jurisdiction and international cooperation – that are essential for the law to play its proper role in guiding national investigations and prosecutions and in facilitating mutual legal assistance in transnational investigations. Instead, the focus is primarily on criminalization of acts that are considered as cybercrime, with many provisions on forbidden speech. GCC cybercrime laws expand the definition of cybercrime to a wide array of forms of expression using vaguely worded provisions that leave the door open to confusion and abuse. Furthermore, the laws impose increased penalties especially on speech criticizing or challenging the ruling establishment. In their current shape, therefore, cybercrime legal frameworks in most GCC countries have an adverse impact on freedom of expression and do not best fulfil their stated intention of combating cybercrime.

The ongoing pace of technological developments and the large opportunities for further digital growth, in conjunction with high internet adoption rates and consumer complacency, are all contributing to the growth of cyber risk in the GCC region. As the governments of the GCC countries continue to invest in and develop their digital economies and smart infrastructures, and as citizens inevitably use the internet and online services in almost every aspect of their daily lives, the potential impact of cybercrime is not just financial: there are major operational disruption and safety risks to consider. There is thus a critical need for the governments of the GCC countries to update their anti-cybercrime capacities, including by means of training their judiciary and law enforcement agencies, creating more awareness at every level, pioneering public-private partnerships and, importantly, revising their cybercrime legal frameworks.

About this paper

This paper forms part of a research project that examines cybercrime laws in the GCC. Its aim is to assess whether these laws are fit for purpose, and to gauge their impact on the economy, security and civil liberties. Previous work within the project has explored the impact of GCC cybercrime laws on the economy, in particular on the digital economy and on the future and security of the smart infrastructures.[3]

This paper examines the impact of cybercrime laws in the GCC with a focus on civil liberties, notably on freedom of expression online. By focusing on the structure and content of the laws and assessing how they compare with relevant international law, the case is made that most cybercrime laws in the GCC raise concerns when viewed through the lens of international human rights law

[1] GCC is used interchangeably in this paper to refer either to the countries belonging to the Gulf Cooperation Council – i.e. Bahrain, Kuwait, Qatar, Oman, Saudi Arabia and the UAE – or to the region as a whole.
[2] While it is difficult to measure precisely the incidence, spread and effects of cybercrime in the GCC countries, a number of trends and figures point to a rapid growth of cybercrime across the region. For a fuller discussion, see Hakmeh, J. (2017), *Cybercrime and the Digital Economy in the GCC*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/publication/cybercrime-and-digital-economy-gcc-countries.
[3] Ibid.

standards. Indeed, these laws play a major role in curtailing freedom of expression and do not offer the needed guide for law enforcement and the judiciary in their efforts to investigate, prosecute and adjudicate cybercrime.

The socio-economic, political and technological background to GCC cybercrime laws

Participation in public affairs under the authoritarian governments of the GCC countries[4] has always been limited and controlled, notwithstanding some elements of representation that vary from country to country. The legitimacy of this model has often been attributed to the social contract of the rentier state, whereby the state obtains revenues from a windfall such as oil, without requiring either taxation or significant economic development policies, and then expects loyalty by disbursing this wealth to its citizens.[5] This is partially the case given the history of the GCC countries both before and after the discovery of oil resources, and the patriarchal social system that acts as the foundation of the existing social contract. However, this model does not hold water with regard to the kind of ambitious development strategy that each of the GCC countries is now putting in place.[6] Many of the younger generation of leaders have, furthermore, been making considerable efforts to associate themselves with futuristic economic development plans that depart from being simply a mechanism for distributing resource wealth.

While national wealth has been one of the main factors underlying the lack of public participation in the GCC states, it has enabled most countries of the region to make sustainable investments and to reinvent themselves on several fronts. They have made remarkable efforts to diversify their economies through initiatives aimed at reducing their reliance on the oil and gas sector, and through investing in digital economies and in 'smart' infrastructures.[7] Moreover, GCC countries have assumed an increasingly important role in foreign aid and in economic statecraft in the Middle East and North Africa region, and have channelled considerable resources and energy towards investments in international sports, arts and culture. All the same, the main political tenets of Rentier State Theory remain relevant for the GCC countries. The 'red lines' determining the extent to which state authority may be challenged by citizens remain as clear as ever.[8]

The current socio-economic and political turmoil in the region has, nonetheless, given a new generation of Gulf leaders and citizens cause to examine the status quo, and in particular the continuing validity of the long-held social contract.[9] As oil revenues decline, and as the rapid growth of the region's youth

[4] The Economist Intelligence Unit's Democracy Index, which in 2016 ranked 167 countries worldwide on a scale of 0–10 based on 60 indicators covering pluralism, political culture and civil liberties, categorizes each of the six GCC countries as authoritarian (i.e. with a ranking on the scale 0–4, where a ranking of 8–10 indicates full democracy). The individual country rankings for 2016 (compared with their equivalent ranking in 2006) were: Bahrain 2.79 (3.53); Kuwait 3.85 (3.09); Oman 3.04 (2.77); Qatar 3.18 (2.78); Saudi Arabia 1.93 (1.92); UAE 2.75 (2.42). See Economist Intelligence Unit (2016), 'Democracy Index', https://infographics.economist.com/2017/DemocracyIndex/ (accessed 21 Mar. 2018).
[5] Rentier State Theory (RST) 'holds that, since the state receives [this] external income and distributes it to society, it is relieved of having to impose taxation, which in turn means that it does not have to offer concessions to society such as a democratic bargain or a development strategy' Gray, M. (2011), *A theory of "Late Rentierism" in the Arab States of the Gulf*, Center for International and Regional Studies (CIRS), Georgetown University, School of Foreign Service in Qatar, https://repository.library.georgetown.edu/bitstream/handle/10822/558291/CIRSOccasionalPaper7MatthewGray2011.pdf.
[6] These include Smart Dubai; Saudi Arabia's Vision 2030 and National Transformation Program 2020; Qatar's Connect 2020 ICT Policy; and Oman's Digital Strategy.
[7] The UAE levels of digital readiness surpass those of the US and Europe in the adoption of digital technologies by consumers and government. For more, see Benni, E., Elmasry, T., Patel, J. and aus dem Moore, J. P. (2016), *Digital Middle East: Transforming the region into a leading digital economy*, McKinsey & Company, October 2016, www.mckinsey.com/global-themes/middle-east-and-africa/digital-middle-east-transforming-the-region-into-a-leading-digital-economy (accessed 22 Jun. 2018).
[8] Gray (2011), *A theory of "Late Rentierism" in the Arab States of the Gulf*.
[9] Chatham House (2016), *The Social Contract in the GCC*, Middle East and North Africa Programme Workshop Summary, 11–12 January 2016, https://www.chathamhouse.org/sites/files/chathamhouse/events/110416-GCC-Social-Contract-Workshop-Summary.pdf.

population continues, the economics of the social contract and the security generated by rentier wealth is coming under increased pressure. The fiscal restraint that these circumstances will inevitably require will make it more difficult for the governments of the GCC countries to maintain the degree of largesse that generations of their citizens have come to expect. This context, together with the ambitions of the economic strategies now being implemented, is increasingly compelling the GCC governments to seek alternative sources of legitimacy and to develop new participatory strategies in order to manage public expectations of what the state might be expected to do for them,[10] or allow them to do.[11]

The rise of social media has offered a platform for a young, tech-savvy generation that is eager for its voice to be heard. The GCC has among the highest internet and mobile penetration rates in the world. Across the GCC countries (as shown in Table 1), an average of 76 per cent of the population use the internet, compared with a global average of 51 per cent. The average mobile subscription rate is 184 per 100 inhabitants (231.8 per 100 in Kuwait), and the average rate of mobile broadband subscription is 115 per 100 inhabitants.

Table 1: Internet, mobile and social media penetration in the GCC

Country	Internet users (% of population, 2015)	Mobile broadband subscriptions (per 100 inhabitants, 2015)	Mobile subscriptions (per 100 inhabitants, 2015)	Social media penetration (Facebook, per 100 inhabitants, 2017)
Bahrain	93.5	131.8	185.3	73
Kuwait	82.0	139.3	231.8	71
Oman	74.2	78.3	159.9	41
Qatar	92.9	80.0	153.6	95
Saudi Arabia	69.6	111.7	176.6	58
UAE	91.2	92.0	187.3	94
GCC average	76.0	115.0	184.0	66

Sources: ITU (for internet users, mobile broadband subscriptions, mobile subscriptions);[14] Arab Social Media Report.[15]

This remarkable online presence, standing in contrast to a traditionally limited public sphere for interaction and restricted space for political opinion, lack of civil society infrastructures and free media, has provided a new vehicle for citizens to voice their opinions and concerns. It has led to a 'cultural revolution' on several fronts.

