Economic and Social Commission for Western Asia

UNITED NATIONS
الاسكوا
ESCWA

# Policy Recommendations on Cybersafety and Combating Cybercrime in the Arab Region

Summary

ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (ESCWA)

# POLICY RECOMMENDATIONS ON CYBERSAFETY AND COMBATING CYBERCRIME IN THE ARAB REGION

## SUMMARY

United Nations

Distr.
LIMITED
E/ESCWA/TDD/2015/1/Summary
14 April 2015
ORIGINAL: ENGLISH

**ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (ESCWA)**

# POLICY RECOMMENDATIONS ON CYBERSAFETY AND COMBATING CYBERCRIME IN THE ARAB REGION

## SUMMARY

United Nations
New York, 2015

## Acknowledgements

The Innovation Section of the Technology for Development Division of the Economic and Social Commission for Western Asia (ESCWA) has designed and coordinated the preparation of the present summary report under the administration and supervision of Ms. Nibal Idlebi, Chief of the Innovation Section, and in collaboration with Ms. Hania Dimassi, Research Assistant, and Ms. Lize Denner, Associate Information Technology Officer.

The present summary report is based on a technical paper prepared by Mr. Wassim Hajjar, a judge and expert in the field of legal informatics and computer engineering. Mr. Imad Sabouni, former Minister of Communications and Technology of the Syrian Arab Republic and an expert in information and communication technology policies and strategies, carried out an substantive review of the present summary report.

A peer review was conducted by ESCWA experts and Mr. Youssef Nusseir, an expert in policies and strategies of the information society, and Ms. Jeanane Khoury, Chief of Legal Department at Juridical and Informatics Centre in Lebanese University.

The present summary report was prepared as part of the continued efforts of the ESCWA Technology for Development Division, headed by Mr. Haidar Fraihat, to develop an information society in the Arab region. It complements ESCWA efforts aimed at developing and harmonizing cyber legislation to establish a knowledge society in the Arab region, focusing on the organizational and procedural frameworks to combat cybercrime and ensure cybersafety.

ESCWA would like to thank member States for their cooperation in completing the questionnaire for the present summary report.

ESCWA welcomes reader’s comments and observations via email on the following address: escwa-tdd@un.org.

# CONTENTS

*Page*

Executive summary ........................................ vi
Introduction ........................................ 1

*Chapter*

I. GLOBAL TRENDS IN COMBATING CYBERCRIME AND ENSURING CYBERSAFETY ........................................ 2

A. Overview of international efforts ........................................ 2

B. Legislative trends........................................ 3

C. Trends related to the application of laws and regulations ........................................ 3

D. Trends of cooperation between states........................................ 4

E. Other technological and administrative trends: collaboration with the private sector ........................................ 4

F. Awareness-raising and training trends ........................................ 5

II. REGIONAL CHALLENGES IN THE AREA OF CYBERSAFETY AND COMBATING CYBERCRIME........................................ 5

A. Cybercrime challenges and specificities in the arab region........................................ 5
B. Strategic challenges in the Arab region ........................................ 6
C. Cyberspace legislative challenges in the Arab region ........................................ 6
D. Challenges of law enforcement in the Arab region ........................................ 7
E. CERTs in the Arab region ........................................ 8
F. Regional coordination and cooperation between Arab countries ........................................ 8
G. Challenges faced by the private sector in the Arab region ........................................ 9
H. Challenges related to culture and cybersafety awareness in the Arab region............... 9

III. FRAMEWORK FOR ENSURING CYBERSAFETY AND COMBATING CYBERCRIME IN THE ARAB REGION........................................ 11

A. Developing national strategies to ensure cybersafety and combat cybercrime ............ 11
B. Proposed legislation to ensure cybersafety in the Arab region........................................ 11
C. Legislation enforcement means and bodies........................................ 12
D. Awareness-raising, education and training methods ........................................ 12
E. Cooperation between the public and private sectors ........................................ 13
F. Cooperation between Arab countries to enhance cybersafety ........................................ 14

## Executive summary

Information and communication technology has become a fundamental tool, used daily in most sectors and economic activities, which contributes to economic and social development. Technological advances, such as the wide availability and affordability of Internet services and broadband services on mobile devices, have led to a rise in Internet users. In 2014, 40 per cent of people in the Arab region had Internet access and 24 per cent used broadband services on their mobile devices, compared to a global average of 32 per cent.[1] However, the openness of the Internet, and cyberspace in general, has made it susceptible to abuse and users (individuals, enterprises, government institutions and organizations) are vulnerable to attacks by criminals and hackers. This underscores the need for concerted efforts at all levels to ensure cybersafety and limit electronic threats.

Joint efforts between sectors and stakeholders, and regional and international cooperation are key to combating cybercrime because of the global nature of cyberthreats. Several problems arise when perpetrators, victims and systems are in different countries; in addition to difficulties caused by cross-border virtual and physical elements, highlighting the complexity of tackling cyberthreats. In 2013, an estimated 556 million people were victims of cybercrime, equivalent to 1.5 million a day; resulting losses have been estimated at $110 billion.[2]

The present summary report complements efforts by the Economic and Social Commission for Western Asia (ESCWA), initiated in 2007, to develop and harmonize cyber legislation in the Arab region and implement it in practice. ESCWA, under the project entitled “Regional harmonization of cyber legislation to promote the knowledge society in the Arab world”, has prepared the ESCWA Cyber Legislation Directives[3] that contain model cyber legislation texts that Arab States can benefit from and adapt when drafting national legislation. Ten Arab States have used the Directives to update and develop their cyber legislation, in collaboration with ESCWA. The present summary report, entitled “Policy recommendations on cybersafety and combating cybercrime in the Arab region”, analyses the current situation at the regional and international levels, sets out methods to strengthen and coordinate efforts to combat cybercrime and ensure cybersafety and proposes a policy framework for enhancing cybersafety in the Arab region.

