International Security Department
Workshop Summary

CHATHAM HOUSE
The Royal Institute of International Affairs

# Cybercrime and the Digital Economy in the GCC Countries

26 March 2017

كلية محمد بن راشد للإدارة الحكومية
MOHAMMED BIN RASHID SCHOOL OF GOVERNMENT



10 St James's Square, London SW1Y 4LE T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
www.chathamhouse.org
Patron: Her Majesty The Queen Chairman: Stuart Popham QC Director: Dr Robin Niblett Charity Registration Number: 208223

## Introduction

This document summarizes the discussions that took place during the 'Cybercrime and the Digital Economy in the GCC Countries' workshop on 26 March 2017 in Dubai, UAE. The workshop was co-hosted by the International Security Department at Chatham House and the Mohammed Bin Rashid School of Government (MBRSG). Participants included regional and international academics, researchers, practitioners and government experts.

The workshop assessed cybercrime legislation in the Gulf Cooperation Council (GCC) countries, and the impact of such legislation on the digital economy. It aimed to draw conclusions and recommendations on how to enhance legal frameworks in the region in order to effectively fight cybercrime and mitigate its impact on digital infrastructure and economic prosperity.

## Context

The GCC has seen a steady increase in cybercrime. In spite of heavy investment in cyber protection and the adoption of different measures – including legislative instruments – cybercrime rates continue to rise. This escalating situation constitutes a threat not only in terms of financial losses, but also in terms of the wider impact on a growing digital economy and the exposure to cyber vulnerabilities in the smart infrastructure that the region is trying to pioneer. From a legal perspective, having cybercrime laws to which everyone adheres, and which are in line with international norms and standards, is vital for a safe, trustworthy and secure internet able to drive economic prosperity. Increasing cybercrime rates show that the current approaches and existing legal frameworks are not fully serving their purpose. One possible explanation could be the dynamism of a technological environment that requires constant assessment and improvement of cybercrime prevention, preparation, response and recovery measures – including of cybercrime laws. Another reason could be related to the substance of these laws and how cybercrime is being defined.

No matter how the situation is interpreted, what is undisputed is that the GCC countries need to revisit their counter-cybercrime strategies if they want to sustain GDP growth rates and develop their full potential as digital economies.

## Session 1: The digital economy in the GCC – facts, figures and progress

The first session of the workshop sought to address the following questions:

1. How can the GCC overcome existing challenges to further digital transformation of society and the economy?
2. What steps are required to transform GCC countries from being consumers of digital content and products to creators of digital content and products?

Technological innovations are helping governments and cities become 'smarter' and more resource-efficient while enhancing sustainability and quality of life. Data are fuelling this transformation. Unlocking the potential of data obtainable from the Internet of Things (IoT), social media and other sources will help cities move from being net consumers of digital content and products to being producers and digital innovators. While harnessing data-driven technological transformations can propel innovation and advancement, it can also help solve classic governance challenges: for example, by making government data available to society and businesses, and by leveraging the ever-increasing applications of big data and artificial intelligence.

These transformations could enable the GCC to become a creator of digital content, fuelling the knowledge economy across the region. The 'Smart Dubai' model exemplifies this. This digital transformation initiative is creating the organizational and legal infrastructure to boost innovation within government and society, and is enhancing quality of life for residents and visitors. For example, 'Dubai Data' is a citywide data sharing initiative (for services and infrastructure) that generates public value. Enabled by the Dubai Data Law of 2015, the initiative is managed by the Dubai Data Establishment, which is the official body responsible for the dissemination and exchange of data in Dubai. The aim of the initiative is to open, curate and share the city's data, based on key data obligations set for all branches of the government.

While the Smart Dubai model is setting the norm in the GCC, ongoing digital transformation and technological advancement have affected the region as a whole. For example, even though eight out of 10 people in the UAE have a smartphone, the Middle East's digital potential is lagging behind that of Europe and the US – if the region could achieve American levels of digital technology penetration, its GDP would increase considerably. This would require more innovation and could be achieved through collaborative problem-solving and public–private partnerships. In this model, government can serve as the enabling platform, driving innovation and nurturing the market by leading the push on digital transformation. The GCC governments are uniquely positioned for this role, and can provide the scaled solutions required for value creation.