Social media use became a new way of life for GCC citizens from the late 2000s, a source of 'unfiltered' and abundant news, and a conduit for citizens to engage and interact with one another. Many women in the GCC were able to use social media platforms as a marketplace, overcoming social taboos and

[10] Ibid.
[11] Some Gulf experts argue that rulers will opt for more social freedom rather than greater political freedom as a way to adapt to the changing circumstances, read for example, Kinnimont, J (2018), 'Why Going to the Cinema in Saudi Arabia is suddenly Okay', Chatham House Expert Comment, https://www.chathamhouse.org/expert/comment/why-going-cinema-saudi-arabia-suddenly-okay.
[12] Ibid.
[13] Ibid.
[14] ITU (2016), *Measuring the Information Society Report 2016*, Geneva: ITU, pp. 240–247, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf (accessed 11 Apr. 2018).
[15] Salem, F. (2017), *Social Media and the Internet of Things – Towards Data-Driven Policymaking in the Arab World: Potential, Limits and Concerns*, Arab Social Media Report 2017 (Vol. 7), Mohammed Bin Rashid School of Government, Dubai, www.mbrsg.ae/getattachment/1383b88a-6eb9-476a-bae4-61903688099b/Arab-Social-Media-Report-2017 (accessed 11 Apr. 2018).

traditions to run businesses from their homes, and contributing to the emergence of a new generation of female entrepreneurs.[16] Social media was also used by GCC leaders for positive PR, to engage with their millions of followers and to share aspects of their personal lives with a wide audience.[17]

Emboldened by the 'anonymity' that social media platforms provide, GCC citizens also started to interact more with their governments to express grievances and criticisms, and to call for political reform and greater participation. In this respect, social media platforms compensated for the lack of a public space and served as a proxy for physical demonstrations, which have always been difficult to convene in GCC countries, and provided a forum for debate between loyalists and opponents of the ruling monarchies.[18] For some in the GCC, social media platforms came to serve as a 'virtual' Tahrir Square.[19]

Emboldened by the 'anonymity' that social media platforms provide, GCC citizens started to interact more with their governments to express grievances and criticisms, and to call for political reform and greater participation.

As the Arab uprisings spread across the Middle East and North Africa, Bahrain and Oman were the two GCC countries most directly affected by the wave of protests and physical demonstrations. In Bahrain,[20] thousands took to the streets to demand greater democracy and an end to sectarian discrimination, in response to which the government declared a state of emergency and sought the assistance of neighbouring countries in quelling the protests. Unprecedented protests in Oman[21] called for economic reforms, more jobs and an end to corruption; these protests were also put down by the security forces. The legitimacy of the political systems of the other GCC countries was also called into question, even if these did not see mass protests in the same way as did Bahrain and Oman.[22] Social media platforms played a key rallying role.

It is in this context that most of the revamping or enactment of cybercrime laws currently in force in the GCC countries took place (see Table 2). With their implementation, the laws criminalized a wide array of forms of expression, using vaguely worded and far-reaching provisions that depart from international human rights norms. A case can be made that these laws were primarily a reaction to governments' concerns about regional political change, and that the principal aim of anti-cybercrime legislation adopted by GCC states from 2011 onwards was to assist in strengthening regional governments' grip on social media, and to stymie the potential for spillover via online platforms of political unrest from other Arab countries. This would, moreover, be consistent with the GCC countries' long-standing restrictions

[16] Buller, A. (2016), *The Female Instagram Entrepreneurs of Saudi*, World Government Summit, 16 February 2016, https://worldgovernmentsummit.org/knowledge-hub/the-female-instagram-entrepreneurs-of-saudi.
[17] Arabian Business (2017), 'Revealed: more than 15m people follow Dubai ruler on social media', 13 January 2017, http://www.arabianbusiness.com/revealed-more-than-15m-people-follow-dubai-ruler-on-social-media-658895.html.
[18] Peel, M. (2012), 'Gulf states crack down on Twitter users', *Financial Times*, 18 June 2012, https://www.ft.com/content/1e647122-a8d1-11e1-be59-00144feabdc0.
[19] Ibid.
[20] BBC (2013), 'Arab Uprising: Country by Country – Bahrain', 16 December 2013, http://www.bbc.com/news/world-12482295.
[21] Ibid.
[22] Peterson, J. E. (2012), *The GCC states: participation, opposition and the fraying of the social contract*, Kuwait Programme on Development, Governance and Globalisation in the Gulf States, London School of Economics (LSE), December 2012, http://eprints.lse.ac.uk/55258/1/Peterson_2012.pdf.

on other forms of freedom of expression. For political activists and ordinary citizens to attempt to challenge the ruling establishment and the status quo via online platforms was bound to be met with an equivalent form of repression.[23]

Table 2: Cybercrime laws in the GCC in the context of the Arab uprisings

Country	Legislation enacted
Saudi Arabia	March 2007*
Oman	February 2011
UAE	August 2012†
Bahrain	September 2014‡
Qatar	September 2014
Kuwait	July 2015

* In March 2015 Saudi Arabia revised its existing legislation to introduce a so-called 'naming and shaming' penalty, for cases in breach of Article 6 of the cybercrime law, allowing for the publication of a summary of the final ruling in one or more local newspapers, with the costs of publication being chargeable to the offender.[24]
† The UAE's previous cybercrime legislation, in force since 2006, was abrogated at this time.
‡ Prior to enacting its cybercrime law, in November 2013 Bahrain inaugurated a Cyber Safety Directorate, mandated with the task of monitoring websites and social media networks.[25]

Cybercrime legislation: comparing the global and GCC approaches

There is no universally agreed definition of the term 'cybercrime'. The approach adopted by most relevant international and regional instruments has been in defining the term as a set of conducts or a collection of acts, making it an umbrella term rather than assigning a single definition. The Council of Europe Convention on Cybercrime (also known as the Budapest Convention),[26] which was opened for signature in 2001, follows this model, and is considered to be the most relevant international instrument on cybercrime. As at June 2018, there were 58 state parties to the convention, not including any GCC or Arab country.[27] It classifies cybercrime acts under one or more of the following four categories shown in Table 3.

[23] It is important to note that cybercrime laws were not the only tool that came to light in the context of the Arab uprisings; several countries in the GCC region have also enacted counterterrorism laws that serve a similar purpose. For instance, Saudi Arabia's 2014 counterterrorism law was strongly criticized by human rights organizations as being in effect a tool to further suppress peaceful political dissent. Moreover, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism expressed concern at Saudi Arabia's 'unacceptably broad' definition of terrorism, and at its use of the 2014 counterterrorism law and other national security provisions, contrary to international human rights standards, against human rights defenders, writers, bloggers, journalists and others who expressed non-violent views. Saudi Arabia updated the law again in November 2017, introducing the death penalty for a number of acts. UAE enacted a similar law in 2014 that was also heavily criticized for its threat to lives and to liberty. Bahrain revised its 2006 law in 2013, whereby revoking of citizenship was added as a penalty. Additionally, cybercrime laws have been used in different cases along with existing laws, particularly the Penal Code, and media law to prosecute people for online speech.
[24] Norton Rose Fulbright Data Protection Report (2015), 'Saudi Arabia updates cybercrime law to include "naming and shaming" penalty', 8 June 2015, https://www.dataprotectionreport.com/2015/06/saudi-arabia-updates-cybercrime-law-to-include-naming-and-shaming-penalty/ (accessed 14 June 2018).
[25] Bahrain News Agency (2013), 'Shaikh Fawaz praises Cyber Safety Directorate', 18 November 2013, http://bna.bh/portal/en/news/588716 (accessed 22 Jun. 2018).
[26] The Budapest Convention aims to help the signatory states harmonize their laws, enhance their cybercrime investigative techniques and increase international cooperation between them. For more, Council of Europe (2001), 'Convention on Cybercrime', 23 November 2001, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[27] In addition to most EU countries, members to the Budapest Convention include countries such as the US, Japan, Australia and Canada, for the full list of member countries, see http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=LeuugkuJ (accessed 18 Jun. 2018).