The full study in Arabic[4] and the present summary report review global trends in combating cybercrime and ensuring cybersafety, focusing on law enactment, implementation and coordination between countries in developed regions. It also highlights the role of policymaking at the international level in promoting cybersafety, and of public and private institutions in developing the necessary techniques to pre-empt and tackle cyberthreats. It contains a detailed analysis of the situation in the Arab region, the challenges it faces and existing disparities between the Arab region and other regions in terms of the growing threat of cybercrime, national cybersafety strategies, enacting and implementing cyber legislation and regional cooperation.

The principal aim of the present study is to set out a cybersafety framework for the Arab region. ESCWA urges Arab Governments to use this framework and adapt it in line with national specificities and needs to establish an integrated environment designed to ensure cybersafety and combat cybercrime. Governments can also use parts of the framework to address shortfalls and update national legislation and institutions to ensure cybersecurity. The framework comprises several sections and recommendations, as follows:

[1] ITU, *Measuring the Information Society Report 2014* (Geneva, 2014).

[2] Todd Neal, Combat cybercrime with compliance and ethics. Available from www.tnwinc.com/2910/information-security-training-2.

[3] ESCWA, Cyber legislation directive (2012), E/ESCWA/ICTD/2011/Technical Paper.5 (in Arabic only).

[4] Available from www.escwa.un.org/arabic/information/pubaction.asp?PubID=1520 (in Arabic).

(a) Formulating a national strategy to ensure cybersafety and combat cybercrime, covering legislative, operational, organizational and educational aspects; It should also covers awareness-raising, specialized training, national approaches to handling cyber incidents, the establishment of specialized institutions, the provision of cadres, and strengthening regional cooperation and partnerships between the public and private sectors;

(b) Proposing legislative measures to ensure cybersafety in the Arab region on the basis of comprehensive national surveys of relevant laws to avoid contradictions, noting that national laws require periodic updating in view of the ever-evolving nature of legal issues related to cyberspace violations;

(c) Developing methods and mechanisms to enforce laws, including establishing offices to investigate cybercrimes, either as part of public prosecution services, as joint forces comprising several institutions or as central investigation offices. Pre-emptive measures include establishing computer emergency response teams (CERTs) as a key tool for protecting the fragile digital infrastructure;

(d) Developing awareness-raising, educational and specialized training courses targeting Internet users and should be disseminated through all communication tools (media, audiovisual and educational); awareness-raising and training courses should include specialized training sessions for judges, investigators, police personnel and technicians in police forces and CERTs;

(e) Strengthening cooperation between the public and private sectors to ensure cybersafety through information exchange, sharing financial burdens, practical cooperation, developing technical solutions and increasing investment;

(f) Enhancing regional and international cooperation, which is vital given the cross-border nature of cybercrime.

It should be noted that annex III to the full study in Arabic contains a model law on the procedural aspects of cybercrime and digital evidence, which Arab States can benefit from and adapt when enacting procedural laws.

## Introduction

Information and communication technologies have created new opportunities for educational, social, economic, political and legal development; however, the ever-increasing dependence on them has given rise to threats resulting from the misuse of such technologies. Moreover, the rising number of Internet users has increased the number of potential victims of cybercrimes resulting from the irresponsible use of the Internet and its applications, attacks on insufficiently protected electronic devices, or intentional or accidental personal attacks. Electronic threats are complicated by anonymity mechanisms, innovative cyberattack methods used by hackers, the fast-paced development of technology and the cross-border nature of cybercrime.

The openness of the Internet is both a source of strength and weakness, rendering it vulnerable to cybercrime. For the Internet to fulfil its purpose, it has to maintain its openness and interoperability[5] with other systems and equipment; nevertheless, this openness facilitates the process of conducting criminal activities on the Internet. Concerted efforts are therefore necessary to limit threats to the Internet and mobile devices and protect all information and communication technology users, individuals and institutions alike. To this end, ESCWA has prepared the present summary report to determine the necessary policy frameworks for enhancing cybersafety in the Arab region and clarify methods for combating cybercrime at the national and regional levels, so as to meet international levels.

Governments and enterprises are gradually becoming aware of the threats cybercrime poses and the importance of cybersafety for national economic and political security. Cybercrime results in significant direct and indirect financial losses, affecting individuals and economies alike. For example, estimated losses in Australia reached $2 billion in 2012.[6] The United States Federal Bureau of Investigation considers cybercrime as one of the most significant threats faced by the United States of America.[7] Around 60 per cent of business owners in the United States believe that losses incurred as a result of cybercrime exceed losses from other crimes.[8] Moreover, a 2011 Europol report[9] on assessing the threat of organized crime indicated that the Internet had become a key facilitator of organized crime. In the Middle East, 48 per cent of those who participated in a 2014 survey conducted by PricewaterhouseCoopers believed that the threat of cybercrime had increased in their enterprises over the past 24 months.[10]

The present summary report is part of continuous efforts by ESCWA to develop the legal and organizational aspects of the information society. It aims to highlight the status of Arab countries with regard to ensuring cybersafety, combating cybercrime and developing mechanisms and practical approaches to improve legal and organizational frameworks for cybersafety in the Arab region. Is also indicates existing disparities between the Arab region and other regions in terms of prevailing policies and laws, implemented

[5] The White House, International strategy for cyberspace, prosperity, security and openness in a networked world (Washington, May 2011), p. 7. Available from www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[6] Norton, 2012 Norton cybercrime report. Available from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

[7] Speech by Steven R. Chabinsky, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation given at the GovSec/FOSE Conference, Washington, D.C. Available from http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom.

[8] IBM survey (2006). Available from www.03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html.

[9] Europol, *EU Organized Crime Threat Assessment: OCTA 2011* (2011), p. 6. Available from www.europol.europa.eu/sites/default/files/.../octa2011.pdf.

[10] PricewaterhouseCoopers, Economic crime in the Arab world (February 2014), p. 16. Available from www.pwc.com/m1/en/publications/gecs2014reportme.pdf.

standards and rules, and awareness-raising and training programmes. It proposes a framework for enhancing cybersafety and combating cybercrime.

