Research Paper

Joyce Hakmeh
International Security Department | June 2017

Cybercrime and the Digital Economy in the GCC Countries

CHATHAM HOUSE
The Royal Institute of International Affairs

Summary

- Cybercrime is an escalating threat to the economies of the Gulf Cooperation Council (GCC), and to their plans for digital transformation. Reliable data on the incidence of cybercrime in the region are lacking, but news reports and statements by police and government officials give anecdotal credence to the likelihood that the problem is increasing.

- A failure to tackle cybercrime would imperil strategic development plans intended to diversify GCC economies and reduce their reliance on the hydrocarbons sector. These plans involve expanding the region's digital capabilities – leveraging, among other things, the existence of a large cohort of tech-savvy young people and high levels of internet and mobile penetration. GCC states and cities are developing – and aspire to expand – 'smart infrastructure' consisting of networked devices, adaptive systems and other digital technologies. But many of the likely components of this infrastructure are known for poor security, and thus vulnerable to cyberattack.

- GCC states have invested heavily in cyber protection, and have developed a variety of legislative and other measures to tackle cybercrime. However, current policies and instruments are inadequate. Legal frameworks are underdeveloped and have yet to be fully implemented, and there is no common approach across the region. The speed of technological change means that anti-cybercrime tools, policies and laws must be continually evaluated and updated to remain effective. Differences in the substance of cybercrime laws, including the very definition of 'cybercrime', among GCC members pose problems for global policy coordination, as does uneven implementation.

- The development of cybercrime legal frameworks is essential to the management of cybersecurity risks in the GCC. Having cybercrime laws to which all states adhere, and that are in line with international norms and standards, would support a safe, trustworthy and secure internet. While all six GCC states have cybercrime laws in place, most of these laws focus on criminalization and expand the definition of content-related cybercrime to a wide spectrum of acts such as defamation and damaging the state's reputation – using vaguely worded provisions which may therefore fail to ensure adequate protection of human rights as defined in international law. In addition, in most cases GCC cybercrime laws neither elaborate on procedural law nor provide a legal basis for interstate cooperation.

- Regional and international anti-cybercrime cooperation in the GCC countries is still in its infancy. Most GCC countries still rely on informal regional and international channels, such as police-to-police or agency-to-agency cooperation. While useful, these mechanisms limit investigative actions, lack a common approach, and must operate within multiple law enforcement networks.

- The GCC needs to explore feasible and practical options for regional and international anti-cybercrime cooperation. One possible course of action would be to build on agreements already in place, such as the Arab Convention on Combating Information Technology Offences. Revising legislation, promoting expertise in the judiciary, and enhancing regional and international cooperation arrangements also need to be pursued as matters of urgency if the region is to benefit from a comprehensive, multi-stakeholder, multifaceted cybersafety framework.

Introduction[1]

Online activity and the use of digital technology have grown rapidly in the Gulf Cooperation Council (GCC) states.[2] Albeit with certain variations between countries, this has helped to boost prospects for a 'digital transformation' in which states and cities in the region could become international hubs for digital services. Such a shift offers a significant opportunity in the context of policy agendas to diversify the region's hydrocarbon-dependent economies. At the same time, however, digital growth has increased the GCC's vulnerability to cybercrime.[3] While the incidence, spread and effects of cybercrime in the region are difficult to measure precisely, a number of trends and figures suggest that cybercrime is growing rapidly[4] and that the region has become a magnet for such crime.

The rise in cybercrime has occurred in spite of heavy investment by GCC states in cyber protection, and the adoption of various measures including legislation. Cybercrime threatens growth of the digital economy. It shakes trust in the foundations of digital commerce, and in the 'smart infrastructure'[5] of interconnected devices, adaptive systems and other digital technologies which governments in the region are developing – and which they aspire to expand.

A number of factors suggest that the incidence, scale and impact of cybercrime are likely to increase further in the future. The first is the prospect of rapid growth in the digital economy, reflecting the prominence of digital strategies in the plans of GCC governments.[6] A second factor is the high speed of technology adoption, which makes it hard for policy to keep pace with rising cybercrime and evolving criminal methods. A third factor is the expected convergence of technologies as the 'Internet of Things' (IoT) expands and develops, potentially creating new risk exposures via huge numbers of networked devices. In short, the GCC region will likely find itself both continuing to grapple with the existing challenges of cybercrime and facing ever-evolving risks as a result of ongoing technological innovation.

Cybercrime is pervasive and cannot be completely eradicated. However, governments can limit its impact by creating a resilient overall economy and robust institutions, and by investing in deterrent capacity. Legislative frameworks play an intrinsic role in this process. In this context, it is important to consider whether existing GCC countermeasures — including legislation — are fit for purpose, or whether an overhaul is needed.

About this paper

This research paper offers an overall picture of the state of the digital economy in the GCC, and of progress to date in the region's attempted digital transformation. It also seeks, in particular,

[1] This paper was originally prepared to feed into discussions at the regional workshop 'Cybercrime and the Digital Economy in the GCC Countries', which was held in Dubai on 26 March 2017 by Chatham House in partnership with the Mohammed Bin Rashid School of Government (MBRSG).

[2] This paper uses the term GCC interchangeably to refer either to the individual countries belonging to the Gulf Cooperation Council (Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates) or to the region as a whole.

[3] For the purposes of this paper, the term 'cybercrime' is defined as any offence or collection of offences falling under at least one of the following categories: (i) offences against the confidentiality, integrity and availability of computer data and systems; (ii) computer-related offences; (iii) content-related offences; and (iv) offences related to infringements of copyright and related rights.

[4] Agence France-Presse (2017), 'Cyber-attacks on the rise, GCC warned', *The National*, 27 February 2017, www.thenational.ae/world/middle-east/cyber-attacks-on-the-rise-gcc-warned.

[5] Smart infrastructure is defined as 'the result of combining physical infrastructure with digital infrastructure, providing improved information to enable better decision making, faster and cheaper'. See Bowers, K., Buscher, V., Dentten, R., Edwards, M., England, J., Enzer, M., Parlikad, A. K. and Schooling, J. (undated), 'Smart Infrastructure – Getting more from strategic assets', Cambridge Centre for Smart Infrastructure and Construction, www-smartinfrastructure.eng.cam.ac.uk/files/the-smart-infrastructure-paper.