Table 3: Cybercrime acts as defined in the Budapest Convention

Offences against the confidentiality, integrity and availability of computer data and systems	Computer-related offences (e.g. credit card fraud, advance fee fraud)	Content-related offences	Copyright-related offences
Illegal access (e.g. hacking, circumventing of a password)	Computer-related forgery	Offences related to child pornography	Offences related to infringements of copyright and related rights
Illegal interception (e.g. email interception)	Computer-related fraud	Acts of racist and xenophobic nature*	
Data interference (e.g. use of malwares, spyware, creating backdoors)		Hate speech	
System interference (e.g. denial of service – DoS)			
Misuse of devices			

* An additional protocol to the Convention was adopted in 2003 to address racist and xenophobic materials committed through computer networks.

In defining the parameters of cybercrime, this paper follows the approach of the Budapest Convention. A similar approach is adopted by the Arab Convention on Combating Information Technology Offences,[28] a League of Arab States (Arab League) convention signed by all GCC countries and ratified by all of them except for Saudi Arabia.[29]

Most national legislation on cybercrime follows the same approach. Only a very small number of national laws include the term 'cybercrime' (or variations thereof) either in the title or in the scope of their legislation.[30] In the GCC, by contrast, the term 'cybercrime' features in the title of the legislation in all countries but Bahrain and Kuwait (see Table 4). As in most countries, however, these laws do not attempt to provide a legal definition of cybercrime. They rather attribute the term, using slightly different formulations, to include the crimes or acts referred to in the provisions of these laws.[31]

Analysis of the cybercrime laws of the GCC countries shows two main areas where these laws depart from international practice on cybercrime legislation. The first relates to the structure of the laws, and the second to content.

[28] League of Arab States (2010), 'Arab Convention on Combating Information Technology Offences'. English-language version available at http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences (accessed 22 Jun. 2018).
[29] The Convention has been criticized for or its vaguely worded provisions, without adequate definitions: see for example Taher, M. (2015), 'Commentary on the Arab Convention for Combating Information Technology Offences' [originally in Arabic], Association for Freedom of Thought and Expression (AFTE), https://afteegypt.org/digital_freedoms/2015/03/11/9770-afteegypt.html.
[30] United Nations Office on Drugs and Crime (UNODC) (2013), *Comprehensive Study on Cybercrime*, Draft – February 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
[31] Saudi Arabia: 'any action which involves the use of computers or computer networks in violation of the provisions of this law'; Qatar: 'any act involving an unlawful use of an information technology technique, an information system or the internet in violation of the provisions of this law'; Kuwait: 'any act committed through the use of computer or information network or other means of information technology in violation of the provisions of this law'; and Oman: 'crimes which are referred to in this law'.

Table 4: Cybercrime laws in the GCC countries

	Bahrain	Kuwait	Oman	Qatar	Saudi Arabia	UAE
English translation	Law No. (60) of 2014 on Information Technology Crimes	Law No. (63) for the year 2015 on Combating Information Technology Crimes	Royal Decree No 12/2011 issuing the Cyber Crime Law[a]	Law No. (14) of 2014 Promulgating the Cybercrime Prevention Law[b]	Anti-Cyber Crime Law, Royal Decree No. M/17, 26 March 2007[c]	Federal Decree-Law No. (5) of 2012 on Combating Cybercrimes[d]
Original title	قانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات[e]	قانون رقم (٦٣) لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات[f]	مرسوم سلطاني رقم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات[g]	قانون رقم (١٤) لسنة ٢٠١٤ بإصدار قانون مكافحة الجريمة الالكترونية[h]	نظام مكافحة الجريمة الالكترونية، م/١٧، ١٤٢٨/٣/٨ ه[i]	مرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات[j]

Sources: a: Available at http://www.qcert.org/sites/default/files/public/documents/om-ecrime-issuing_the_cyber_crime_law-eng-2011.pdf; b: Available at http://chato.cl/blog/files/QatarCybercrimeLaw_unofficial_translation.pdf; c: Available at http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf; d: Available at http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf; e: Available at http://www.acees.gov.bh/cyber-crime/anti-cyber-crime-law-in-the-kingdom-of-bahrain/; f: Available at https://www.e.gov.kw/sites/kgoarabic/Forms/CAITLawNo.63of2015oncombatingInformationTechnologyCrimes.pdf; g: Available at http://www.cert.gov.om/library/publications/Cyber_Crime_Law.pdf; h: Available at http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/100242/120183/F1232109237/100242.pdf; i: Available at https://www.bog.gov.sa/ScientificContent/RelatedSystems/Documents/äÜÇã%20ãßÇÝÍÉ%20ÇáÌÑÇÆã%20ÇáãÚáæãÇÊíÉ%201428åÜ.pdf; j: Available at http://www.wipo.int/wipolex/ar/text.jsp?file_id=316910.

Structure

The main issue in the GCC countries with regard to cybercrime legislation is in the lack of procedural laws that regulate cybercrime investigations and prosecutions. All cybercrime laws in the GCC countries include definitions of the terms used in the law, as well as substantive criminal law articles that criminalize the offences considered as constituting cybercrimes. However, few of these laws elaborate on other important aspects of the law that are found in some of the main international and regional instruments on cybercrime.[32] These include: *procedural law* (such as search and seizure of computer hardware or data, order for stored computer data, expedited preservation of computer data); *electronic evidence* (such as admissibility of electronic evidence and records); *jurisdiction* (such as the territorial principle, nationality principle of offender, dual criminality); *international cooperation*; and *service provider liability and responsibility* (such as monitoring obligations, voluntary supply of information, liability of hosting providers).

Of the GCC countries, Qatar's anti-cybercrime law is the most comprehensive, elaborating on, in addition to criminalization provisions:

- Evidence and investigation procedures;
- Service providers' obligations;
- State authorities' obligations;
- International cooperation;
- Mutual legal assistance; and
- Extradition of criminals.

[32] For more on cybercrime legislation and frameworks, see Annex 3, Provisions of International and Regional Instruments, UNODC (2013), *Comprehensive Study on Cybercrime*.

The other GCC countries rely in their procedures on general rules that do not take into account the specificity of cybercrime cases. Bahrain has provisions on procedural law, but no provisions on other pertinent areas of the law mentioned above.

The absence of such provisions – which would normally be enacted in new cybercrime laws or incorporated in existing laws – seriously hampers the effectiveness of any cybercrime investigation, since these guide the work of law enforcement and the judiciary in efforts to combat cybercrime. In addition to guiding the fight against cybercrime, these provisions should also contain the necessary safeguards to ensure that the powers granted to law enforcement and the judiciary through these laws are not being abused or used in an intrusive way.

Given the transnational dimension of cybercrime, the lack of legal frameworks regulating how states deal with one another in the context of a cybercrime undermines a country's ability to perform cross-border investigations and prosecutions in a timely manner and also raises issues of sovereignty.[33] It also means that any country that lacks the appropriate frameworks is left outside global efforts aimed at identifying the best responses to the emerging challenges presented by cybercrime.

In the absence of these provisions, therefore, the capacity of states to investigate, prosecute and adjudicate on cybercrime nationally, and to facilitate cooperation in transnational investigations in a way that is conducive to successful results, is seriously constrained.[34]

> The lacuna in dealing with electronic evidence has led in some cases to the mishandling of evidence, rendering it inadmissible. The absence of procedural law specifically applicable to cybercrime cases is thus an obstacle to all those involved in investigating, prosecuting and adjudicating cybercrime cases.