## I. GLOBAL TRENDS IN COMBATING CYBERCRIME AND ENSURING CYBERSAFETY

Cybercrime is developing and spreading in line with technological progress. Electronic devices are getting smaller but memory space and processing speeds are growing. All devices contain processors and it is expected that electronic control will become more widespread with the development of the Internet of Things. Cyberspace challenges can be summarized as follows:[11] it is mainly the trade sector that monitors cyberspace, which is not a centralized system by nature; it is difficult to predict how cyberspace will be used in the future because of fast-paced advancements in technology and innovation, which cyberspace protection and defence methods cannot keep up with.

Lately, countries have adopted general trends to combat cybercrime at the global level, which could form the foundation of national policies and strategies on cybersafety, taking into account that such trends must be adapted to meet country specificities, capabilities and legal and social systems. A study by the International Telecommunication Union (ITU)[12] on 62 countries across the world shows that 57 per cent have cybersafety strategies; of the countries that do not, 67 per cent are in the process of developing them. However, the majority of Arab countries do not have cybersaftey strategies and many have not yet begun drafting national strategies.

### A. Overview of international efforts

At the international level, the General Assembly has issued several resolutions on cybercrime, notably resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies. Resolution 55/63 provides that States should ensure that their laws and practices eliminate safe havens for those who criminally misuse information technologies, and that legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized. Outputs from the World Summit on the Information Society, held in Geneva in 2003 and in Tunis in 2005, indicate the importance of developing the information society in all countries. These documents, which include the Geneva Declaration of Principles,[13] the Geneva Plan of Action,[14] the Tunis Commitment[15] and the Tunis Agenda for the Information Society,[16] highlight the importance of enhancing confidence and security in the information society and set out the frameworks for achieving those objectives. A total of 174 States have adopted these outcome documents.

The Council of Europe Convention on Cybercrime (also known as the Budapest Convention), which came into effect on 1 July 2004, is a key regional treaty aimed at harmonizing national cybercrime legislation, building national capacities to investigate cybercrime and strengthening cooperation in this field. Moreover, to harmonize cybercrime legislation in the Commonwealth of Nations, a group of experts prepared a model law in 2002 inspired by the Budapest Convention, known as the Computer Related

[11] Cabinet Office, The UK cyber security strategy: protecting and promoting the UK in a digital world (November 2011), p. 18. Available from www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final. pdf.

[12] ITU, *2013 ITU survey on measures to raise awareness on cybersecurity* (August 2013), p. 15. Available from www.itu.int/en/ITU-D/Cybersecurity/Documents/22survey.pdf.

[13] Available from www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|0.

[14] Available from www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

[15] Available from www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|0.

[16] Available from www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

Offences Act. Furthermore, in 2003, the European Union adopted a legal framework on information system violations, which came into effect in 2005.

In the Arab region, the Arab Convention on Combating Information Technology Offences was adopted on 21 December 2010.[17] By 2014, 18 Arab States had signed the Convention and seven had ratified it. ESCWA, under the project entitled "Regional harmonization of cyber legislation to promote the knowledge society in the Arab world",[18] implemented over the period 2009-2012, prepared its directives on cyber legislation,[19] which can be considered as model legislation for Arab countries.

## B. LEGISLATIVE TRENDS

Responses from countries surveyed under a study by the United Nations Office on Drugs and Crime (UNODC) [20] show that some cyberactivities are classed as offences pursuant to traditional legal texts, but others have been criminalized under special laws, taking into account that the latter are also bound by traditional criminal laws in terms of identifying elements of crimes and perpetrators, criminal attempts, defences to criminal charges, among other things. The majority of States are attempting to broaden the application of their traditional laws to cover cybercrime.

Responses from countries also show that legal texts on cybercrime are not codified under one law; they are spread among several laws including penal laws, information technology laws and criminal procedure laws. Moreover, responses indicate that legislative work is focusing on aspects of cybercrime other than criminalization, such as procedures, evidence collection and international cooperation. Several countries are updating both the substantive and procedural aspects of their legislation to combat cybercrime.

The UNODC study recommends harmonizing legislation between countries to eliminate safe havens for perpetrators and to collect electronic evidence, given that certain States require the dual criminality of the act for juridical cooperation. The study shows that the majority of recognized cybercrimes are considered offences in most countries, except those related to spam, and to a lesser extent those related to the misuse of electronic devices, cyber-racism and online grooming of children.

Although the Arab region has generally been slow in updating its laws in general, and cyber legislation in particular, Arab States have been focusing on combating cybercrime and several have implemented special laws, even if this type of legislation is labelled differently between countries.[21]

## C. TRENDS RELATED TO THE APPLICATION OF LAWS AND REGULATIONS

The first operational step to ensuring cybersafety and combating cybercrime is for States to develop comprehensive policies on the issue, which include requirements and procedures for cybersafety; effective electronic and physical methods; technical, organizational and operational protection measures; and procedures to combat and report cyberthreats and support victims. Such policies should be disseminated to government institutions, individuals and enterprises to raise awareness on the issue. The UNODC study[22] shows that 70 per cent of surveyed countries have some form of policy on cybercrime or are in the process of

[17] Available from http://www.lasportal.org/ar/legalnetwork/Pages/typicalarablaws.aspx (in Arabic).

[18] Available from http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/en-LB/Default.aspx.

[19] Available from http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Directives-Full.pdf (in Arabic).

[20] United Nations Office on Drugs and Crime (UNODC), *Comprehensive study on cybercrime,* draft (February 2013), pp. 51-52.

[21] ESCWA, *Regional Profile of the Information Society in the Arab Region* (2013), p. 76. Available from www.escwa.un.org/information/publications/edit/upload/E_ESCWA_ICTD_13_6_E.pdf.

[22] UNODC, 2013, pp. 225, 226 and 233.

developing one, covering awareness-raising, international cooperation and law application; this percentage drops among Arab countries.