[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.

to highlight shared regional cybercrime challenges and their impact. The paper surveys the extent and effectiveness of existing measures – including legal instruments – for countering cybercrime, and proposes improvements to the policy regime and areas for potential intergovernmental cooperation. Although the focus is mainly on the GCC in aggregate, the paper also takes into account variations between the six countries in terms of digital development, the prevalence of cybercrime, and the nature and extent of countermeasures available.

The digital economy in the GCC countries: facts, figures and prospects

As shown in Table 1, GCC states have some of the highest internet and mobile penetration rates in the world.[7] GCC populations have high proportions of young people,[8] resulting in a tech-savvy generation of consumers of digital products and services. The tastes, consumption patterns and online habits of this cohort will play a large role in dictating the region's digital development.[9]

Table 1: Internet metrics for the GCC

Country	Internet users (% of population)	Mobile broadband subscriptions (per 100 inhabitants)	Fixed broadband penetration (per 100 inhabitants)	Mobile subscriptions (per 100 inhabitants)	Social media penetration (Facebook, per 100 inhabitants)	International bandwidth per internet user (Bit/s)
Bahrain	93.5	131.8	18.6	185.3	73	47,205
Kuwait	82.0	139.3	1.4	231.8	71	48,619
Oman	74.2	78.3	5.6	159.9	41	59,784
Qatar	92.9	80.0	10.1	153.6	95	71,566
Saudi Arabia	69.6	111.7	12.0	176.6	58	88,669
United Arab Emirates	91.2	92.0	12.8	187.3	94	107,914
GCC aggregate	76.0	115.0	12.8	184.0	66	84,659

Sources: 2016 data – ITU (2016), *Measuring the Information Society Report 2016*, pp. 240–247, www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2016.aspx (accessed Mar. 2017); 2017 data – 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, www.mbrsg.ae/getattachment/1383b88a-6eb9-476a-bae4-61903688099b/Arab-Social-Media-Report-2017 (accessed Mar. 2017).

GCC governments have been trying to capitalize on these attributes, and digital activity and processes are now well established. Countries in the region score either 'very high' or 'high' on the UN's E-Government Development Index (EGDI)[10] and E-Participation Index (EPI).[11] These two indicators measure, among other things, connectivity, the availability of government data, and mechanisms for informing government decision-making through online engagement. In addition, a growing number of the GCC's 24 largest cities[12] are embarking on ambitious 'smart city'

[7] ITU (2016), *Measuring the Information Society Report 2016*, pp. 240–247, www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf (accessed Mar. 2017).

[8] The average age in the GCC region is 27. Raghu, M. R. and Sartawi, M. (2012), 'GCC Demographic Shift: Intergenerational risk-transfer at play', Kuwait Financial Centre "Markaz", June 2012, www.markaz.com/MARKAZ/media/Markaz/Documents/Business%20Activities/DemographicsResearch-MarkazResearch-June-2012.pdf.

[9] Elmasry, T., Benni, E., 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.

[10] United Nations Department of Economic and Social Affairs (UNDESA) (2016), *United Nations E-Government Survey 2016*, p. 109 http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf.

[11] Ibid., p. 59.

[12] There are 24 cities with more than 300,000 inhabitants in the GCC, according to data from UNDESA (2015), *World Population Prospects: The 2015 Revision*, UNDESA, Population Division, https://esa.un.org/unpd/wpp/ (accessed Mar. 2017).

initiatives that involve widespread implementation of IoT platforms and a revamp of technological infrastructure. However, most states in the region still face considerable obstacles to digital transformation. Although this is primarily due to the lack of adequate governance structures,[13] shortcomings at the corporate level are also a factor. GCC companies have not fully embraced the digital economy. With their adoption of digital technology still in its infancy, companies are lagging behind governments and customers in terms of digital readiness.[14]

Several studies underline the region's progress, but also the limitations to this progress to date. According to a McKinsey paper[15] illustrating countries' current 'digitization' status – their variations in digital readiness, potential for digital growth, and challenges faced in effecting the necessary transition in their economies – the United Arab Emirates (UAE) is the most digitally advanced of the GCC states. In fact, it surpasses the levels of digital readiness of the US and Europe in terms of the adoption of digital technologies by consumers and government, and almost matches their level for the adoption of digital technologies by businesses. Qatar and Bahrain come second and third, respectively, in the study's ranking. Saudi Arabia, Oman and Kuwait are still behind the curve in terms of digital adoption.[16]

As a region, the GCC remains largely a consumer rather than a creator of digital technology and services. That is true for all GCC countries; they all score below the average in terms of information and communications technology (ICT) supply and innovation, with Qatar having a slightly more advanced position.[17] One striking fact in evidence of this is the low uptake of domain names relative to the region's remarkably high penetration of social media. The numbers of country code top-level domains (ccTLDs) – which are the domain names reserved for each country[18] – per 1,000 people are very low: for example, below 15 per 1,000 people in the UAE, below 11 in Qatar and below two in Saudi Arabia.[19] The Netherlands, in contrast, has around 330 ccTLDs per 1,000 people, Denmark around 232, and the UK around 165.[20] This shows the extent to which digital services in the GCC still rely heavily on foreign platforms, and the big gap that exists between GCC states and other digitally developed countries.

To establish itself as a leading region in the digital field, the GCC needs to become more of an innovator and producer. However, it is impeded in this by several aspects of its digital infrastructure.[21] Studies show that the GCC has so far realized only a small fraction of its 'digital potential' (as measured by the shares of digital services/products in private consumption, private investment, government expenditure, and imports and exports). As a result, the contribution of the digital economy to the GDP of these countries is still lower than in the benchmark digital economies in the West.[22] Venture capital funding is also less readily available,[23] and there are fewer ICT companies and 'unicorns'.[24]

[13] Elmasry et al. (2016), *Digital Middle East*.

[14] Papazian, S., Samad, R. A., Bohsali, S. (2016), *Preparing for the digital era: The state of digitization in GCC businesses*, Strategy Siemens, www.ideationcenter.com/media/file/Preparing-for-the-digital-era.pdf?_ga=1.55991470.42186429.1473322171.

[15] Elmasry et al. (2016), *Digital Middle East*.

[16] Ibid. Refer to Exhibit 4, p. 20.

[17] Ibid.