To take the example of the UAE, given the lack of special procedures for cybercrime cases, procedures for electronic evidence are governed by the Criminal Procedures Law. Judges thus apply general rules of evidence to cybercrime cases. The main issue with this is that these rules apply to 'traditional' types of crimes, investigation of which is primarily focused on traditional eyewitness accounts and the collection of physical evidence. There are no provisions regulating, for example, the collection, retention and disclosure of stored computer data or traffic. This lacuna in dealing with electronic evidence has led in some cases to the mishandling of evidence, rendering it inadmissible.[35] The absence of procedural law specifically applicable to cybercrime cases is thus an obstacle to all those involved in investigating, prosecuting and adjudicating cybercrime cases. Key judicial figures in the UAE seem to be supportive of a new law dealing with electronic evidence,[36] identifying the lack of such legislation as a major impediment to dealing with the distinct nature of electronic evidence. The need

[33] For more on this, see Hakmeh, J. (2016), 'Building a Stronger International Legal Framework on Cybercrime', Chatham House Expert Comment, 6 June 2017, https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime.
[34] Ibid.
[35] Aljneibi, K. (2014), 'The Current Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform', University of Bangor, thesis for DPhil, http://e.bangor.ac.uk/4992/1/Aljneibi%20khaled%20thesis.pdf (accessed 22 Jun. 2018).
[36] According to the former president of the UAE's Federal Supreme Court, the UAE faces procedural problems related to electronic evidence. In his assessment, there is a lack of knowledge regarding how to both preserve and examine electronic evidence. He has called for new legislation to be enacted, as the existing general rules of evidence are not commensurate with the nature of electronic evidence. Dubai's Chief Prosecutor has identified the absence of a law regulating electronic evidence as one of the major problems, in addition to the lack of effective international cooperation and cooperation mechanisms emphasizing the necessity of having a procedural for cybercrime and to regulate electronic evidence. The General Director of the Institute of Training and Judicial Studies in Abu Dhabi has agreed with this, stating that the UAE's current laws are unable to deal with the distinct nature of electronic evidence calling for the creation of a specific procedural law. See Aljneibi, K. (2014), 'The Current Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform'.

for laws regulating effective international cooperation, and cooperation mechanisms in global evidence collection and in transnational investigations, was also highlighted as a key shortcoming of the current UAE legal framework.

In Oman, moreover, one of the main obstacles to successful convictions in cybercrime cases, according to the country's Information Technology Authority, is that judges are not incorporating the concept of computer crime, and what constitutes digital evidence, in their cybercrime cases.[37] And in Bahrain, inadequacies in the legislation especially in relation to electronic evidence are in effect resulting in impunity for many apparent perpetrators.[38]

Content

As already stated, all GCC cybercrime laws cover in their texts offences that are broadly similar to the offences detailed under the Budapest Convention – i.e. offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences and copyright-related offences. Notably, however, when it comes to the content-related offences, all GCC countries, with the exception of Bahrain,[39] have introduced as part of their cybercrime laws provisions that criminalize a wide spectrum of content. Such content is not covered by the Budapest Convention and is in tension with the broad latitude given to freedom of expression in international human rights law. Table 5 sets out these provisions, along with the corresponding sanctions.[40]

[37] Oman response to a cybercrime questionnaire for member states by the United Nations Office on Drugs and Crime (UNODC) as part of the *Comprehensive Study on Cybercrime, 2013*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjArvyW5v_aAhWiA8AKHTURDH0QFjAAegQIABAq&url=http%3A%2F%2Fwww.combattingcybercrime.org%2Ffiles%2Fvirtual-library%2Fnational-laws%2Freply-to-cybercrime-questionnaire-for-member-states-%2528oman%2529.xlsm&usg=AOvVaw1LhyOBaGoNWaQ2ifzsTye1 (accessed 22 Jun. 2018).

[38] A thesis at the University of Bahrain confirms the importance of electronic evidence as a definitive proof in the criminal field, Al Wasat, in Arabic, '6', الإلكتروني' الدليل حجية تؤكد البحرين جامعة في أطروحة July 2015, http://www.alwasatnews.com/news/1006310.html (accessed 22 Jun. 2018).

[39] During a workshop, *Cybercrime and the Digital Economy in the GCC Countries*, organized by Chatham House and the Mohammed Bin Rashid School of Government in Dubai in March 2017, one participant noted that the reason behind not including in the Bahraini cybercrime law provisions on content-related speech that were not mentioned in the international instruments is that because these offences are already criminalized under the Bahraini Penal Code and therefore there was no need for re-including them in the cybercrime law.

[40] Table 5 groups the offences across the six GCC countries into several categories to show the similarities that exist in the offences and punishments in the GCC cybercrime laws. However, it is important to note that the text and the extent of each offence(s) vary from one law to the other. Therefore, for a specific wording of the offence(s), the actual texts of the laws should be consulted.

Table 5: Content-related offences not foreseen in other international instruments[41]

Offence	Kuwait	Saudi Arabia	Oman	Qatar	UAE
Insulting or defaming religion or religious values	**Article 6** Imprisonment: up to 1 year; and/or Fine: 5,000–20,000 KWD	**Article 6** Imprisonment: up to 5 years; and/or Fine: up to 3,000,000 SAR	**Article 19** Imprisonment: up to 3 years; and/or Fine: 1,000–3,000 OMR		**Article 35** Imprisonment: up to 7 years (if targeted at Islamic religion); and/or Fine: 250,000–1,000,000 AED
Prejudicing public order, public ethics/morals and social values	**Article 4(4)** Imprisonment: up to 2 years; and/or Fine: 2,000–5,000 KWD **Article 6** Fine: 3,000–1,000 KWD	**Article 6** Imprisonment: up to 5 years; and/or Fine: up to 3,000,000 SAR	**Article 17** Imprisonment: up to 3 years; and/or Fine: 100–3,000 OMR **Article 19** Imprisonment: up to 3 years; and/or Fine: 1,000–3,000 OMR	**Article 8** Imprisonment: up to 3 years; and/or Fine: up to 100,000 QAR	**Article 24** Imprisonment: Temporary (period not specified); and Fine: 500,000–1,000,000 AED **Article 28** Imprisonment: Temporary (period not specified); and Fine: up to 1,000,000 AED
Invading privacy, publishing news, secrets, electronic photos or photographs, scenes, comments, statements or information even if true or correct	**Article 6** Fine: 3,000–1,000 KWD	**Article 3** Imprisonment: up to 1 year; and/or Fine: up to 500,000 SAR **Article 6** Imprisonment: up to 5 years; and/or Fine: up to 3,000,000 SAR	**Article 16** Imprisonment: up to 3 years; and/or Fine: 1,000–5000 OMR	**Article 8** Imprisonment: up to 3 years; and/or Fine: 100,000 QAR	**Article 21** Imprisonment: at least 6 months; and/or Fine: 150,000–500,000 AED
Defamation and slander		**Article 3** Imprisonment: up to 1 year; and/or Fine: up to 500,000 SAR	**Article 16** Imprisonment: up to 3 years; and/or Fine: 1,000–5,000 OMR	**Article 8** Imprisonment: up to 3 years; and/or Fine: up to 100,000 QAR	**Article 20** Imprisonment: period not specified; and/or Fine: 250,000–500,000 AED **Article 21** Imprisonment: at least 1 year; and/or Fine: 250,000–500,000 AED
Damaging state reputation, criticizing, offending, insulting or slandering the ruler, his family, state symbols or a public official	**Article 6** Fine: 5,000–20,000 KWD				**Article 20** Imprisonment: period not specified; and/or Fine: 250,000–500,000 AED **Article 29** Imprisonment: Temporary (period not specified); and Fine: up to 1,000,000 AED

[41] As of 18 June 2018: 1 USD = 0.30 KWD; 3.75 SAR; 0.39 OMR; 3.64 QAR; 3.67 AED.

Offence	Kuwait	Saudi Arabia	Oman	Qatar	UAE
Damaging/threatening national unity and security, foreign policy Overthrowing the ruling regime/changing the system	**Article 6** Fine: 3,000–10,000 KWD **Article 7** Imprisonment: up to 10 years			**Article 6** Imprisonment: up to 3 years; and/or Fine: up to 500,000 QAR	**Article 24** Imprisonment: Temporary (period not specified); and Fine: 500,000–1,000,000 AED **Article 28** Imprisonment: Temporary (period not specified); and Fine: up to 1,000,000 AED **Article 30** Imprisonment: Life
Organizing marches without permission					**Article 32** Imprisonment: period not specified; and Fine: 500,000–1,000,000 AED
Spreading false news which damage the reputation and prestige of the country (retweeting)				**Article 6** Imprisonment: up to 3 years; and/or Fine: up to 500,000 QAR **For disseminating the news (e.g. retweeting)** Imprisonment: up to 1 year; and/or Fine: up to 250,000 QAR	
Insulting the constitution or judges and prosecutors or infringing on judicial integrity and impartiality	**Article 6** Fine: 3,000–10,000 KWD				
Participating and supporting an unauthorized group					**Article 26** Imprisonment: at least 5 years; and Fine: 1,000,000–2,000,000 AED

International law and freedom of expression online

The right to freedom of expression is a fundamental human right enshrined in all major international and regional human rights law instruments, such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights (ECHR), the Arab Charter on Human Rights (Arab Charter), the American Convention on Human Rights (ACHR), and the African Charter on Human and Peoples' Rights (ACHPR).