There is a debate as to whether the legal framework is hindering or encouraging digital transformation, as the lack of data protection laws facilitates responsiveness and innovation in some respects but also creates vulnerabilities to cybercrime. An environment conducive to growth needs flexibility, collaboration, constant capacity-building and increasing engagement from all stakeholders. However, in the absence of data privacy laws in the region in general, individuals need to be educated as to what data should be shared in different environments. It was determined that this dynamic nature of 'privacy' makes legislation on data protection difficult, but that more research is needed in this area.

More interventionist frameworks were called for, with a focus on encouraging innovation and entrepreneurship in digital sectors while avoiding over-regulation. One possible solution is a GCC-wide data legislation framework that establishes close relationships between governments and business, reviews insolvency laws, and builds on existing structures to determine the best ways to encourage digital innovation without infringing on individual privacy.

## Session 2: Cybercrime in the GCC countries – trends, economic impact and current countermeasures

The second session sought to address the following questions:

1. Are cybercrime statistics accurate? How can statistical reporting be improved to better tackle cybercrime?
2. How advanced and comprehensive are the cybersafety frameworks in the GCC countries?
3. What are the new risks associated with the emergence of smart infrastructure and the IoT in the GCC? How vulnerable might the GCC be?

The issue of cybercrime proved difficult to tackle due to diverging definitions, its shifting nature, and complexities relating to investigation and prosecution. Some define 'cybercrime' as a crime carried out using technological tools; for others, it extends to crimes that include an electronic aspect. This is a particular issue in the GCC, where defamation, slander and other content-related offences are all

considered cybercrimes. In the region as a whole, there is confusion as to how cybercrime laws are defined and used, given different attitudes on what constitutes a crime. As such, approaches to e-investigation necessarily vary: they need to be chosen on the basis of the relevant legislation and according to the nature of the crime.

In Dubai, for example, investigations cover four general categories of cybercrime: crimes of honour/reputation; crimes involving fraud; financial crimes; and privacy crimes. In all four categories, international and local cooperation would be required to make the investigation processes more efficient. Local law enforcement agencies could be granted the authority to gather information more freely. It would also be useful to raise public awareness of cyber risk in order to facilitate information-gathering and encourage reporting of cybercrimes.

Combating cybercrime is challenging given the nature of such offences. Laws and technology need to be updated as the often unpredictable nature of cybercrime evolves. The virtual and sometimes fleeting nature of electronic evidence poses special challenges for evidence-gathering, and agility is required in order to catch perpetrators of cybercrime. While some intergovernmental cooperation on this already occurs in the GCC, such activity is mostly bilateral and more effort is still required.

There is the additional challenge of raising awareness in groups most vulnerable to ransomware – i.e. the elderly and student populations. Raising awareness of cybercrime at the individual level is critical, as it empowers citizens to protect themselves. Awareness campaigns will help educate these groups about the threats of cyber blackmail, online gossip and fraud. The necessity of such campaigns is heightened by the increased use of social media to commit crimes.

Challenges also remain in terms of identifying the perpetrators of cybercrime and the nature of offences being committed. Analysis of a wide range of data offences is required to better understand the threat, particularly as the information gathered thus far indicates a lack of systematic research in this area. This is especially concerning given the growing vulnerabilities in IoT implementations, which provide potential routes for cyberattacks and which could become key sources of risk to ‘smart city’ infrastructure.

There is a need to understand and carefully analyse the information provided on cybercrime, as it comes from varying and often incompatible sources. While cybercrime statistics include significant information on fraud, online bullying and electronic harassment, concerns about their accuracy persist. The data can, nonetheless, serve to alert citizens to the need to improve online safety. That said, the statistics show a 24 per cent increase in phishing and fraud in the GCC in 2016, compared with the previous year.

Most government entities fighting cybercrime in the GCC work by balancing ‘offensive’ and ‘defensive’ strategies. The ability to collect and analyse all forms of data is central to the authorities’ anti-cybercrime capabilities. Governments must couple their technological dependency with data protection, and the question of securing, sharing and/or using data is critical. Are over-prescriptive data protection laws helpful, particularly in the GCC region? In some cases, such as in the e-commerce sector, legal frameworks are hindering economic growth, participants noted. In another context, there was a view that laws do not go far enough and that governments struggle to manage and share data across different environments. Laws provide one instrument for balancing openness with protection, but more innovative approaches are needed.