[18] The ccTLDs for the GCC countries are: Bahrain (.bh), Kuwait (.kw), Oman (.om), Qatar (.qa), Saudi Arabia (.sa) and the United Arab Emirates (.ae).

[19] EURid, (2016), *Middle East and Adjoining Countries DNS Study*, p. 78, www.icann.org/en/system/files/files/meac-dns-study-26feb16-en.pdf.

[20] EURid, (2016), *Quarterly update, 2016 Q1 Progress Report*, p. 11, https://eurid.eu/media/filer_public/df/fd/dffd1715-b85b-4013-9f09-bc70e06b5318/q1_2016.pdf.

[21] Taylor, E. (2016), *The Internet in the Gulf Countries: How Issues of Internet Access and Cybercrime Impact the Region*, Discussion Paper, London: Royal Institute of International Affairs, www.chathamhouse.org/event/internet-gulf-countries-how-issues-internet-access-and-cybercrime-impact-region.

[22] The digital economy accounts for the following shares of GDP in the GCC countries: 8 per cent in Bahrain, 5.1 per cent in Kuwait, 0.9 per cent in Oman, 0.4 per cent in Qatar, 3.8 per cent in Saudi Arabia and 4.3 per cent in the UAE. Elmasry et al. (2016), *Digital Middle East*, p. 15. Also see Exhibit 5, p. 25.

[23] Ibid. See Exhibit 10, p. 30.

[24] 'Unicorns' are start-ups valued at over $1 billion. Ibid. See Exhibit 9, p. 29.

Nevertheless, the outlook for growth in the digital economy remains positive. The rate of internet adoption by young people is high, and digital activity (as measured by data flows that enable rising connectivity, improved processes and economic value addition)[25] is increasing. The Middle East's digital universe is projected to reach two zettabytes[26] in size by 2020.[27] GCC governments also have ambitious plans for further development. All this conveys a picture of a region in which the opportunities for digital growth are tremendous if they can be seized quickly enough.

Reinforcing this sense of urgency is the need to diversify the GCC's existing economic base. Reliance on hydrocarbons constitutes a structural economic risk. Exploring sustainable options for the post-oil era is thus a policy priority.[28] This explains in part the appeal to policymakers of digital technology, with its promise of new services and business models supporting a vibrant knowledge economy that contributes to social inclusion, supports the development of small and medium-sized enterprises (SMEs), and boosts job creation, productivity and government efficiency.[29]

However, transforming a traditional economy into a digital one is a disruptive process. It requires all actors, from government downwards, to review their approaches to ensure that the clear vision, strong leadership and flexibility needed to adapt to change are in place. Part of this effort involves ensuring that risks – including of cyberattack – are identified and managed, and that a cybersecurity framework is in place.[30] Legal and regulatory frameworks must support the security of, and users' trust in, digital infrastructure. Law enforcement mechanisms and the judiciary also need to play their role in ensuring trust in the digital commercial environment.

Cybercrime in the GCC countries: trends, economic impact and current countermeasures

Accurate data on cybercrime are hard to come by. Most cybercrime victims in the GCC tend to be unaware of the occurrence of the crime,[31] and when they are aware of it, they tend to conceal their losses for fear of reputational damage or out of cultural considerations. Additionally, no official monitoring bodies produce independent, reliable statistics on a regular basis. More often than not, research tends to be conducted by private companies based on inconsistent methodologies and questionable assumptions and samples; in some instances this produces conflicting data with startling variations.[32] This raises the question of whether measuring cybercrime in statistics will ever be the best route to a well-informed understanding of its development, especially as most cybercrime goes unreported or undetected. Nonetheless, anecdotal evidence from news outlets and statements by police departments and high-level officials seems to confirm that cybercrime in the GCC is escalating.

[25] World Economic Forum, (2016), *Global Information Technology Report*, 'Chapter 1.2: Cross-Border Data Flows, Digital Innovation, and Economic Growth', p. 42, www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf.

[26] A zettabyte equals 1^{21} bytes, or 1 trillion gigabytes.

[27] This number is supposedly greater than the estimated number of grains of sand covering the entire Arabian Desert. Elmasry et al. (2016), *Digital Middle East*, p. 15.

[28] Kinninmont, J. (2015), *Future Trends in the Gulf*, Chatham House Report, London: Royal Institute of International Affairs, www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150218FutureTrendsGCCKinninmont.pdf.

[29] Elmasry et al. (2016), *Digital Middle East*, p. 26.

[30] Ayoub, R., Firth, C. M. and Nayaz, M. (2017), *Cyber resilience in the digital age*, World Government Summit in collaboration with EY, p. 5, https://worldgovernmentsummit.org/api/publications/document?id=24717dc4-e97c-6578-b2f8-ff0000a7ddb6.

[31] In 2014, an estimated 90 per cent of cybercrime victims in the UAE were unaware of the occurrence of the crime. See George, J. (2014), 'Majority UAE users hit by cyber bugs happily unaware', *Emirates 24/7*, 10 June 2014, www.emirates247.com/news/emirates/majority-uae-users-hit-by-cyber-bugs-happily-unaware-2014-06-10-1.552256.

[32] United Nations Economic and Social Commission for Western Asia (UNESCWA) (2015), *Policy Recommendations on Cybersafety and Combating Cybercrime in the Arab Region*, p.5, www.unescwa.org/sites/www.unescwa.org/files/uploads/policy-recommendations-cybersafety-arab-region-summary-english.pdf.

For example, according to the undersecretary of the Ministry of Interior in Kuwait, the incidence of cybercrime in that state rose by 170 per cent from 2015 to 2016.[33] Meanwhile the governor of Qatar's central bank, HE Sheikh Abdulla Bin Saoud Al-Thani, has stated that cybercrime in the country increased by 52 per cent in 2015.[34] In the UAE, cybercrime increased by 23.5 per cent year on year in 2015, according to the Dubai police.[35] In Saudi Arabia, 58 per cent of the population has experienced cybercrime, a rate 10 percentage points above the global average.[36]

Cyberattacks on infrastructure have caused repeated difficulty at government level. Major incidents have included the Shamoon malware attacks, which initially targeted state-owned Saudi Aramco in 2012 and disrupted the company's operation for five months in what was referred to as the biggest hack in history.[37] The same malware caused disruption again in November 2016[38] and January 2017.[39] Although the damage from the two most recent attacks has been arguably less than that of the attacks in 2012, the vulnerability to cyberattack of critical national infrastructure remains evident.[40]

The implications for the corporate sector are no less substantial. A recent survey showed that the losses incurred by companies in the Middle East as a result of cybercrime are significantly larger than those of their international counterparts. In 2015, 56 per cent of those surveyed lost more than US$500,000, compared with 33 per cent of companies globally; and 13 per cent lost at least three working days to the effects of cybercrime, compared with 9 per cent of global respondents to the survey. Eighteen per cent of respondents experienced a total of over 5,000 attacks in that year, a higher percentage than for any other region and almost double the global average.[41]

The main factors contributing to cybercrime in the GCC have arguably been vulnerabilities in digital communications networks and supply chains, consumer complacency[42] and growth in the user base of online consumers.