Regarding the implementation of cyber legislation, there is a need for specialized official investigative bodies to investigate cybercrimes and traditional crimes with complex digital evidence. Their aim should be to support investigation procedures, which are legal in principle, with technical expertise to collect digital evidence from crime scenes and other places and retain it, ensuring its validity, so that it can be analysed to reach legal conclusions that can be presented in court in comprehensive reports containing necessary explanations. The same UNODC study shows that 90 per cent of surveyed countries have established or are establishing cybercrime and digital evidence investigation offices, although the number of their personnel, even in developed countries, does not exceed one per cent of the number of police personnel.[23] The majority of Arab countries have developed specialized offices to investigate cybercrime.[24]

Developed countries have formed CERTs, which are key to protecting the fragile digital infrastructure. Their responsibilities include monitoring cyber threats, providing solutions and measures to tackle them, publishing information on them of their websites, launching media campaigns to warn individuals and offer advice and guidelines on protecting their devices and information, and implementing comprehensive awareness-raising campaigns. In some countries, CERTs cooperate with certain specialized institutions, such as public prosecution offices, judicial investigative bodies, research centres and universities, to prepare rules of conduct for individuals and enterprises to protect their computer systems and data.

### D. Trends of cooperation between States

The UNODC study stresses the need for official and unofficial mechanisms for judicial cooperation between States, either under international and bilateral agreements, national laws or the principle of reciprocity to avoid violating national sovereignty. It might be necessary for States to carry out investigations in other countries, given that 50 per cent of surveyed countries indicated that over 50 per cent of cybercrimes have an international element. International cooperation also results in the exchange of information and lessons learned from the experiences of and best practices in other countries, which contributes to national cybersecurity.[25]

### E. Other technological and administrative trends: collaboration with the private sector

Of the surveyed countries in the UNODC study, 50 per cent stated that their strategies included collaboration with the private sector to combat cybercrime, which covered the exchange of information, cases and assistance; awareness-raising; exchanging best practices and prevention measures; developing technical solutions; international cooperation; and policymaking. Collaboration with Internet service providers allows States to block illegal websites or prevent data transfer from suspicious electronic addresses. Web hosting companies can monitor services provided by websites they host (illegal content or intellectual property infringements) and prohibit the unlawful use of these services. Technical issues include requiring information technology companies to follow security standards when designing smart services and applications.[26]

[23] Ibid, p. 152 and 154.

[24] See annex V to the full report in Arabic.

[25] Secretariat of the Security and Defense Committee, *Finland's Cyber Security Strategy* (2013), p. 9. Available from www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

[26] Ibid., p. 10.

### F. Awareness-raising and training trends

Raising the awareness of users on the key principles of cybersecurity must be a fundamental part of any national or regional strategy or initiative to combat cybercrime;[27] most countries are aware of this and strive to raise awareness among users of cyberthreats and cybercrimes and how to prevent them.[28] The complex nature of information technology and the specific rules that govern it, whether at the procedural or substantive levels, and the technical language that judges might be obliged to use, mean that judges, investigators and police personnel must undergo training on how to handle cybercrimes and digital evidence.

## II. REGIONAL CHALLENGES IN THE AREA OF CYBERSAFETY AND COMBATING CYBERCRIME

Challenges in the Arab region do not differ greatly from those other developing regions face. The following sections set out Arab specificities.

### A. Cybercrime challenges and specificities in the Arab region

#### 1. *Development of Internet use and the increase in cybercrime*

In the Arab region, Internet use is growing significantly. Statistics show that 40 per cent of Internet users in the Middle East and North Africa (MENA) spend over 20 hours a week online, which is the same as the global average.[29] Data show that cybercrime averages in the Middle East are relatively higher than global averages because of the weakness of mechanisms to combat such crimes. Criminals in the Arab region are increasingly using information technologies to commit offences because of its significant gains, low risks, remote access and the relative difficulty of assigning liability. The rise in cybercrime has led to an increase in traditional crime, given that the former can be used to facilitate the latter.

In the Arab region, the majority of cybercrimes are a means to commit traditional crimes. According to a 2011 study, [30] the United Arab Emirates ranks nineteenth and Lebanon twenty-fifth globally in the list of countries that are affected by cyberattatcks.

#### 2. *Lack of statistics and studies on cybercrime*

It can be difficult to conduct regional studies on cybercrime and cybersafety that compare between Arab countries for the following reasons: absence of standardized definitions of what constitutes cybercrime and of certain legal and technical concepts; shortage of information sources for analytical studies because of a lack of public awareness and the unfamiliarity of the judiciary and police personnel with the technical aspects of cybercrime; the absence of official bodies to record complaints and publish reliable statistics on cybercrime; cybercrime victims not coming forward to complain or share their experiences; and the absence of specialized investigative bodies to combat cybercrime. Moreover, cybercrime statistics are unreliable, scarce and contradictory in the Arab region, especially when compared to those of developed countries. This weakness indicates that the issue is not accorded enough importance by stakeholders, which complicates the development of effective policies and strategies built on solid and reliable information.

[27] ITU, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (September 2012), p. 18.

[28] University of Mississippi School of Law, National Center for Justice and the Rule of Law, *Combating Cyber Crime: Essential Tools and Effective Organizational Structures: A Guide for Policy Makers and Managers* (2007), p. 47. Available from www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf.

[29] Rassed, *The attitudes of online users in the MENA region cybersafety, security and data privacy* (May 2014), p. 9. Available from www.ictqatar.qa/sites/default/files/Cybersafety,%20security%20and%20data%20privacy.pdf.

[30] Hamadoun I. Touré, Cybersecurity: global status update (December 2011), p. 5. Available from www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf.

## B. Strategic challenges in the Arab region

Developing a comprehensive strategy on cybersafety would set out the desired goals and the required activities to achieve them, which could then be divided into stages, thus facilitating the allocation of human, financial, organizational and technical resources and the organization of funding methods in line with specific plans. Developing strategies would also determine operational timeframes, mechanisms and stakeholders, and facilitate the establishment of coordination mechanisms between them. Most Arab countries lack comprehensive cybersafety strategies, but some (like Jordan) are developing them on the basis of international experiences. The remainder of Arab countries, including Egypt, the Syrian Arab Republic and the United Arab Emirates, only have general strategies for the information and communication technology sector.

