UNITED NATIONS E

Distr.
LIMITED
E/ESCWA/TDD/2018/….
12 April 2019

ORIGINAL: ENGLISH

Economic and Social Commission for Western Asia (ESCWA)

REPORT

Arab Regional Dialogue and Experts Meeting on Internet Governance and Cybersecurity Nexus - Promoting Trust in Cyberspace Beirut, 4-6 December 2018

Summary

The Arab Regional Dialogue and Experts Meeting on Internet Governance and Cybersecurity Nexus - Promoting Trust in Cyberspace was held at the UN-House in Beirut, from 4 to 6 December 2018, and was organized by ESCWA in partnership with the League of Arab States. The meeting aimed at addressing the theme of cybersecurity and trust in line with Internet governance priority areas for the Arab region, as stipulated in the Second Arab Roadmap for Internet Governance.

The meeting was attended by around 47 experts, 23 per cent of them women, and participants were from various stakeholders - governments, business Sector, civil society organizations, technical community, academia, and international and regional organizations. The participants from the region included representatives from 14 Arab countries, namely Algeria, Egypt, Iraq, Jordan, Kuwait, Lebanon, Morocco, Oman, Palestine, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen.

The main outcomes of the meeting included the preparation of a set of key recommendations related to the theme of cybersecurity and trust in line with Internet governance priority areas for the Arab region and advancing the thematic preparations for the fifth Arab IGF as well as exploring the opportunities of partnerships for strengthening collaboration on the Arab IGF process.

CONTENTS

Page

Introduction

1. The Arab Regional Dialogue and Experts Meeting on Internet Governance and Cybersecurity Nexus - Promoting Trust in Cyberspace was held at the UN-House in Beirut, from 4 to 6 December 2018, and was organized by ESCWA in partnership with the League of Arab States. The meeting was part of the preparations for the Fifth Arab IGF meeting and have included a meeting for the Arab IGF Multistakeholder Programme Advisory Committee (AMPAC) and involved the participation of the Arab IGF Secretariat, represented by the National Telecommunication Regulatory Authority of Egypt.

2. This event has mainly discussed the theme of cybersecurity and trust in line with Internet governance priority areas for the Arab region, as stipulated in the Second Arab Roadmap for Internet Governance. It sought to present, examine and discuss Internet trust, safety and security issues as well as their linkages with the other strategic priorities of the Roadmap.

3. Participants addressed the important and emerging topics in the field at the global, regional and national levels, in line with specificities and priorities of the Arab region, and the members of the Arab IGF Multistakeholder Programme Advisory Committee (AMPAC) have collaborated on the preparations for the Fifth Arab IGF that is planned to be held in 2019. Opportunities for partnerships were explored towards strengthening collaboration with all stakeholders on the Arab IGF process. The members of AMPAC have further developed the programme of the Fifth Arab IGF and coordinators of working groups prepared concept notes for each of the topics identified as priority areas for the Forum.

I. MAIN OUTCOME - RECOMMENDATIONS

4. The main outcome of the meeting was a set of recommendations (in Arabic) targeting the development of legislative frameworks in Arab countries, regional and international cooperation, and national frameworks for cybersecurity in the Arab region. The recommendations were prepared by ESCWA based on inputs from the participating experts and the meeting discussions and were circulated after the meeting for further review and fine-tuning before finalization. A summary of these recommendations is provided below, and the original recommendations are included in Annex I of this report.

5. The recommendations related to developing the legislative framework in Arab countries aimed at the following: combating cybercrime, strengthening the security of information systems, managing and harmonizing between digital records, governing relations with international companies, strengthening the ability to address cybercrimes, forming a regional centre on cybersecurity for setting laws and harmonizing their implementation, forming a virtual cybersecurity monitor for laws and regulations on cybersecurity and cybercrime, and protecting personal data.

6. For strengthening regional and international cooperation on cybersecurity, the recommendations raised the need for various actions at the regional level, for example: Developing an Arab strategy for cybersecurity that would pave the way for harmonization of data classification, support patenting, define standards of information security and cybersecurity, and establish a compliance scoreboard; Building confidence and security in the use of ICTs; Establishing a regional cybersecurity centre to respond to cyber-attacks and build capabilities; Establishing an effective mechanism for cybersecurity, and supporting initiatives such as the Global Cybersecurity Index (GCI); Preparing an institutional map with their roles in promoting confidence and security in cyberspace; Developing basic principles for cybersecurity that aim at limiting Internet use for peaceful purposes; Extending the scope of child online protection (COP) to cover potential risks of smart devices; Ratifying existing Arab treaties on cybersecurity issues and preparing an Arab agreement for sharing digital evidence; Support countries under sanctions to access devices that facilitate digital investigations and cybersecurity; Support cybersecurity research in a similar way to the way it is applied in Europe and north America; Invite the region for cyber truce and code of conduct as a basis for cooperation on cybersecurity, and create the role of privacy officer to promote and protect privacy rights; and identify the promoters of cybercrime for the aim of having counter laws at the regional and global levels.