Box 1: International Covenant on Civil and Political Rights – Article 19

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
   a. For respect of the rights or reputations of others;
   b. For the protection of national security or of public order (ordre public), or of public health or morals.

With the progression of communications technology – in particular the very rapid increase in the importance of social media as a medium for seeking, receiving and imparting information – the critical need to interpret human rights norms as they might apply in the contemporary interconnected world was recognized. Protecting online users from violations of their internet-related human rights became all the more imperative as governments in certain countries enacted legislation that allowed for monitoring the internet not as a tool to fight cybercrime but instead as a mechanism against dissidence, including critical and unwanted speech online.[42]

In this context, in July 2012 the UN Human Rights Council[43] adopted Resolution 20/8, on the promotion, protection and enjoyment of human rights on the internet, affirming:

> The same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[44]

[42] See for example Human Rights Watch (HRW) (2012), 'Philippines: New 'Cybercrime' Law Will Harm Free Speech', 28 September 2012, https://www.hrw.org/news/2012/09/28/philippines-new-cybercrime-law-will-harm-free-speech.
[43] The Human Rights Council is an intergovernmental body within the UN system, made up of 47 states responsible for the promotion and protection of all human rights around the globe, created on 15 March 2006 by UNGA A/RES/60/251.
[44] UN General Assembly (UNGA) (2012), *The promotion, protection and enjoyment of human rights on the Internet*, 16 July 2012 A/HRC/RES/20/8 http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8.

This ground-breaking resolution – the first to recognize the importance of a global and open internet as a 'driving force in accelerating progress towards development in its various forms',[45] and as 'an important tool for development and for exercising human rights'.[46] Those principles were reaffirmed in several resolutions, including UN General Assembly Resolution 26/13 of June 2014[47] and Resolution 32/13 of July 2016.[48]

The Human Rights Council subsequently adopted several other resolutions to reaffirm previously guaranteed rights in an internet context. These include Resolutions 21/16[49] and 24/5,[50] on the rights to freedom of peaceful assembly and association; Resolution 22/6,[51] on protecting human rights defenders; and Resolution 23/2,[52] on the role of freedom of opinion and expression in women's empowerment.

It should be noted, however, that – as is similarly the case with regard to 'offline' speech – freedom of expression online is not absolute. In accordance with Article 19 of the ICCPR, freedom of speech can be subject to certain restrictions as provided for by law and as necessary to protect the rights and reputations of others, national security, public order and public health and morals.[53] In practice, this means that while freedom of expression is the rule, whether offline or online, some restrictions are permissible, albeit they are considered as the exception to this rule.

In 2011 the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion emphasized the importance of distinguishing between three types of expression:

> (a) expression that constitutes an offence under international law and can be prosecuted criminally;
> (b) expression that is not criminally punishable but may justify a restriction and a civil suit; and
> (c) expression that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others.[54]

Under the first type, several 'exceptional' forms of expression are prohibited. These are content related to: child pornography; direct and public incitement to commit genocide; advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; and incitement to terrorism.[55]

According to the Special Rapporteur, any other form of expression – i.e. that falls outside these prohibited four categories – should not be criminalized, as this may be counter-effective and the threat of harsh sanctions may create a significant 'chilling effect' on the right to freedom of expression.[56] In relation

[45] Ibid.
[46] Ibid.
[47] UNGA (2014), *The promotion, protection and enjoyment of human rights on the internet*, 20 June 2014, A/HRC/26/L.24 https://documents-dds-ny.un.org/doc/UNDOC/LTD/G14/059/67/PDF/G1405967.pdf?OpenElement.
[48] UNGA (2016), *The promotion, protection and enjoyment of human rights on the internet*, 1 July 2016, A/HRC/RES/32/13, http://www.refworld.org/docid/57e916464.html.
[49] UNGA (2012), *The right to freedom of peaceful assembly and of association*, 11 October 2012, A/HRC/RES/21/16, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/21/16.
[50] UNGA (2013), *The right to freedom of peaceful assembly and of association*, 8 October 2013, A/HRC/RES/24/5, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/24/5.
[51] UNGA (2013), *Protecting Human Rights defenders*, 12 April 2013, A/HRC/RES/22/6 http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/22/6.
[52] UNGA (2013), *The role of freedom of opinion and expression in women's empowerment*, 24 June 2013, A/HRC/RES/23/2 http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/23/2.
[53] UNGA (1966), *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, Article (19), http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf.
[54] UNGA (2011), *Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 10 August 2011, A/66/290, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290.
[55] Ibid.
[56] Ibid.

to defamation offences, for example, a number of human rights organizations and experts have called for the abolition of all criminal defamation laws, and for these to be replaced, where necessary, by appropriate civil defamation laws.[57]

Exceptionally, some limitations on the right to freedom of expression may be permissible under international human rights law; however, any such restrictions must pass the three-part, cumulative test of legality, legitimacy and proportionality:[58]

For restrictions to be permissible, they need first to be *prescribed by an unambiguous law* – i.e. the laws limiting specific kinds of speech must be very precise and clear so that the citizens are able to understand these laws and regulate their behaviour accordingly. Vaguely worded laws or provisions would not meet this standard and would therefore be considered illegitimate.

Second, limitations should be *enacted for the pursuance of a legitimate purpose* as per Article 19(3) of the ICCPR, namely for the respect of the rights or reputations of others; and/or for the protection of national security or of public order, or of public health or morals.

Third, any restrictions must *respect the principles of necessity and proportionality* – i.e. they have to be necessary and proportionate to the interest protected.

Freedom of expression online under GCC cybercrime laws

At the national level, five of the GCC countries protect freedom of expression – although with some far-reaching caveats – under their constitutions (see Table 6); the exception is Saudi Arabia, which does not have a written constitution.

Table 6: GCC constitutional provisions regarding freedom of expression

Country	Article
Bahrain	**Article 23:**[a] 'Freedom of speech and freedom to carry out scientific research shall be guaranteed. Every person shall have the right to express and propagate his opinion in words or in writing or by any other means, in accordance with the conditions and procedures specified by the law.'
Kuwait	**Article 36:**[b] 'Freedom of opinion and of scientific research is guaranteed. Every person has the right to express and propagate his opinion verbally, in writing, or otherwise, in accordance with the conditions and procedures specified by law.'
Oman	**Article 29:**[c] 'The freedom of opinion and expression thereof through speech, writing and other means of expression is guaranteed within the limits of the Law.'
Qatar	**Article 47:**[d] 'Freedom of expression of opinion and scientific research is guaranteed in accordance with the conditions and circumstances set forth in the law.'
UAE	**Article 30:**[e] 'Freedom of opinion and expressing it verbally or in writing or by other means shall be guaranteed within the limits of the law.'

Sources: a: Available at http://confinder.richmond.edu/admin/docs/Bahrain.pdf; b: Available at http://www.wipo.int/edocs/lexdocs/laws/en/kw/kw004en.pdf; c: Available at https://www.constituteproject.org/constitution/Oman_2011.pdf?lang=en; d: Available at http://portal.www.gov.qa/wps/wcm/connect/5a5512804665e3afa54fb5fd2b4ab27a/Constitution+of+Qatar+EN.pdf?MOD=AJPERES; e: Available at https://www.constituteproject.org/constitution/United_Arab_Emirates_2004.pdf.

[57] Joint declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression (2002), 'International Mechanisms for Promoting Freedom of Expression', http://www.oas.org/en/iachr/expression/showarticle.asp?artID=87&.

[58] UNGA, Promotion and protection of the right to freedom of opinion and expression; *The Sunday Times v. United Kingdom*, 26 April 1979, Application No. 6538/74, para. 49 (European Court of Human Rights); Lingens v. Austria, 8 July 1986, Application No. 9815/82, paras. 39–40 (European Court of Human Rights).