Standardization of security standards was seen as relatively easy within the public sector, due to the presence of common or similar standards, but more difficult for the private sector. Private companies may be unwilling to disclose weaknesses in their information systems, or potentially do not know when they

have been victims of cybercrime. In contrast, government agencies can cooperate with other governments on security measures not available to the private sector or individuals.

Despite the differing needs and requirements of public-sector and private-sector organizations, there was concern about the implications of a lack of common security standards. The problem is compounded by the fact that fighting cybercrime requires different forms of data to be collected from different agencies. However, most workshop participants agreed that strengthening public–private partnerships will be key to fighting cybercrime threats.

Finally, it was observed that interstate cooperation in the GCC is poor, as the region's governments have weak collaborative processes. Participants also discussed instances of cooperation between the US and Dubai in a highly successful e-investigation, which indicated the usefulness of international cooperation in tackling cybercrime.

## Session 3: The role of legal and regulatory frameworks in combating cybercrime

The third session sought to address the following questions:

1. Are the national cybercrime laws enacted thus far in the GCC countries fit for purpose?
2. How are these laws affecting cybersecurity and economic prosperity in these countries?

A comprehensive cybercrime law needs to define its terms and the parameters of its application, criminalize conduct considered as a cybercrime, define procedural powers, set out the rules for electronic evidence, define the jurisdiction, regulate international cooperation, and outline service providers' liability and responsibility.

The absence of procedural provisions in most GCC cybercrime laws, combined with a loose adherence to general procedural law, forces entities to adapt their methodology. Cybercrime is constantly evolving, so regular reviews of laws are seen as a minimum requirement. Some participants argued that establishing proper policies, rather than laws, was preferable; they saw laws as difficult to manage, whereas policies provide more flexibility to adapt.

National governmental standards regarding cybersecurity are limited within the GCC, but international standards exist. For example, government departments in the UAE are audited to determine their compliance with international information security standards; training is provided when departments fall short of these standards.

The Bahraini cybercrime law is an example of the application of international standards. The law is modelled on the Budapest Convention; Bahrain's decision to base a domestic law on this framework reflected recognition of the international expertise involved in the convention's development, its adequate procedural provisions, and its process for judicial cooperation. The Bahraini cybercrime law does not refer to content-related offences that exist in the Bahraini Penal Code, and as such it departs from the practice of the other GCC countries in that aspect. The law makes some actions, such as interference with public infrastructure, aggravated criminal offences that incur substantial penalties.

The Bahraini cybercrime law was extended by parliament beyond the remit originally recommended by the authors of the law – for example, provisions against child pornography have been widened to include all pornography. Similarly, the Qatari cybercrime law sought to use the Budapest Convention as a model,

but the entire law was redrafted after circulation within the government. The workshop discussions revealed weak coordination between those drafting cybercrime laws and those enforcing them.

Additionally, despite the fact that all GCC countries are signatories to the Arab Convention on Combating Information Technology Offences, none of the GCC states refer to it in their cybercrime laws. The fact that the convention provides a legal framework for cooperation and includes procedural provisions, which most GCC countries do have in their cybercrime laws, means that the convention could cover this gap. This is an area for further development.

While GCC nations have developed informal, robust and flexible methods for preservation of evidence, these methods do not have the force of law behind them. It is thus important to ensure that political will exists in support of robust enforcement. With the absence of comprehensive laws, committees are being established to suggest further legislation on cybercrime, add necessary amendments to laws, and supplement appropriate practices. In the future, intergovernmental cooperation will be needed to address all the gaps that committees have identified in the regulatory framework on cybercrime.

## Session 4: Regional and international cooperation for fighting cybercrime

The fourth session sought to address the following questions:

1. What are the existing frameworks for cooperation against cybercrime?
2. What channels for international cooperation are available to the GCC?
3. What benefits would GCC countries get from acceding to the relevant international instruments for fighting cybercrime? How can these be operationalized?