## C. Cyberspace legislative challenges in the Arab region

### 1. *Cybercrime legislation in some Arab countries*

The status of cybercrime laws differs among Arab countries; some have issued specific laws (Bahrain, Jordan, Oman, Saudi Arabia, the Sudan, the Syrian Arab Republic and the United Arab Emirates), while others (Morocco and Tunisia) have included articles on cybercrime in existing laws, especially in electronic transactions and trade and intellectual property protection laws. Palestine is drafting provisions on cybercrime to add to its penal code, and Egypt and Lebanon have drafted laws on cybercrime.

### 2. *Obstacles to enacting and updating cyber legislation*

In the Arab region, pursuant to high-level decisions, cybercrime legislation has been enacted and then developed, as is the case in the United Arab Emirates. However, in Lebanon, for example, cybercrime legislation was not enacted until 2014, either because of a lack of political stability and the prioritization of other issues or because of an absence of a digital culture among officials who were not aware of the importance of the issue. In the meantime, penal codes and other laws are being used to try certain cybercrimes, meaning that many cybercrimes remain unbound by laws.

### 3. *Rules of criminal procedure in cybercrime cases*

Legislators in the Arab region have not developed procedural rules to regulate investigations and digital evidence collection in cybercrime cases, which require specific rules of procedure because of their nature. However, for example, Syrian legislative decree No. 17 of 8 February 2012 on regulating communication on the Internet and combating cybercrime included some rules of procedure, especially related to the responsibilities of service providers, such as storing network traffic data, identifying the domain owners and providing data to the judicial authorities, and establishing judicial police forces under interior ministries that specialize in cybercrime and determining their mandates in terms of investigation, inspection and regulation. In the UNODC study, 60 per cent of surveyed Arab countries indicated that national legal texts on cybercrime were insufficient, especially in terms of new investigative procedures, such as remote digital evidence collection.

### 4. *Developing regulations or executive decrees for the enforcement of laws*

Some Arab countries have developed executive decrees to apply laws, which can be issued and amended in line with technological developments and used to breakdown laws, given the slowness of legislative processes and the general nature of some laws, which can be broken down into regulations, circulars and decrees. For example, the United Arab Emirates issued circular No. 6 of 2013 on the Government's policy and standards for information security. The Emirati Cabinet also issued decision No. 21 of 2013 on information security regulation in federal entities. In the Syrian Arab Republic, the Ministry of Communications and Technology, represented by the National Commission for Network Services and the

Telecommunications Regulatory Authority, has been granted the authority to develop regulations for Internet communication, digital crimes and violations and telecommunication crimes. As a result, several regulations[31] were issued on digital safety and on national policies for information security.[32]

### 5. *Digital and electronic evidence in legislation*

In the Arab region, problems arise regarding the legality of digital evidence and their admissibility in court as proof of cybercrimes or traditional crimes if laws do not specify this. In some countries that implement systems of conditional proof or legal evidence or mixed systems where the law clearly sets out the types of admissible evidence and their strength, as is the case in Libya, digital evidence might not be admissible in court.[33] Less problems arise in that regard in countries that follow the Roman-Germanic legal system, whose codes of criminal procedure do not cover digital evidence, but that follow a system of free evaluation of evidence by judges whereby judges have the discretion to admit or reject evidence, as is the case in Lebanon.

## D. CHALLENGES OF LAW ENFORCEMENT IN THE ARAB REGION

### 1. *Addressing legislative shortfalls*

Arab countries have developed various solutions to address cyber legislation shortfalls. For example, the Public Prosecutor's Office in Lebanon issued circulars for communication service providers requiring them to retain Internet traffic data for a set period until the adoption of draft legislation currently being considered by Parliament. The Egyptian Public Prosecution has regulated its powers to issue decisions during investigations, which Egyptian enterprises must abide by.[34] The judiciary in some countries is applying traditional penal code texts to cybercrimes. In Lebanon, for example, vandalism rulings have been issued in computer abuse cases, public indecency rulings have been issued in cases where pornographic material has been posted online and fraud sentences have been given in Internet fraud cases.

### 2.. *Weakness of investigative bodies*

Many cybercrimes in the Arab region are not effectively investigated and perpetrators remain unidentified because of the limited resources available to investigative bodies, especially in countries with limited financial resources. Moreover, in some countries, specialized police units are not well equipped to handle cases. In developing countries, there is an acute lack of specialized police personnel to investigate cybercrimes, estimated at 0.2 for each 100,000 Internet users; between two and five times less than developed countries. In some countries, police personnel only have basic equipment and limited knowledge and expertise.

### 3. *Absence or weakness of specialized investigation offices*

Progress is being made in some Arab countries in terms of establishing specialized police offices to investigate cybercrimes and collect and analyse digital evidence. These offices comprise trained information system technicians who use equipment and software to process digital evidence. These offices have specific and clear powers that do not conflict with those of other offices. Such offices include the electronic investigation department established in Dubai in 2008 and the cybercrime investigation section of the Public Security Department under the Criminal Investigations Department in Jordan.[35] In Lebanon, the Cybercrime

[31] Available from http://nans.gov.sy/index.php/nansdocuments (in Arabic).

[32] Available from http://nans.gov.sy/images/stories/doc/isc_doc/policy-isc.pdf (in Arabic).

[33] www.startimes.com/f.aspx?t=30245909: طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ص 7 وما يليها.

[34] Response of the Arab Association for Electronic Arbitration on an ESCWA survey under this study, September 2014.

[35] Response of the Jordanian National Information Technology Centre on an ESCWA survey under this study, September 2014.

and Intellectual Property Rights Bureau was established in 2006 under the Internal Security Forces. In Egypt, the Interior Ministry established the Intelligence Administration for Crimes of Computer and Information Networks in 2002.