Apart from the direct financial losses it causes, cybercrime can be damaging at many levels. It can result in the loss of intellectual property and confidential business information, reducing a company's competitiveness. It can present opportunity costs, including service and employment disruptions. It can add to the costs of network security, insurance and post-cyberattack recovery.[43] And it can cause reputational damage, in some cases even leading to criminal proceedings against the affected organization and reducing public trust in the organization's online operations.

[33] *Al Anbaa* (2017), 'Cybercrimes increased by 170% in 2016 and a 15% decrease in traffic accidents' [original in Arabic], www.alanba.com.kw/ar/kuwait-news/incidents-issues/718379/31-01-2017-9.

[34] Carnegie Mellon University Qatar (2016), 'Qatar Central Bank governor outlines plan to ensure cyber resiliency', 15 November 2016, www.qatar.cmu.edu/news/qatar-central-bank-cybersecurity/.

[35] Agarib, A. (2016), 'Internet crimes up by 23.5% in Dubai', *Khaleej Times*, 16 October 2016, www.khaleejtimes.com/nation/crime/internet-cyber-crimes-up-by-235-in-dubai.

[36] Arab News (2016), 'Cybercrime hit 6.5m in Kingdom last year', 11 August 2016, www.arabnews.com/node/967966/saudi-arabia.

[37] Pagliery, J. (2015), 'The inside story of the biggest hack in history', CNN, 5 August 2015, http://money.cnn.com/2015/08/05/technology/aramco-hack/.

[38] Finkle, J. and Wagstaff, J. (2016), 'Shamoon virus returns in new Gulf cyber-attacks after four-year hiatus', Reuters, 1 December 2016, www.reuters.com/article/us-cyber-saudi-shamoon-idUSKBN13Q38B.

[39] Paganini, P. (2017), 'Saudi Arabia is warning organizations in the country of a resurrection of the dreaded Shamoon malware', *Security Affairs*, 25 January 2017, http://securityaffairs.co/wordpress/55643/cyber-crime/shamoon-2-saudi-arabia.html.

[40] Habboush, M., Ackerman, G. and Riley, M. (2016), 'Hack of Saudi Arabia Exposes Middle East Cybersecurity Flaws', Bloomberg Technology, 12 December 2016, www.bloomberg.com/news/articles/2016-12-12/hack-of-saudi-arabia-exposes-middle-east-cyber-security-flaws.

[41] PwC (2016), *A false sense of security? Cybersecurity in the Middle East*, Global State of Information Security Survey, March 2016, www.pwc.com/m1/en/publications/documents/middle-east-cyber-security-survey.pdf.

[42] SSN Gulf Staff (2016), 'Norton by Symantec reveals 2.5m UAE consumers hit by cybercrime in past year', *Security Systems News*, 28 November 2016, http://ssngulf.com/norton-symantec-reveals-2-5m-uae-consumers-hit-cyber-crime-past-year/.

[43] McAfee and Center for Strategic and International Studies (CSIS) (2013), *The Economic Impact of Cybercrime and Cyber Espionage*, www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

Although cybercrime's impacts vary – and can be threatening to governments and even the largest companies – it is a particular risk for small businesses and start-ups, which tend to be less resilient. These companies are crucial as the digital economy develops in the GCC, as they play a major role in creating jobs, injecting competition into the market and spurring innovation.[44] In other words, SMEs are the building blocks for a sustainable and successful digital economy.

Several GCC officials have been vocal in warning of the continuing threat of cybercrime, especially in light of its potential impact on the economy. They have made cybersecurity a priority in their security agenda, and have stressed the need for more cooperation regionally and internationally.[45] To date, the response has primarily involved increasing investment in cybersecurity technology[46] – yet as evidenced by the apparent rise in cybercrime, this has not proved sufficient to tackle the problem.

Companies in the GCC are in a similar position: they are world leaders in terms of investment in cybersecurity technology, but rank poorly on education and training in this area.[47] Anti-cybercrime measures have not been accompanied by the needed recruitment, governance and processes. As a result, the corporate sector's investment in cybersecurity has had a limited impact – indeed, to a certain extent it has created a false sense of security.[48]

The GCC's blossoming digital ecosystem and potential for further growth mean that cybercrime will only take a more serious turn in the future. Attacks on smart-city infrastructure[49] will become common. IoT devices, known for their poor security, will act as enablers for larger and more powerful attacks,[50] as seen with the recent distributed-denial-of-service (DDoS) attack that brought down the Dyn domain name system.[51]

Technology is only part of the answer. Establishing a cybersafety framework requires a multifaceted approach that involves all relevant stakeholders, as well as a comprehensive remit to build a resilient and robust ecosystem. Proposing legislative measures, developing methods and mechanisms to enforce laws, promoting the presence of an adept judiciary, and enhancing regional and international cooperation are some of the main tasks that governments need to accomplish.[52]

[44] Wiens, J. and Jackson, C. (2015), 'The Importance of Young Firms for Economic Growth', Kauffman Foundation, 13 September 2015, www.kauffman.org/what-we-do/resources/entrepreneurship-policy-digest/the-importance-of-young-firms-for-economic-growth.

[45] Al Wasmi, N. (2017), 'UAE calls for global effort against cyber crimes following WannaCry attack', *The National*, 16 May 2017, www.thenational.ae/uae/technology/uae-calls-for-global-effort-against-cyber-crimes-following-wannacry-attack; and *Al Watan* (2017), 'Major General Dr. Abdulqaddous Al-Obaidli: The Gulf states are among the safest countries in the world' [Arabic], 13 May 2017, http://alwatannews.net/article/714560.