All GCC countries except for Oman are states parties to the Arab Charter on Human Rights.[59] The Charter enshrines in articles 24 and 32 the rights to information, freedom of opinion, political activity, and freedom of assembly and association.[60]

Internationally, of the GCC countries, only Bahrain and Kuwait have ratified the ICCPR, which is a legally binding instrument for states parties. All the GCC countries are members of the UN; this in theory means that their laws should respect the Universal Declaration on Human Rights, which, while not a binding human rights treaty, is a foundational document of the UN, and which upholds the right to freedom of expression in Article 19.[61] For the GCC states that have not ratified the ICCPR, this provision, together with the above provisions in the Arab Charter on Human Rights, provides the minimum rights to which citizens are entitled.[62]

Notwithstanding these various national, regional and international commitments and obligations on the part of the GCC countries, the provisions listed in Table 5 do not appear to meet the cumulative requirements of the three-part test as set out by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, and in the case law of international human rights bodies such as European Court of Human Rights. This raises concerns when viewed through the lens of international human rights law standards.

Under the three-part test, for limitations to be legitimate, they need first to be *prescribed by an unambiguous law*, which must be both accessible and foreseeable.

Most controversial provisions in the GCC cybercrime laws are drafted using vague terms, with no explicit definitions as to what these terms mean. As a result, citizens and residents could unintentionally break the law because of its ambiguity. This goes against the stipulation of the Human Rights Committee that legislation 'must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly', and that laws 'must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not'.[63]

Furthermore, the vagueness of their laws could enable creative interpretation on the part of the GCC governments to include new behaviours that may not have been anticipated when a piece of legislation was originally enacted. Notably, for example, in the context of the diplomatic crisis with Qatar that began in mid-2017,[64] the UAE general prosecutor announced that any sympathy shown for Qatar on social media (in practice by any user in the UAE) would be considered a cybercrime and could lead to imprisonment between three and 15 years or to a fine of at least 500,000 AED.[65] Clearly, this behaviour was not envisaged under the original text of the UAE's 2012 Federal Decree-Law No. (5) on Combating Cybercrimes.

[59] For a list of ratifications (in Arabic), see League of Arab States, http://www.lasportal.org/ar/legalnetwork/Documents/ÇáãíËÇÞ%20ÇáÚÑÈì%20áÍÞæÞ%20ÇáÃäÓÇä.pdf. Although this Arab League portal does not mention Kuwait's ratification of the Charter, other sources do mention it; see for example Mattar, M. (2013), 'Article 43 of the Arab Charter on Human Rights: Reconciling National, regional and International Standards', *Harvard Human Rights Journal*, 26 pp.91–147 http://harvardhrj.com/wp-content/uploads/2013/05/V26-Mattar.pdf.
[60] League of Arab States (2004), 'Arab Charter on Human Rights', 22 May 2004, https://app.icrc.org/elearning/curso-sobre-privacion-libertad/story_content/external_files/Carta%20Arabe%20de%20Derechos%20Humanos%20(2004).pdf.
[61] UNGA (1948), *Universal Declaration of Human Rights*, 10 December 1948, http://www.un.org/en/universal-declaration-human-rights/.
[62] Hannum, H. (1996), 'The UDHR in National and International Law', *Georgia Journal of International and Comparative Law*, 25(1), http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1396&context=gjicl.
[63] UN Human Rights Committee (HRC), General comment no. 34, Article 19, *Freedoms of opinion and expression*, 12 September 2011, CCPR/C/GC/34 para. 25.
[64] For a summary, see BBC (2017), 'Qatar crisis: what you need to know', 19 July 2017, http://www.bbc.com/news/world-middle-east-40173757.
[65] Al Arabiya English (2017), 'UAE: Showing sympathy for Qatar on social media is a cybercrime', 7 June 2017, http://english.alarabiya.net/en/News/gulf/2017/06/07/UAE-General-Prosecutor-says-showing-sympathy-for-Qatar-on-social-media-is-a-crime.html.

The second element under the three-part test is that restrictions should be *enacted for the pursuance of a legitimate purpose*:

The cybercrime laws of the GCC countries expand the definition of cybercrime to acts that are not considered as cybercrime by international legal instruments and other model laws, putting their legitimacy into question. Most of these laws criminalize offences such as defamation that give rise to civil liability only in jurisdictions with a high record of freedom of expression, and should be treated as such according to the international human rights standards.[66]

According to the terms of the ICCPR, legitimate purposes that would justify limitations on free speech entail the respect of the rights or reputations of others, the protection of national security or of public order, or of public health or morals.[67] A high threshold is set as regards what each legitimate purpose means. Concerning the protection of public morals, for example – an offence mentioned under all GCC laws, and an argument often used in the region to justify the curtailment of speech – the Human Rights Committee states that 'the concept of morals derives from many social, philosophical and religious traditions; consequently, limitations on the freedom to manifest a religion or belief for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition'.[68] Therefore, permissible limitations to free speech should be formulated taking into consideration the universality of human rights and based on the non-discrimination principle.[69] Limitations in the GCC are not in harmony with this rule.

Third, limitations must *respect the principles of necessity and proportionality*:

The provisions highlighted in Table 5 are far-reaching, giving governments extensive powers to prosecute anyone who publishes content that is not considered compatible with the social or political norms of the country. This goes strictly against the principles of necessity and proportionality. As set out by the Human Rights Committee:

> When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.[70]

The Committee further stipulates:

> The principle of proportionality must also take account of the form of expression at issue as well as the means of its dissemination. For instance, the value placed by the Covenant upon uninhibited expression is particularly high in the circumstances of public debate in a democratic society concerning figures in the public and political domain.[71]

The GCC cybercrime provisions shown in Table 5 do not meet these conditions in that they are broad, vague and far-reaching, and therefore at odds with international human rights standards.

To illustrate in more detail some limitations in the GCC cybercrime laws and the way international human rights law elaborates on these limitations, Table 7 considers Article 6 of the Kuwaiti cybercrime law[72] as against the ICCPR, to which Kuwait is a state party, and the Human Rights Committee's General Comments in this regard.

---

[66] Duffy, M. J. (2014), 'Arab Media Regulations: Identifying Restraints on Freedom of the Press in the Laws of Six Arabian Peninsula Countries', *Berkeley Journal of Middle Eastern & Islamic Law* (6)2, pp. 1–31, https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1036&context=jmeil.
[67] UNGA, *International Covenant on Civil and Political Rights*, Article (19).
[68] UN Human Rights Committee (1993), CCPR General Comment No. 22: Article 18 (Freedom of Thought, Conscience or Religion), 30 July 1993, CCPR/C/21/Rev.1/Add.4 https://tavaana.org/sites/default/files/G9318602.pdf.
[69] UN Human Rights Committee, 102 session, General Comment No.34, Article 19, paragraph 32.
[70] Ibid.
[71] Ibid, paragraph 35.
[72] i.e. Law No. (63) for the year 2015 on Combating Information Technology Crimes.

Table 7: Article 6 of Kuwait's cybercrime law compared with international human rights law

Criminalized under Article 6 of the Kuwaiti cybercrime law	International human rights law (ICCPR and Human Rights Committee ['The Committee'] General Comments)
Challenging, ridiculing or insulting God, the Holy Quran, the Prophets, the good companions or the wives of the Prophet.[a]	• Speech criticizing or ridiculing religion is protected under the ICCPR; hence, blasphemy laws are not compatible with the ICCPR unless they amount to advocacy of 'religious hatred that constitutes incitement to discrimination, hostility or violence'.[b] This qualification does not exist in Article 6. • The Committee stipulates that prohibitions that 'discriminate in favour of one religion or its adherents are impermissible, as are prohibitions on criticizing religious leaders or commentary on religious doctrine and tenets of faith'.[c]
Criticizing the Emir or quoting him without a special permission written by the Emiri Diwan.[d]	• ICCPR protects political speech, emphasizing the importance of the debate that involves public figures. • The Committee considers heads of states and public figures to be legitimate subjects of criticism and political opposition.
Insulting the judiciary or members of the Public Prosecution or infringing on the integrity and neutrality of the judiciary or the decisions of the courts or the investigative bodies.[e]	• The Committee allows criticism of state institutions and restrictions are permissible if they are in line with the proportionality principle. Hence, if the criticism is made for the defence of public interest, for example against abuse or misconduct, truth and error, it will be protected by international law particularly if the criticism was made without malevolence.
Publishing official secret communication and the publication of agreements and treaties held by the government of Kuwait prior to publication in the Official Gazette, except with the special permission of the concerned Ministry.[f]	• The Committee protects journalists as well as the access to information by the public. It states that the public is entitled to information which is of legitimate public interest and that this information should be disclosed unless it constitutes harm to national security which could be shown in an adequate manner by the authorities.
Damaging the relationships between Kuwait and other Arab or friendly countries if this is done through media campaigns.[g]	• The Committee has held that a state party to the ICCPR 'must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat'.[h] Article 6 does not elaborate on how 'harm to relationships' can be measured, and therefore its execution will be subject to the authorities' discretion.