### 4. *Problems with judicial specialization*

Legal bodies face judicial specialization problems in applying laws in terms of investigating cybercrimes and pursuing perpetrators. Offenders and victims exist in the physical world whereas cybercrimes are committed in the virtual world; servers and communication devices are not in the same places as offenders and victims.[36] From a judicial perspective, the issue of double criminality raises problems when investigating cybercrimes and pursuing and trying perpetrators. Moreover, cybercrimes are transboundary by nature, which poses difficulties when moving from one legal system to another, such as when moving from the Anglo-Saxon to the Roman-Germanic legal system; a problem compounded when one country is more specialized that another in combating cybercrime, which may lead to disputes over where judicial proceedings should take place.

## E. CERTs in the Arab region

In line with the international approach of establishing State bodies concerned with cybersecurity, several Arab countries have set up national CERTs.

Table 1. CERTs in the Arab region

| Country | Name of CERTs | Website | Year of establishment |
|---|---|---|---|
| United Arab Emirates | aeCERT | www.aecert.ae | 2008 |
| Jordan | Computer Emergency Response Team | | Underway |
| Kuwait | Computer Emergency Response Team | | Underway |
| Saudi Arabia | CERT.sa | www.cert.gov.sa | |
| Syrian Arab Republic | SyCERT under the National Commission for Network Services | | Underway |
| Sudan | Sudan CERT | www.cert.sd | 2010 |
| Tunisia | tunCERT | www.tuncert.ansi.tn | 2007 |
| Oman | OCERT | www.cert.gov.om | 2010 |
| Qatar | Q-CERT | www.qcert.org | 2005 |
| Egypt | EG CERT | www.egcert.eg | 2010 |

## F. Regional coordination and cooperation between Arab countries

There is a lack of effective judicial cooperation between Arab countries in the field of cybercrime investigation. Although the Arab Convention on Combating Information Technology Offences was developed on 21 December 2010, which contains a chapter (Chapter IV) on legal and judicial cooperation, coordination between Arab countries remains ineffective even though 18 States had adopted the Convention by 2014. The Arab law to combat information technology offences[37] does not contain texts on procedure or international cooperation; it only sets out substantive rules that break down information technology offences.

[36] Kristin M. Finklea, and Catherine A. Theohary, Cybercrime: conceptual issues for Congress and U.S. law enforcement (January 2013), p. 10. Available from http://fas.org/sgp/crs/misc/R42547.pdf.

[37] Available from www.carjj.org/node/246 (in Arabic).

The absence of standardized definitions of cybercrimes also hampers cooperation between countries; certain actions may be criminalized in some countries but not in others. Countries where such offences are not criminalized do not cooperate to solve such cases. Moreover, sentences given for the same offence might differ between countries; some countries may issue fines (infractions), while others might sentence offenders to short-term imprisonment (misdemeanours) or to severer sentences (felonies).

## G. Challenges faced by the private sector in the Arab region

Private sector institutions in the Arab region are striving to understand and prevent cybercrime and its threats to avoid becoming victims of cyberattacks. It is difficult to accurately estimate material losses from cybercrime in the Arab region. A study[38] has shown that 40 per cent of surveyed institutions had not suffered any losses from the cybercrimes that had affected them, which is worrying because in many cases the damage is only discovered at a later date; 6 per cent of institutions estimated their losses at over $1 million and 2 per cent between $5 million and $10 million.

The following are problems related to cybersecurity and cybercrime in the private sector: the cost of security systems and work disruption; the negative effects of cybercrime on revenue and profit and on computer systems; loss of reputation; and loss of opportunities owing to avoiding certain products or markets. Factors that weaken Internet service providers in the Arab region include policies and regulations that impede their involvement to prevent data being transferred to offenders, because of the principle of network neutrality. Privacy laws also ban them from monitoring content and exchanging information on criminal activities with other providers.[39]

## H. Challenges related to culture and cybersafety awareness in the Arab region

In the Arab region, the actions of cyber-offenders and public opinion sometimes differ greatly to those across the world. They are influenced by social, cultural, religious and economic factors that reflect regional specificities, which impose special rules that might diverge from those applied elsewhere.

A 2014 study by Rassed of 14 countries[40] indicated that people in the Arab region are not very aware of cyberthreats. Internet users in the MENA region, although 45 per cent state that they take precautions when on the Internet, are more likely to communicate with strangers online than in any other region and open emails and attachments from unknown sources.

Awareness-raising and user-training campaigns are relatively ineffective and unsuccessful because of weak coverage and marketing. They are also limited in number, do not target those most in need, do not attract many participants, their topics and techniques are outdated and their lecturers are badly chosen. The majority of school and university curriculums do not cover cybersafety and there are no media campaigns to bridge these gaps. Awareness-raising campaigns targeting women are especially weak, in particular on crimes that affect women more than men.

Victims in the Arab region do not report cybercrimes for many reasons, including belief that the process is futile because offenders cannot be discovered; fear that their business reputation would be affected leading to a loss of clients; lack of technical knowledge; lack of confidence in the technical knowledge of police personnel; and embarrassment from having fallen victim to such crimes. There are several cases of women who have suffered online abuse but have chosen not to inform the authorities.

[38] John Wilkinson, and Tareq Haddad, Economic crime in the Arab world (February 2014), p. 16. Available from www.pwc.com/m1/en/publications/gecs2014reportme.pdf.

[39] Micheal Barrett, and others, Combating cybercrime: principles, policies and programs (April 2011), p. 5. www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf.

[40] Rassed, May 2014, pp. 3, 10 and 31.