[46] Mustafa, A. (2014), 'UAE to Double Security Budget, Focus on Cyber', *Security Assistance Monitor*, 25 February 2014, http://securityassistance.org/africa/content/uae-double-security-budget-focus-cyber.

[47] PwC (2016), *A false sense of security?*

[48] Ibid.

[49] Hardy, I. (2016), 'Are smart city transport systems vulnerable to hackers?', BBC, 5 August 2016, www.bbc.co.uk/news/business-36854293.

[50] Bryce, H. (2017), 'The Internet of Things Will Be Even More Vulnerable to Cyber Attacks', Chatham House Expert Comment, 18 May 2017, www.chathamhouse.org/expert/comment/internet-things-will-be-even-more-vulnerable-cyber-attacks.

[51] Woolf, N. (2016), 'DDoS attack that disrupted internet was largest of its kind in history, experts say', *Guardian*, 26 October 2016, www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[52] UNESCWA (2015), *Policy Recommendations on Cybersafety and Combating Cybercrime in the Arab Region*.

The role of legal and regulatory frameworks in combating cybercrime – an overview of GCC cybercrime laws

Cybercrime legislation plays an important role, at both national and international level, in preventing and combating cybercrime. Such legislation has several dimensions. First and foremost, it frames criminal conduct by defining what acts constitute offences, as well as the corresponding sanctions that apply, based on the *nullum crimen sine lege* ('no crime without law') principle.[53]

Additionally, cybercrime legislation provides a dynamic tool that governments can use to balance society's needs for security, privacy and freedom of speech.[54] Given the fast pace at which technology is developing, this policy challenge takes on a special dimension: cybercrime legislation needs to be responsive to the emerging consequences of the use of new technologies.

Cybercrime laws provide the foundations and framework for successful investigation, prosecution and adjudication of cybercrime. As cybercrime is largely a transborder crime, investigations cannot be confined to one country; laws are therefore needed to regulate interactions between states.

A comprehensive cybercrime law[55] should define its terms and the parameters of its application, criminalize specific conduct, define procedural powers, set out rules for electronic evidence, define its jurisdiction, regulate international cooperation, and outline service providers' liability and responsibility.

Table 2: Key features of GCC cybercrime laws

	Bahrain	**Kuwait**	**Oman**	**Qatar**	**Saudi Arabia**	**United Arab Emirates**
Definitions	Y	Y	Y	Y	Y	Y
Criminalization	Y	Y	Y	Y	Y	Y
Procedural powers	Y			Y		
Electronic evidence						
Jurisdiction						
International cooperation				Y		
Service provider liability and responsibility				Y		
Additional offences not foreseen in other international instruments		Y	Y	Y	Y	Y

Source: Author's own research, based on comparison of national laws.

All GCC countries have cybercrime laws in place. However, as Table 2 shows, most of these laws focus on criminalization. Moreover, they define as cybercrimes additional offences not foreseen in the main cybercrime legal instruments. They include provisions on defamation and slander,[56] the organization

[53] United Nations Office on Drugs and Crime (UNODC) (2013), *Comprehensive Study on Cybercrime,* Draft–February 2013, p. 53, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[54] Ibid.

[55] Annex 1 lists all provisions available in binding and non-binding regional and international cybercrime instruments, and compares which of these provisions are present in the Budapest Convention and Arab Convention respectively.

[56] Saudi Arabia cybercrime law Art. 3, Oman cybercrime law Art. 16, Qatar cybercrime law Art. 8, UAE cybercrime law Art. 20, Art. 30.

of marches without permission,[57] and the spreading of false news damaging to the reputation of the country.[58] Most GCC cybercrime laws have been subject to heavy criticism by human rights organizations for limiting free speech and imposing self-censorship on citizens and activists.[59] In most cases, GCC cybercrime legislation does not extend to other areas of law, such as procedural powers and international cooperation, which are central to legislation being fit for purpose.

Regional and international cooperation for fighting cybercrime – existing frameworks

International cooperation has become essential to fighting cybercrime,[60] given the transnational nature, rapid development and widening reach of such crime. Cooperation is particularly important for two reasons. First, it can help to identify the best responses to the emerging challenges presented by cybercrime. Cybercrime today is arguably more aggressive, more complex, more organized and – importantly – more unpredictable than before. When trying to combat cybercrime and mitigate its impact, governments find themselves on unfamiliar ground, facing situations that they are unable to anticipate or contain.

Countermeasures tend to have short lifespans, as the techniques and tactics of cybercriminals are developing continuously. So what might work today might not work in a month's time. The technological knowledge of cybercriminals often exceeds that of the law enforcement agencies, which makes combating cybercrime more challenging and often results in policing measures that are rudimentary in relation to the sophistication of the offences they seek to tackle. The only way forward in fighting cybercrime is thus one based on imagination, creativity and cooperation. Countries need to share information, intelligence, experiences and lessons learned in order to come up with the best ways to curb cybercrime and address its emerging challenges. Regulatory, legal and technological tools need to be developed collectively and updated on a continuous basis.

The second rationale for international cooperation is that it is needed on an operational level in cross-border investigations and prosecutions. Cybercriminals have the upper hand over law enforcement agencies because such criminals tend to operate in organized groups based in one or more jurisdictions; meanwhile their actions affect computers and victims in other jurisdictions. In contrast, law enforcement agencies such as the police and prosecution offices are confined to their own national jurisdiction; this complicates timely collection of electronic evidence and prosecution. Due to the constraints of national sovereignty, cross-border investigations have to go through formal legal channels involving state-to-state requests for assistance. This process can be lengthy and complicated, limiting the success of investigations and, more often than not, letting cybercriminals off the hook. International cooperation platforms[61] can help to address this problem and mitigate its impact. They can provide law enforcement agencies with the powers to join forces in criminal investigations, in effect removing national barriers while respecting the rule of law in

[57] UAE cybercrime law Art. 32.

[58] Qatar cybercrime law Art. 6, Art. 38

[59] See, for example, Human Rights Watch (2012), 'UAE: Cybercrimes Decree Attacks Free Speech Threatens Peaceful Activists, Ordinary Citizens Alike', 28 November 2012, www.hrw.org/news/2012/11/28/uae-cybercrimes-decree-attacks-free-speech.