Sources: Based on Human Rights Watch (2015), 'Kuwait: Cybercrime Law a Blow to Free Speech', https://www.hrw.org/news/2015/07/22/kuwait-cybercrime-law-blow-free-speech. a: Original text in Arabic, Article 6 of the Law No. (63) for the year 2015 on Combating Information Technology Crimes, https://www.e.gov.kw/sites/kgoarabic/Forms/CAITLawNo.63of2015oncombatingInformationTechnologyCrimes.pdf; and Article 19 of Law No 3 of 2006 regarding Publications and Publishing, available at http://www.gcc-legal.org/LawAsPDF.aspx?country=0&LawID=3280; b: UNGA, Promotion and protection of the right to freedom of opinion and expression, and Article 20 (2), ICCPR; c: HRW (2015), 'Kuwait: Cybercrime Law a Blow to Free Speech'; d: Original text in Arabic, Article 6 of the Law No. (63) for the year 2015 on Combating Information Technology Crimes, at https://www.e.gov.kw/sites/kgoarabic/Forms/CAITLawNo.63of2015oncombatingInformationTechnologyCrimes.pdf; and Article 20 of Law No 3 of 2006 regarding Publications and Publishing, http://www.gcc-legal.org/LawAsPDF.aspx?country=0&LawID=3280; e: Original text in Arabic, Article 6 of the Law No. (63) for the year 2015 on Combating Information Technology Crimes, https://www.e.gov.kw/sites/kgoarabic/Forms/CAITLawNo.63of2015oncombatingInformationTechnologyCrimes.pdf; Article 21 of Law No 3 of 2006 regarding Publications and Publishing, http://www.gcc-legal.org/LawAsPDF.aspx?country=0&LawID=3280; f: Ibid; g: Ibid; h: HRW (2015), 'Kuwait: Cybercrime Law a Blow to Free Speech'.

At the time of their enactment, the cybercrime laws of the GCC countries were condemned by international human rights organizations, which deplored the laws' damaging impact on civil liberties and their incompatibility with guarantees of human rights. GCC governments were urged to reconsider provisions intended to crack down on free speech and target online activism.[73]

Some GCC governments countered such criticism of their countries' respective cybercrime laws with public statements of their commitment to the defence of freedom of expression. In an official letter to the Committee to Protect Journalists in October 2013, Qatar's prime minister affirmed that the provisions of the forthcoming Qatari cybercrime law were 'free of any restrictions on the freedom of opinion and expression'; that the legislation was 'fully adherent' to the Qatar's constitution, 'ensuring the freedom of opinion and expression'; and that it did not breach 'the relevant international instruments'.[74] In mid-2015 Kuwait's justice minister, in response to speculation that had been circulating via social media that the country's new cybercrime legislation would enable the authorities to monitor online communications, stated: 'Everybody has the right to use […] mobile devices without being monitored.' He gave assurances that the cybercrime law's provisions were aimed at 'protecting the society, individuals and general security from online abuse', and asserted that the main objective of the law was 'responsible freedom'.[75]

Some GCC news outlets were similarly critical of the laws, as well as of their wide scope of application. There have been allegations that in some cases this has resulted in retaliatory measures against certain such organizations. There was speculation, for instance, that the temporary blocking of access to the Qatar-based online Doha News in late 2016 was linked, *inter alia*, to its recent criticism of Qatar's cybercrime law.[76] Notably, a few weeks before access was abruptly blocked, Doha News had published an editorial alleging that the law was being used 'by criminals and individuals with personal agendas to silence others', and urging that it be amended in the interests of preserving free speech and protecting journalism.[77]

> Several human rights defenders and activists have been prosecuted under these laws, deported or jailed for online comments, for blogging or for posting pictures that were aimed at social, religious or political ends.

Moreover, several human rights defenders and activists, as well as other regular social media users, have been prosecuted under these laws, deported or jailed for online comments, for blogging or for posting pictures that were aimed at social, religious or political ends. Some people who posted content that was intended to be humorous and satirical were also jailed and prosecuted.[78]

---

[73] See for example HRW (2012), 'UAE: Cybercrimes Decree Attacks Free Speech', 28 November 2012, https://www.hrw.org/news/2012/11/28/uae-cybercrimes-decree-attacks-free-speech; Amnesty International (2014), 'Qatar: New cybercrimes law endangers freedom of expression', 18 September 2014, https://www.amnesty.org/en/latest/news/2014/09/qatar-new-cybercrimes-law-endangers-freedom-expression/; Committee to Protect Journalists (CPJ) (2014), 'New cybercrime law could have serious consequences for press freedom in Qatar', 17 September 2014, https://cpj.org/2014/09/new-cybercrime-law-could-have-serious-consequences.php; (on Kuwait) Reporters Without Borders (2016), 'New Cyber Crimes Law restricts free expression and targets online activists', 21 January 2016, https://rsf.org/en/news/new-cyber-crimes-law-restricts-free-expression-and-targets-online-activists.

[74] Embassy of the State of Qatar, Washington DC (2013), Letter addressed by HE Abdullah Bin Nasser Bin Khalifa Al Thani, Prime Minister of Qatar to the Executive Director of the Committee to Protect Journalists (CPJ), 11 October 2013, available at https://cpj.org/Qatar-Alert_letter.pdf.

[75] *The Times of Kuwait* (2015), 'Cybercrime law guarantees privacy of individuals – Minister Al-Sane', 23 June 2015, http://www.timeskuwait.com/Times_Cybercrime-law-guarantees-privacy-of-individuals---Minister-Al-Sane.

[76] *The New Arab* (2016), 'Qatar accused of censorship after Doha News website blocked', 1 December 2016, https://www.alaraby.co.uk/english/news/2016/12/1/qatar-accused-of-censorship-after-doha-news-website-blocked.

[77] *Doha News* (2016), 'Qatar's cybercrime law is being abused by criminals and must be changed', 8 October 2016, https://dohanews.co/qatars-cybercrime-law-is-being-abused-by-criminals-and-must-be-changed/.

[78] Cassim, S. (2014), 'I went to jail for posting a comedy skit on YouTube. Is this the modern UAE', *Guardian*, 9 February 2014, https://www.theguardian.com/commentisfree/2014/feb/09/shezanne-cassim-jail-uae-youtube-video.

Some of these cases[79] have been taken up by international media as well as by human rights organizations in calling for the release of detainees and, in some instances, considering them 'prisoners of conscience'.[80]

The Human Rights Committee has emphasized that restrictions imposed by states on free speech 'may not put in jeopardy the right itself'.[81] However, the provisions of the GCC countries' cybercrime laws, given their text and scope of application, do jeopardize the right to free speech. Moreover, they have a chilling effect on freedom of expression and may lead to self-censorship. Their impact is on citizens and residents as well as on journalists and media workers who may be prosecuted for the mere fact of doing their job.

It is important to note that it is not only the GCC countries that have been criticized for their legal response to regulating the online sphere. In fact, most governments have been grappling with the issue of providing security while protecting liberties, the approach to which is largely determined by the historical, political and socio-economic backgrounds of the country in question. To give one example from Europe, Germany's 'NetzDG' law, which entered effect in January 2018, has been widely criticized by human rights organizations for chilling online speech, for not providing for adequate judicial oversight, and for placing the responsibility for censoring online content on social media companies on behalf of governments, and fining them if they fail to do so.[82]

Conclusion

While many countries around the world are still in the early stages of addressing the way they deal with cybercrime, the GCC countries have been taking decisive measures in recent years to protect their economies and populations from its consequences. For several reasons, however, the cybercrime laws that have been enacted in the region constitute, by their structure and content, an incomplete step towards fighting cybercrime.