TABLE 2. SUMMARY OF THE STATUS OF CYBERSECURITY IN THREE ARAB COUNTRIES

| | **United Arab Emirates** | **Egypt** | **Lebanon** |
|---|---|---|---|
| **Political will to update cybersecurity** | A clear political will exists | Affected by sporadic political instability and a lack of security; other issues have priority | Affected by a lack of political stability and security; other issues have priority |
| **Cybersecurity strategy** | A strategy exists that requires updating and detailing | A strategy exists that requires updating and detailing | No strategy exists |
| **Cyber legislation** | -Legislation has been enacted which is being updated continuously<br>-Some legislation is still lacking | -Some legislation has been enacted<br>-Key legislation is still lacking<br>-Legislation is not updated as often as required | -Limited legislation has been enacted<br>-Draft bills have been prepared<br>-A legal workshop is required |
| **Procedural laws** | Non-existent | Non-existent | Non-existent |
| **Legislation application** | Existing legislation is easily applied | The judiciary applies texts from the traditional Penal Code | The judiciary applies texts from the traditional Penal Code |
| **Regulation** | -Specialized investigative bodies exist<br>-Absence of specialized courts | -Specialized investigative bodies exist<br>-Absence of specialized courts | -Specialized investigative bodies exist<br>-Absence of specialized courts |
| **CERTs** | Exists | Exists | Non-existent |
| **Cybersecurity code of conduct** | Exist but require updating | Non-existent | Non-existent |
| **Private sector cooperation** | Cooperates with investigative bodies | Cooperates with investigative bodies | Cooperates with investigative bodies but obstacles exist |
| **Awareness-raising** | Public and specialized campaigns are held (must be done continuously) | Insufficient public and specialized campaigns are held | Insufficient public and specialized campaigns are held |
| **Training** | Specialized training sessions are held for judges and police personnel (must be done continuously) | Insufficient specialized training sessions were held for judges and police personnel | Insufficient specialized training sessions were held for judges and police personnel |
| **Statistics** | Statistics exist on cybercrime and information security | Insufficient statistics exist on cybercrime and information security | Insufficient statistics exist on cybercrime and information security |

# III. FRAMEWORK FOR ENSURING CYBERSAFETY AND COMBATING CYBERCRIME IN THE ARAB REGION

ESCWA suggests the framework below to enhance cybersafety and combat cybercrime in the Arab region. Arab Governments can use this framework at the national level as a comprehensive method to ensure cybersafety or can select sections to adapt to their legislative, legal and organizational situations and national requirements.

## A. DEVELOPING NATIONAL STRATEGIES TO ENSURE CYBERSAFETY AND COMBAT CYBERCRIME

It is recommended that national strategies to ensure cybersafety and combat cybercrime cover the following:

(a) Developing and updating necessary cyber legislation;

(b) Implementing methodologies to respond to cyber incidents, in particular forming CERTs and establishing communication and cooperation methods between these teams in the Arab region;

(c) Supporting the software and hardware industry and the development of technical solutions for cyberthreat protection;

(d) Strengthening partnerships between the public and private sectors, especially in terms of awareness-raising campaigns, technical solutions, storing network traffic data, identifying domain users and funding;

(e) Encouraging Internet users to adopt electronic identities, especially when accessing sensitive websites, such as financial websites;

(f) Developing systems for the quick reporting of cybercrimes that ensure confidentiality and uphold the rights of women and children;

(g) Adopting gender-sensitive indicators that can assess cybercrime levels and updating them regularly;

(h) Continuously raising the awareness of individuals and institutions on cybersafety and cybercrime;

(i) Improving cybersafety training to increase the number of specialists in the field;

(g) Cooperating to combat cybercrime under the auspices of the League of Arab States to increase information exchange between official bodies.

## B. PROPOSED LEGISLATION TO ENSURE CYBERSAFETY IN THE ARAB REGION

To develop effective legislative policy founded on accurate information, States must conduct comprehensive and detailed analyses of existing national laws before enacting new ones, to avoid unclear laws that may conflict with existing ones and arbitrary interpretations of vague terms and phrases by public prosecutors during trials.[41] National legislation also requires regular updating, especially to address legal issues arising from the evolving nature of cyberspace. Arab countries can apply the following best practices whose effectiveness has been proven in other countries:

(a) Carrying out the minimum legislative amendments required to ensure appropriate levels of cybersafety;

[41] Steven Titch, Four principles for effective cybersecurity law and policy (25 April 2014). Available from www.rstreet.org/2014/04/25/four-principles-for-effective-cybersecurity-law-and-policy.

(b) Interpreting laws in ways that allow stakeholders to prioritize cybersafety;

(c) Avoiding combining cybercrime with other issues, such as intellectual property and privacy;

(d) Enacting legislation that enables State bodies to attack command and control servers (botnet controllers) that compromise individuals' devices;

(e) Expediting cooperation processes between national investigative bodies through electronic connectivity;

(f) Trying offenders in their country of residence rather than in victims' if deportation requests are denied.

There should be a unified legislative approach between Arab countries, or approaches should be coordinated at the very least. Standardized and consistent definitions for cybercrimes are also necessary. Categorization of offences should also be standardized; offenders can escape prosecution if one country criminalizes an action and another does not. Cooperation between official bodies in Arab countries is not sufficient; it is important to include the private sector , especially enterprises that develop computer software and programmes and communication companies.[42] When enacting legislation, Arab States can draw substantive and some procedural aspects from the ESCWA 2012 cyber legislation directives, which are applicable in Arab countries with Roman-Germanic legal systems. States can also refer to the Budapest Convention, the 2010 Arab convention on combating information technology crimes and the 2003 Arab law to combat information technology offences.

## C. Legislation enforcement means and bodies

Countries offer several examples of ways to organize digital evidence investigation offices. Some have established specialized offices within their public prosecution offices to investigate cybercrimes, headed by a public prosecutor and comprising a team of investigators and technicians. Another option is to establish a common force combining several institutions that include investigators, technicians and police personnel. Other countries have established central investigation offices for digital evidence or decentralized offices.[43] Any of these models can be adopted in Arab countries.

Coordination between ministries and specialized bodies within a country is vital for combating cybercrime, especially between ministries of justice, economy, communications and the interior. Regarding women's issues, investigative teams must have experience handling gender-based cybercrimes or crimes of violence against women; investigative teams should therefore comprise well-trained female personnel. Public prosecution personnel should also have experience in these issues to pursue perpetrators of gender-based cybercrimes, without negatively affecting the mental and physical health of victims. It is also vital to build the capacities of official bodies in Arab countries to pre-empt and prevent cybercrimes; "pre-emptive investigators" are therefore being trained to identify potential offenders.