[60] Hakmeh, J. (2016), 'Tackling Cybercrime: Time For the GCC to Join Global Efforts', Chatham House Expert Comment, 8 December 2016, www.chathamhouse.org/expert/comment/tackling-cybercrime-time-gcc-join-global-efforts.

[61] Such as the 24/7 Points of Contact under the Convention on Cybercrime, www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%207%20567%2024-7%20text%20ets_en.pdf.

each jurisdiction. An essential condition for these efforts is the presence of cybercrime laws that are harmonized between different countries, so as to eliminate safe havens for cybercriminals and ensure that a 'dual criminality' requirement applies.[62]

The Budapest Convention[63] is considered the most relevant international instrument for fighting cybercrime to date.[64] It allows for the harmonization of laws, supports improvement of investigation techniques, and facilitates international cooperation. Yet none of the GCC countries are parties to it or in the process of joining. Article 37 of the convention stipulates that states have to be invited to accede to the convention (see Box 1).[65] However, according to the Executive Secretary of the Committee of the Parties to the Budapest Convention on Cybercrime, accession can also be triggered through informal consultations.[66]

Box 1: Budapest Convention. Article 37 – Accession to the Convention

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Concerns about human rights protection are a particular issue for the GCC in relation to the Budapest Convention. Article 15 stipulates that the powers provided to member states must be subject to international human rights safeguards and liberties (see Box 2).[67] In this context, the additional offences that exist in most of the GCC cybercrime laws might act as an impediment to accession. This is particularly the case given that some of the laws' provisions on content-related offences are vaguely worded[68] and could constitute restrictions on human rights. According to international human rights law – specifically UN Human Rights Council Resolution 20/8 – the same level of protection should apply to the online realm as to the offline one.[69]

[62] 'Dual criminality' (also known as 'double criminality') is a requirement in the extradition law of many countries. It holds that a suspect can be extradited from one country to stand trial for breaking a second country's laws only when a similar law exists in the extraditing country.

[63] Council of Europe (2001), 'Convention on Cybercrime', 23 November 2001, www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[64] Other regional binding instruments have also addressed the issue of cooperation on cybercrime. These instruments include the Draft African Union Convention, the Commonwealth of Independent States Agreement and the Shanghai Cooperation Organization Agreement. There are also non-binding instruments dealing with the same issue, including the COMESA Draft Model Bill, the Commonwealth Model Law and the ITU/CARICOM/CTU Model Legislative Texts.

[65] Council of Europe (2001), 'Convention on Cybercrime'.

[66] Author's interview with Alexander Seger, Executive Secretary of the Committee of the Parties to the Budapest Convention on Cybercrime, Strasbourg, France, November 2016.

[67] Council of Europe (2001), 'Convention on Cybercrime'.

[68] Human Rights Watch (2015), 'Kuwait: Cybercrime Law a Blow to Free Speech', 22 July 2015, www.hrw.org/news/2015/07/22/kuwait-cybercrime-law-blow-free-speech.

[69] UN Human Rights Council Resolution 20/8 on 'the promotion, protection and enjoyment of human rights on the internet', 2012, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement.

Box 2: Budapest Convention. Article 15 – Conditions and safeguards

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

While the Budapest Convention has a substantial international membership,[70] several big countries – including Russia, India, Brazil and China – have not joined it. Their main argument for not joining the convention relates to the fact that they did not participate in its negotiation. While this might appear to limit their role in further development of the convention, that is not necessarily the case: for example, India has joined other Council of Europe conventions – on international cooperation in tax matters, and on the transfer of sentenced persons – without having participated in the negotiation of either of those agreements. Another argument used by countries that have resisted accession is that Article 32(b) of the convention allows for a party to gain transborder access to data without authorization from another party, which would violate the state's sovereignty.[71] In 2014, the Cybercrime Convention Committee issued a guidance note on Article 32(b)[72] limiting its scope and correcting misunderstandings regarding transborder data access under the convention.

Although the GCC is not party to any global anti-cybercrime agreement, a cooperation framework of sorts exists at the regional level in the form of the Arab Convention on Combating Information Technology Offences (the 'Arab Convention').[73] This League of Arab States instrument was enacted in 2010 with the aim of enhancing cooperation between Arab countries 'to combat information technology offences threatening their security, interests and the safety of their communities' and enabling parties to 'adopt a common criminal policy aimed at protecting the Arab society against information technology offences'.[74]

While the convention has been criticized for its vaguely worded provisions, without adequate definitions,[75] its provisions are in fact almost the same as those of the Budapest Convention, especially in relation to procedural powers and international cooperation, the two main elements absent from most GCC cybercrime laws (see Annex 1 for more details).

[70] Council of Europe (2017), 'Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime, Status as of 08/06/2017', 8 June 2017, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=LeuugkuJ.
[71] Council of Europe (2001), 'Convention on Cybercrime'.
[72] Council of Europe (2014), 'T-CY Guidance Note #3, Transborder access to data (Article 32)', 3 December 2014, https://rm.coe.int/16802e726a.
[73] Arab Convention on Combating Information Technology Offences, 2010. English copy available at http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences.
[74] Ibid.
[75] 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.

The Arab Convention has been signed by 18 Arab countries, including all six GCC members. It has not been ratified by Saudi Arabia, however.[76] Indeed despite wide acceptance, the convention has not been formally activated and coordination between state parties to it remains ineffective.[77] There is no reference to its provisions in any of the GCC cybercrime laws. While Chapter V Article (1) of the convention stipulates that 'competent authorities in State Parties shall take the domestic procedures necessary to implement this convention',[78] this step has not yet occurred.

As things stand, intra-GCC cooperation on combating cybercrime therefore relies on bilateral relationships and informal channels, such as police-to-police or agency-to-agency cooperation. While these mechanisms are useful, they are insufficient for an effective regime: they place limitations on investigative actions, lack a common approach, and have to operate within multiple law enforcement networks. Informal mechanisms normally serve as a precursor to formal requests for Mutual Legal Assistance Treaties[79] (MLATs), which are 'agreements between governments that facilitate the exchange of information relevant to an investigation happening in at least one of those countries'.[80] However, the nature and frequency of cybercrime, as well as the nature of evidence, make informal channels inadequate for dealing with cybercrime investigations. They do not guarantee the required speed of response,[81] nor do they provide the required interstate alignment of priorities.