International cooperation to combat cybercrime is increasingly important. Cybercrime is damaging to the global economy, with complex cybercriminal networks committing crimes on an unprecedented scale. The transnational dimension of cybercrime requires transnational investigations, involving agile and structured cooperation between national law enforcement agencies. Traditional crimes are also evolving as cybercrime opportunities proliferate, and are thus becoming more widespread and damaging themselves. In an increasingly networked world, international cooperation is essential for creating resiliency against cybercrime. In short, no one can afford to fight cybercrime alone.

The current model of cooperation in the GCC includes a binding instrument (Arab Convention on Combating Information Technology Offences), non-binding instruments (the GCC strategy on fighting cybercrime – principle 5 on international cooperation), and informal cooperation (police-to-police cooperation and agency-to-agency cooperation). Most GCC countries still rely on informal channels. While these mechanisms are useful, they have limitations in terms of the investigative actions that can be carried out under such arrangements. Other challenges include the lack of a common approach among agencies, and the existence of multiple law enforcement networks. The use of formal channels of international cooperation such as extradition and mutual legal assistance treaties (MLATs), on the other hand, can make obtaining evidence in a cybercrime investigation too time-consuming. A UN survey shows a median response time of 120 days for extradition requests, and 150 days for MLA requests received and sent by the countries included in that survey.

'Operation Avalanche' – an internationally coordinated four-year operation between police in 30 countries and agencies such as the FBI, Europol and Eurojust, which succeeded in dismantling a global cybercriminal network – illustrates the importance of international cooperation in the investigation of a transnational crime. It serves as the first example of a successful international collaborative effort to

combat cybercrime. Moreover, it demonstrates the importance of cross-sector cooperation. Private-sector and individual stakeholders were important in dismantling the Avalanche network, as they allowed law enforcement to speak to representatives from governments and offered subject matter expertise during the investigation.

As there is currently little cooperation in fighting cybercrime within the region, many workshop participants stressed the need for regional and international initiatives. The Budapest Convention is attractive to the GCC, as the convention provides a legal platform for continuous cooperation and the option to develop new protocols in real time in response to emerging threats. However, to join the convention a country needs to have appropriate legislation in place – including legislation safeguarding human rights, as outlined in Article 15 of the convention. Additionally, states have to be invited to accede to the convention, although accession can be triggered through informal consultations before an official invitation.

The existence of the Budapest Convention provides the necessary framework for international cooperation. Bahrain's cybercrime law, incidentally, does not provide for international cooperation because its drafters believed that this would be achieved through accession to the Budapest Convention. The idea was that Bahrain could subsequently use the convention's provisions for international cooperation. However, none of the GCC states is an observer or state party to the convention yet.

Participants then discussed whether international information sharing is practical for the GCC, and, if not, whether a viable alternative exists. One speaker pointed out that there is a difference between information sharing and formal MLA. The latter necessitates an agreement over aspects of cybercrime that is currently not in place: anti-harassment laws and free-speech protections, for example, have different standards and definitions in the GCC than under the international standards. This means that what constitutes a cybercrime in the GCC is not necessarily a cybercrime elsewhere. The Budapest Convention would be useful for the GCC in this regard, as it creates laws in harmony and establishes 'double criminality', allowing a perpetrator to be prosecuted and extradited in more than one jurisdiction.

The GCC needs to explore options for fostering international cooperation on fighting cybercrime. In doing so, it should look both at what is feasible and at what is practical. One possible course of action could include each of the GCC countries adopting observer status in the Budapest Convention, in order to learn about the convention and determine if, and how, they should accede to it. Additionally, channels for activating the Arab Convention on Combating Information Technology Offences should be explored, as the convention provides a useful platform for judicial cooperation, and as it has been signed by all GCC countries and ratified by all of them except Saudi Arabia. This convention is in place, but has not been implemented and used despite its potential utility in establishing a basis for GCC cooperation.

Additionally, all GCC states are parties to the UN Convention Against Transnational Organized Crime (UNTOC), and could utilize the extensive international cooperation provision of this treaty in cross-border cybercrime investigations. However, this is not a cybercrime convention and has limitations such as the absence of provisions relating to the preservation of data or evidence.

Finally, it is important to establish international cooperation in order to share information and speed up decision-making. It is unhelpful to focus on the difficulties in adhering to international instruments related to cybercrime; rather, exploratory talks regarding how GCC states can work towards enhancing cooperation should be taking place.