## D. Awareness-raising, education and training methods

There are many methods to raise awareness on the dangers of cyberspace, including television programmes, media interviews, leaflets, seminars in schools and universities, short films, interactive games, websites, web pages, facebook pages, text messages, conferences and public speeches. It is also important to raise awareness of online violence against women, and government authorities should interact with non-governmental organizations and civil society organizations concerned with women's issues to educate

[42] Fausto Pocar, New challenges for international rules against cyber-crime (2004).

[43] University of Mississippi School of Law, 2007, p. 17.

women on the dangers of cybercrime and available protection mechanisms. Arab Governments must take practical steps to encourage individuals and institutions to report cybercrimes for several reason, including the establishment of national databases used to formulate strategies to combat cybercrime.

Building the capacities of legal personnel is a key government activity to ensure cybersafety. States must hold specialized training sessions for those who work in the field of cybersafety and cybercrime, and periodic sessions for technicians in police forces and CERTs. Governments should also encourage the introduction of subjects on strengthening cybersecurity mechanisms and combating cybercrime in the curriculums of specialized universities, especially informatics and law faculties and in judicial and management institutes.

### E. Cooperation between the public and private sectors

Arab countries should offer incentives to encourage cooperation and partnership between the public and private sectors, especially for communication service providers, the exchange of cybercrime information, network traffic data storage, domain owner identification and data provision to judicial authorities. The private sector and Internet service providers play a key role in developing secure software, publishing methods that prevent cybercrimes and protect from cyberthreats, and launching public awareness campaigns. The following are best practices in the field of cybersafety that countries can refer to:[44]

(a) Governments should oversee technical monitoring in the field of cybersecurity rather than delegating the responsibility to the private sector;

(b) Developing solutions that ensure cybersecurity without affecting privacy;

(c) Partnering with Internet governance institutions to develop solutions;

(d) Collecting information on cybercrimes and building national, regional and international databases;

(e) Requiring information technology device manufactures to guarantee the safety of their products by ensuring that safety software update automatically and that remote maintenance can only be accessed using complex passwords;

(f) Raising awareness among individuals for their own protection and the protection of others;

(g) Looking at the issue of cybersafety from an international perspective because of the global nature of the Internet, which would require countries to undertake coordinated technical amendments;

(h) Retaining the metadata of sellers partaking in electronic trade, given that anonymity is not conducive to combating cybercrime;

(i) Increasing investment in applying laws to combat cybercrime, given that they remain relatively underfunded compared to traditional laws;

(j) Monitoring networks and cooperating with communication service providers by providing them with the IP addresses of compromised ("zombie") computers so they can inform their owners;

(k) Allowing transit providers to stop data emanating from botnets, after assessing packet header data;

[44] Micheal Barrett, and others, *Combating Cybercrime: Principles, Policies and Programs* (April 2011), pp. 7-25. Available from www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf.

(l) Allowing communication service providers to prevent packet headers from leaving their networks if senders' IP addresses are incorrect (IP spoofing);

(m) Increasing public and private funding for efforts to raise user awareness of cybersafety;

(n) Preventing unprotected devices from connecting to the Internet;

(o) Establishing secure methods for enterprises to exchange information on hackers that go beyond traditional methods;

(p) Urging registrars to examine domain owner data to identify false information and urging the Internet Corporation for Assigned Names and Numbers to implement its safety regulations.

## F. COOPERATION BETWEEN ARAB COUNTRIES TO ENHANCE CYBERSAFETY

Countries should implement the 2010 Arab Convention on Combating Information Technology Offences, which sets out up to date cooperation mechanisms. They can also refer to the ESCWA cyber legislation directives, including the directive on electronic crimes and procedure, detailed in annex III to the document and derived from the Budapest Convention. In important criminal investigations, where time is a vital factor, judicial cooperation on cybercrimes has significantly improved recently, as a result of the Budapest Convention and the Arab Convention on Combating Information Technology Offences. The shortfalls of the Budapest Convention include that it has not been adopted by key parties, such as China, the Russian Federation and some Asian, Latin American and African States, but several countries have incorporated the Convention's contents within their national laws. In this regard, special focus should be given to unofficial cooperation mechanisms between countries specialized bodies, given that official procedures in the area of judicial cooperation are time-consuming and could lead to the loss of digital evidence and offenders.

Information and communication technology has become a fundamental tool, used daily in most sectors and economic activities. Technological advances, such as high Internet and mobile phone penetration and the availability and affordability of mobile broadband services, have led to a growing number of Internet users and an increasing reliance on these technologies in economic and social development. However, the openness of the Internet, and cyberspace in general, has made it susceptible to abuse and users are vulnerable to attacks by criminals and hackers. Thus, legal, regulatory and procedural frameworks are needed to combat cyberthreats and raise awareness among individuals and institutions of such risks and their impact on work and personal life.

The present study complements activities initiated by the Economic and Social Commission for Western Asia (ESCWA) in 2007 to develop, harmonize and enforce cyber legislation in the Arab region. It focuses on cybersafety and combating cybercrime given their importance to building and developing an information society in the Arab region. It provides an analytical overview of the current situation at the regional and international levels and highlights measures to strengthen and harmonize efforts to combat cybercrime and promote cybersafety. It also proposes a guiding policy framework to enhance cybersecurity and build confidence in information and communication technologies and cyberspace. The framework stresses the need to develop a national strategy to ensure cybersafety and combat cybercrime and proposes legislative measures to ensure cybersecurity in the Arab region, including the establishment of law-enforcement bodies and cybercrime investigation offices. The framework also focuses on the importance of awareness-raising, education and specialized training; public-private partnerships to support cybersecurity; and regional and international cooperation, given the cross-border nature of cybercrime.

ESCWA urges Arab Governments to use this framework and adapt it to their national context and needs, to create an integrated cybersafety environment and combat cybercrime. Government experts can also build on parts of this framework to bridge legislative gaps and upgrade the legislative and institutional aspects of their national cybersafety and security systems.

15-00223