With regard to fighting cybercrime, the structure of the GCC cybercrime laws does not elaborate on essential parts of the law that are crucial for investigations and for handling electronic evidence. Nor do these laws provide the necessary legal frameworks for international cooperation. None of the GCC countries is party to any international agreement on cybercrime; and the only regional platform that does exist in this respect – the Arab Convention on Combating Information Technology Offences – has not been used in fighting cybercrime, nor mentioned under any GCC cybercrime law. At present, GCC countries rely mostly on bilateral relationships and informal channels, such as police-to-police cooperation or informal agency-to-agency cooperation for fighting cybercrime. These routes are useful, but are not enough. Moreover, the fact that they are not based on clear and defined policies limits their efficacy in conducting successful investigations.

[79] See for example HRW (2013), 'Saudi Arabia: 600 Lashes, 7 Years for Activist Convicted of Insulting Islam Through Website, TV Interviews', 30 July 2013, https://www.hrw.org/news/2013/07/30/saudi-arabia-600-lashes-7-years-activist; Doha News (2015), 'WhatsApp insults lead to jail sentence for Qatar woman', 25 November 2015, https://dohanews.co/whatsapp-insults-leads-to-jail-sentence-for-qatar-woman/; Australian Associated Press via *Guardian* (2015), 'Australian deported from Abu Dhabi after 'writing bad words' on Facebook', 14 July 2015, https://www.theguardian.com/world/2015/jul/15/australian-deported-from-abu-dhabi-after-writing-bad-words-on-facebook; World Organization Against Torture OMCT (2016), 'Kuwait: Cyber Crimes Law silencing dissent, as Sara Al-Drees remains subject to prosecution in ongoing trial, says coalition trial observation report', 12 December 2016, http://www.omct.org/human-rights-defenders/urgent-interventions/kuwait/2016/12/d24098/.

[80] Amnesty International (2017), 'United Arab Emirates: Release Emirati Human Rights Defender Ahmed Mansoor!', 28 March 2017, https://www.amnesty.org/en/latest/campaigns/2017/03/release-emirati-human-rights-defender-ahmed-mansoor/.

[81] UN Human Rights Committee, 102 session, General Comment No.34, Article 19, paragraph 21.

[82] HRW (2018), Germany: Flawed Social Media Law. NetzDG is Wrong Response to Online Abuse, February 2018, https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law (accessed 22 Jun. 2018).

The Budapest Convention is the most relevant international instrument on cybercrime. Membership of the Convention is increasing, and new protocols are being added to address emerging challenges in cybercrime. Joining the Convention would help the GCC countries in harmonizing and updating their laws, in enhancing their cybercrime investigative techniques and in increasing international cooperation between them and between the other signatory countries.[83] However, the current content of most GCC countries' cybercrime laws may constitute an impediment to this endeavour. Article 15[84] of the Convention makes the powers provided to state parties subject to international human rights law standards. So it could be argued that the additional offences that exist in most of the GCC cybercrime laws highlighted in Table 5 might act as a barrier to these countries' accession to the Convention as the laws do not meet the protection safeguards set out in international human rights law.

Should the GCC countries choose not to accede to the Convention, each could seek observer status and could use the Convention as a guideline and a reference to update their laws accordingly, primarily as regards procedural law, electronic evidence and international cooperation. This would contribute to building mutual ground and would play a significant role in facilitating international cooperation on fighting cybercrime.

> Encouraging dialogue on social media and contributing to positive content – as opposed to stifling online speech – would go a long way towards creating common ground between citizens and their governments and, equally important, between citizens with different viewpoints, and contribute to fighting extremism and keeping vulnerable groups away from radicalization.

From a social standpoint, research has shown that youth in the GCC countries are not necessarily liberal or anti-establishment; their attitudes in fact reflect the variety of views that exist within the Gulf societies.[85] Therefore, encouraging dialogue on social media and contributing to positive content – as opposed to stifling online speech – would go a long way towards creating common ground between citizens and their governments and, equally important, between citizens with different viewpoints, and contribute to fighting extremism and keeping vulnerable groups away from radicalization. It would also foster dialogue on issues of public interest in the current regional context of socio-economic and political challenges.

Monitoring all online speech, which is what most cybercrime laws in the GCC countries in effect do, creates confusion regarding the issues at stake – i.e. between the issues that constitute a real risk and those that are simply in disagreement with what 'ought', in the view of the state, to be the narrative. International law strikes a good balance in this respect, elaborating on rights and limitations while respecting national differences. It sets the rules on how to limit extremism, hate speech, incitement to violence and other potential risks, while protecting free speech and other human rights. This gives governments that may otherwise fear for their citizens' safety a certain degree of comfort that should encourage them to lift the lid on social media and unleash its potential. The cybercrime laws

[83] For more on this, read Hakmeh, J. (2016), 'Tackling Cybercrime: Time for the GCC to Join the Global Efforts', Chatham House Expert Comment, 8 December 2016, https://www.chathamhouse.org/expert/comment/tackling-cybercrime-time-gcc-join-global-efforts (accessed 11 Apr. 2018).
[84] Budapest Convention (2001) http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (accessed 22 Jun. 2018).
[85] Kinnimont, J. (2015), *Future Trends in the Gulf*, Chatham House Report, London: Royal Institute of International Affairs, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150218FutureTrendsGCCKinninmont.pdf.

of the GCC countries do not at present take account of this. In their current form, these laws are at odds with international human rights law, standards and safeguards, and have an adverse impact on freedom of expression.

An argument can be made that the GCC governments have been attempting to constrain online speech through the enforcement of cybercrime laws, among other laws, that restrict freedom of expression and that give the authorities a very wide degree of discretion in the application of their provisions, as evidenced by recent cases prosecuted under these laws. Others might make the case that the reason for the laws being in their current shape is, rather, attributable to a draconian approach to the drafting process, limited policy expertise within the civil service, and the absence of civil society institutions that would feed into the process. Regardless of the reason, the end result is an online sphere that is heavily censored. Whether the censorship efforts serve as a distraction from the main social, political and economic issues that are being discussed over social media, or as a deterrence from discussing them, they are certainly an impediment to, and a distraction from, combating growing cybercrime, and they put the GCC governments in an untenable position globally in terms of the divergence from international human rights norms.

The institution, in the GCC countries, of cybercrime laws that are actually fit for purpose would go a long way in fighting cybercrime as internationally recognized, and in reaping the genuine benefits of social media. To this end, revamping the cybercrime laws of the six GCC members is urgently required, and is essential for better security, a better society and for better civil liberties.

About the author

Joyce Hakmeh is a research fellow in the International Security Department at Chatham House, and co-editor of the *Journal of Cyber Policy*. She is also a member of the Advisory Board to the Global Forum on Cyber Expertise (GFCE) and a member of its Working Group on Cybercrime. Her areas of expertise include cybercrime, cybersecurity, the rule of law and good governance, international criminal justice, and human rights. Previously, she worked for the UN, as well as for a number of other international and non-profit organizations. She was a fellow of the Queen Elizabeth II Academy for Leadership in International Affairs at Chatham House in 2016–17, during which time she published her first research paper for the institute, *Cybercrime and the Digital Economy in the GCC Countries*.

Acknowledgments

Thanks are due to all the reviewers who contributed to this paper, including the external reviewers and those from the International Security Department, the International Law Programme, and the Middle East and North Africa Programme at Chatham House. The author would also like to thank Jo Maher for editing the paper, and Henry Dodd for his support throughout this project.

This research paper is part of a three-year project, run by Chatham House and supported by the Ministry of Foreign Affairs of the Netherlands and the UK Cabinet Office, aiming to deepen the understanding of the dynamics of political and economic change in the Gulf and Arabian Peninsula.

Independent thinking since 1920

Cover image: A Saudi woman talks on her phone during the 'MiSK Global Forum', held in Riyadh under the slogan 'Meeting the Challenge of Change', on 15 November 2017.

Photo credit: Copyright © Fayez Nureldine/AFP/Getty Images

ISBN 978 1 78413 261 3

Typeset by Soapbox, www.soapbox.co.uk

This publication is printed on recycled paper.

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223