Evidently, the GCC needs to explore further options for fostering regional and international cooperation. In doing so, it should look at what is feasible and practical. One possible course of action could be to explore channels for activating the Arab Convention, which provides a useful platform for judicial cooperation and has at least been signed by all GCC countries. Another possibility would be for GCC countries to seek observer status within the Budapest Convention in order to learn about the convention and determine whether, and how, they might accede to it. Alternatively, GCC states could rely on the United Nations Convention against Transnational Organized Crime (UNTOC),[82] as they have all ratified this convention and as it provides broad scope for international cooperation – which could in some cases establish a platform for international cooperation in fighting cybercrime.

Conclusion

Most GCC countries have ambitious plans[83] to diversify their economies for the post-oil era. Initiatives include investing in the digital economy and smart infrastructure, with a strong emphasis on private-sector involvement and development of human capital. While the region's full digital potential

[76] State parties to the Arab Convention on Combating Information Technology Offences [in Arabic], available at www.lasportal.org/ar/legalnetwork/Documents/%D8%A7%D9%84%D8%AA%D8%B5%D8%AF%D9%8A%D9%82%20%D8%B9%D9%84%D9%89%20%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A9%20%D8%A7%D9%84-%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%20%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9%20%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%AA%D9%82%D9%86%D9%8A%D8%A9%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf. Bahrain ratified the convention in January 2017. See Legislation and Legal Opinion Commission (2017), 'Law No. (2) of 2017 on the ratification of the Arab Convention on Combating Information Technology Offences' [in Arabic], 26 January 2017, www.legalaffairs.gov.bh/Media/LegalPDF/K0217.pdf.

[77] UNESCWA (2015), *Policy Recommendations on Cybersafety and Combating Cybercrime in the Arab Region*, p. 8.

[78] Arab Convention on Combating Information Technology Offences, 2010. English copy available at http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences.

[79] UNODC (2013), *Comprehensive Study on Cybercrime*, Draft–February 2013.

[80] More on MLATs available at https://mlat.info/.

[81] Commission on Enhancing National Cybersecurity (2016), *Report on securing and growing the digital economy*, www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

[82] UNODC (undated), 'United Nations Convention against Transnational Organized Crime and the Protocols Thereto', www.unodc.org/unodc/treaties/CTOC/. However, UNTOC is limited in how much it can be used against cybercrime, as it is not a cybercrime convention and does not include specific provisions such as ones relating to the preservation of data or evidence.

[83] Ministry of Cabinet Affairs (undated), 'The UAE Vision 2021 National Agenda aims for the UAE to be the safest place in the world', Vision 2021, www.vision2021.ae/en/national-priority-areas/safe-public-and-fair-judiciary.

has not yet been reached, a number of GCC countries have had breakthroughs in development of digital services and innovation, to the point that they can match the levels of the most advanced countries in some areas. The region's potential for further digital transformation is significant, indicating that the GCC could become a leading international player in the digital sphere.

However, achieving this potential is contingent on the region meeting numerous challenges, two of the most important of which are to ensure cybersecurity and fight growing cybercrime. A holistic approach is required that puts cybercrime legal frameworks at the centre of cooperation between states and national stakeholders. Failure to establish such a basis for cooperation could have repercussions that threaten the viability and sustainability of the digital economy that the region has developed to date.

There is increased recognition in the GCC of the importance of international cooperation in addressing the risks from cybercrimes that transcend national borders. There is also a consensus on the need for stronger cooperation mechanisms at national, regional and international level. Most GCC cybercrime laws do not provide an adequate legal framework for cooperation, nor do they include clear procedural provisions for implementation. In this sense, they are not fit for purpose. An overhaul of laws that addresses these gaps is needed.

Cybercrime laws constitute one category of a broader cyber legislation framework[84] that will require constant upgrading by GCC governments if ICT is to be regulated in a way that fosters, rather than hampers, development and growth.

At the current stage of the region's digital development, GCC governments have a unique opportunity to capitalize on the success achieved so far and to set solid foundations for a sustainable and resilient digital economy.

[84] According to UNESCWA, 'Cyber legislation can be categorized under the following four topics: laws aimed at protecting users by safeguarding privacy, personal data and user rights; criminal legislation on the misuse of cyberspace; laws to protect intellectual property rights regarding products, programmes and information posted on the Internet, in accordance with country specificities and innovation stimulation; and laws aimed at regulating administrative and commercial transactions.' UNESCWA (2013), 'Policy Note: Development and Harmonization of Cyber Legislation in the Arab Region', http://unctad.org/meetings/en/Contribution/CIIEM5_ESCWA2_en.pdf.

Annex 1: Budapest Convention vs Arab Convention on Combating Information Technology Offences[85]

Exhaustive list of provisions available in all binding and non-binding regional and international cybercrime instruments	Budapest Convention + Optional Protocol	Arab Convention on Combating Information Technology Offences
Definitions		
Computer/information system	Art. 1(a)	Arts 2(1), 2(5)
Computer/information network	–	Art. 2(6)
Device/storage media	–	–
Critical infrastructure	–	–
Computer data/information (including computer program)	Art. 1(b)	Arts 2(3), 2(4)
Electronic record	–	–
Subscriber/traffic/content data/information	Arts 1(d), 18	Art. 2(9)
Electronic communication/mail	–	–
Malware/malicious software	–	–
(Internet) service provider	Art. 1(c)	Art. 2(2)
Child/minor	Art. 9(3)	–
Cybercrime/computer crime	–	–
Criminalization		
Illegal access to a computer system	Art. 2	Art. 6
Illegal access, interception or acquisition of computer data	Arts 2, 3	Arts 6, 7, 18
Illegal interference with computer data	Art. 4	Art. 8
Illegal interference with a computer system	Art. 5	Art. 6
Computer misuse tools	Art. 6	Art. 9
Breach of privacy or data protection measures	–	–
Computer-related forgery	Art. 7	Arts 10, 8
Computer-related fraud	Art. 8	Art. 11
Offences involving electronic payment tools	–	Art. 18
Identity-related crime	–	–
Computer-related copyright and trademark offences	Art. 10	Art. 17
Spam	–	–
Computer-related harassment, extortion or acts causing personal harm	–	–
Computer-related acts involving racism or xenophobia	Arts 3,4, 5 (OP)	–
Computer-related denial or justification of genocide or crimes against humanity	Art. 6 (OP)	–
Computer-related production, distribution or possession of child pornography	Art. 9	Art. 12
Computer-related solicitation or 'grooming' of children	–	–
Computer-related acts in support of terrorism	–	Art. 15
Computer-related offences involving money-laundering	–	Art. 15
Computer-related offences involving illicit trafficking	–	Art. 16
Computer-related offences against public order, morality or security	–	Arts 12, 13, 14, 15

[85] For the full list of articles of other international and regional instruments, refer to Annex 3 of UNODC (2013), *Comprehensive Study on Cybercrime*, Draft–February 2013.

Exhaustive list of provisions available in all binding and non-binding regional and international cybercrime instruments	**Budapest Convention + Optional Protocol**	**Arab Convention on Combating Information Technology Offences**
Law enforcement investigation-related offences	Arts 16(3), 20(3), 21(3)	Arts 23(3), 28(3), 29(3)
Aggravating circumstances for conventional crime committed by means of a computer system	–	Art. 21
Attempt and aiding or abetting	Arts 11, 7(OP)	–
Corporate liability	Art. 12	–
Procedural powers		
Search for computer hardware or data	Arts 19(1), 19(2)	Art. 26
Seizure of computer hardware or data	Art. 19(3)	Art. 27(1)
Order for stored computer data	Art. 18(1)(a)	Art. 25 (1)
Order for subscriber information	Art. 18(1)(b)	Art. 25(2)
Order for stored traffic data	Art. 17(1)(b)	Art. 24
Real-time collection of traffic data	Art. 20	Art. 28
Real-time collection of content data	Art. 21	Art. 29
Expedited preservation of computer data	Arts 16, 17(1)(a)	Art. 23(2)
Use of (remote) forensic tools	–	–
Transborder access to computer data	Art. 32(b)	Art. 40(2)
Provision of assistance	Art. 19(4)	Art. 27(2)
Retention of computer data	–	–
Electronic evidence		
Admissibility of electronic evidence/records	–	–
Admissibility of electronic signature	–	–
Burden of proving authenticity	–	–
Best evidence rule	–	–
Print-outs as best evidence	–	–
Presumption of integrity	–	–
Evidence on recording/preservation standards	–	–
Electronic evidence/records from other countries and foreign documents	–	–
Jurisdiction		
Territorial principle	Art. 22(1)(a)	Art. 30(1)(a)
Using a computer system/data located within the territory	–	–
Directed against a computer system/data located within the territory	–	–
Nationality principle (offender)	Art. 22(1)(d)	Art. 30(1)(d)
Nationality principle (victim)	–	–
Habitual residence principle	–	–
Legal person – incorporation principle	–	–
States interests principle	–	Art. 30(1)(e)
Jurisdiction when extradition refused	Art. 22(3)	Art. 30(2)
Ships and aircraft	Art. 22(1)(b)(c)	Art. 30(1)(b)(c)
Dual criminality	Art. 22(1)(d)	Art. 30(1)(d)
Concurrent jurisdiction	Art. 22(5)	Art. 30(3)
Establishment of place of offence	–	–

Exhaustive list of provisions available in all binding and non-binding regional and international cybercrime instruments	**Budapest Convention + Optional Protocol**	**Arab Convention on Combating Information Technology Offences**
International cooperation		
General principle of international cooperation	Art. 23	–
Extradition for instrument offences	Art. 24	Art. 31
General mutual legal assistance	Arts 25, 27	Arts 32, 34
Mechanism for expedited assistance	Art. 25(3)	Art. 32(3)
Assistance – preservation of computer data	Art. 29	Art. 37
Assistance – seizure/access to/collection of/disclosure of computer data	Arts 30, 31, 34	Arts 38, 39, 41, 42
Transborder access to computer data	Art. 32(b)	Art. 40(2)
Provision of unsolicited information/exchange of information	Art. 26	Art. 33
Confidentiality of request	Art. 28	Art. 36
Dual criminality	Arts 24(1), 25(5)	Arts 32(5), 37(3), 37(4)
Establishment of point of contact or 24/7 network	Art. 35	Art. 43
Service provider liability and responsibility		
Monitoring obligations	–	–
Voluntary supply of information	–	–
Take-down notifications	–	–
Liability of access providers	–	–
Liability of caching providers	–	–
Liability of hosting providers	–	–
Liability of hyperlink providers/search engines	–	–

Source: UNODC (2013), *Comprehensive Study on Cybercrime*, Draft–February 2013.

About the author

Joyce Hakmeh is an Academy Fellow, hosted by the Chatham House International Security Department. She is a legal and development expert working on the Middle East and North Africa region since 2006. Her areas of expertise include cybercrime, rule of law, good governance, international criminal justice and international aid.

Her research at Chatham House focuses on cybercrime legislation in the Gulf countries and their impact on the economy, security and freedoms. Prior to this position, Joyce worked for different organizations including the United Nations Development Programme, the International Federation of Red Cross and Red Crescent Societies, and the Special Tribunal for Lebanon, as well as for NGOs and media organizations. Additionally, Joyce acted as ambassador for the European Commission's initiative on reforming aid mechanisms and advised the Lebanese prime minister's office on cooperation and outreach. In 2015, Joyce led an initiative on fighting cybercrime with the Lebanese Investigation Commission as well as with the cybercrime bureau of the Lebanese police.

Joyce is a Chevening Scholar and received her master's in international law from SOAS, University of London.

Joyce's fellowship is supported by the Asfari Foundation.

Acknowledgments

This paper would have not been possible without the support of the International Security Department at Chatham House and the Queen Elizabeth II Academy for Leadership in International Affairs at Chatham House. Much gratitude goes to Patricia Lewis, Hannah Bryce and Emily Taylor for insightful feedback and comments; to Henry Dodd for his exceptional support throughout the project; and to Jake Statham for editing the paper.

The author would also like to thank the Mohammed Bin Rashid School of Government for its input and the Asfari Foundation for its generous support and sponsorship. Finally, the author would like to thank the Ministry of Foreign Affairs of the Netherlands and the UK Cabinet Office for providing funding support for the project under which this paper was drafted.

Independent thinking since 1920

Chatham House, the Royal Institute of International Affairs, is an independent policy institute based in London. Our mission is to help build a sustainably secure, prosperous and just world.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

Cover image: View of Dubai.

Photo credit: Copyright © Edward Tian/Contributor/Getty

ISBN 978 1 78413 235 4

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