7. The recommendations related to developing national frameworks for cybersecurity included the following: Promoting public-private partnerships and engagement of all stakeholders towards having an effective strategy for cybersecurity; Raising awareness on cybercrime and need for protection of private information through Governments initiatives, media institutions, and academic programmes; Encouraging public investments in cybersecurity and reliance on the services of digital investigation labs; Updating national

strategies and engaging the private sector in implementation and measuring their effectiveness; Increasing cooperation on cybersecurity market research and applying incentives for investments in cybersecurity; Forming a specialized cybersecurity council to address the lack of data; Integrating the cybersecurity industrial policy in national strategies; Promoting the application of international Internet rules and related harmonization processes under the framework of United Nations, and the prevention of activities that undermine stability of cyberspace; Developing national capabilities to respond to risky practices related to large data and artificial intelligence; Strengthening consumer protection practices and capabilities related to Internet of things while benefiting from international experiences from Europe, Canada and Australia; and using e-signature and other technologies to ensure transactions and protection of data and content, and to address risks from the use of emerging technologies, Internet of things and blockchain.

II. PRESENTATIONS AND DISCUSSIONS

A. Meeting on Internet Governance and Cybersecurity Nexus - Promoting Trust in Cyberspace

1- Opening Session

8. The opening included statements by the main organizers of the meeting, namely ESCWA, the League of Arab States and the Lebanese Ministry of Telecommunications, and a highlight on each of these statements is provided below.

9. Mr. Ayman El-Sherbiny, Chief of ICT Policies, Technology for Development Division (TDD), ESCWA gave a welcome statement in which he pointed to the high importance dedicated by ESCWA to the area of technology for sustainable development in general, and highlighted the existing collaboration with various stakeholders and organizations in the Arab region for the aim of fostering the use of digital technologies for sustainable development at the national and regional levels. These partnerships cover many development processes, which include the Arab IGF process that has emanated from the established partnership between ESCWA and the League of Arab States and the joint initiative on Arab Dialogue on Internet Governance (ArabDIG).

10. The opening statement of ESCWA was delivered by the Acting Deputy Executive Secretary, Ms. Rola Majdalani, who pointed to the high importance that ESCWA puts on the topic of Internet governance and cybersecurity and on the overall topic of technology for development that affects all economic sectors and stakeholders' groups and is part of our daily life. She has further emphasized the importance of the topic in various areas of work of ESCWA on social and economic development; and the key role of technologies in areas of knowledge society, natural resource management, and in addressing the global challenge of climate change that needs monitoring and the use of advanced and frontier technologies, such as Artificial Intelligence. She has commended the strategic partnership with the League of Arab States on various development activities, including the partnership on Internet governance for the Arab region.

11. The statement of the League of Arab States was delivered by Mr. Khaled Fouda, Director for ICT Development, who started by extending appreciation to ESCWA for hosting the event at the start of a second round of the Arab IGF process, after a two-year cessation of its activities, the Egyptian National Telecom Regulatory Authority (NTRA) for serving as the Arab IGF Secretariat, and to the Lebanese Ministry of Telecommunications for their continuous support to the umbrella organizations and the Arab IGF process. The widely based Internet systems that rely on inputs and interactions of various stakeholders from all economic sectors makes the topic of Internet governance a global issue that started with the the World Summit of Information Society in 2005 and the formation of the global IGF. The area of Internet governance has also extended to be addressed at the regional level, which has led to the start of partnership between ESCWA and the League of Arab States in 2009 through the preparation for an Arab roadmap for Internet governance; and this partnership has led in 2012 to the formation of the Arab IGF under the joint umbrella organizations of ESCWA and League of Arab States. He emphasized the importance of dialogue and engagement of all stakeholders, including governments, private sector, academia and technical community, and civil society organizations, for the formulation of policies and governing plans for the Internet.

12. On behalf of the Minister of Telecommunications in Lebanon, Mr. Mohamed Chaaban, Advisor to the Minister and Member of the Ministry’s Owners Supervisory Board, delivered a statement in which he briefed the audience on the status of telecommunications sector and the various projects underway in Lebanon, and

linked the efforts with the regional ones on Internet governance. Considering the telecommunication sector as booming in Lebanon, he elaborated on the progress made on few strategic projects, such as the FTTX project that would result in few years with a wide spread connectivity to all customers and all stakeholders throughout Lebanon; the 3G and 4G service improvement plan, and the 5G service. These projects entail the big and borderless data and raise the importance of cybersecurity that constitutes a key aspect for all users and goes beyond the country level and would subsequently raise the need for having protection measures from cyberattacks.

2- Setting the Scene: Internet Governance, Cyber Security and Trust

13. This session aimed at showing different perspectives and contextualizing the topics of Internet governance, and cybersecurity nexus and the need for promoting trust in cyberspace; and has included briefings on the following: 2018 IGF on Internet of Trust; Preparations for the Fifth Arab IGF and the efforts of its Working Group on Cybersecurity; and the "Paris Call for Trust and Security in Cyberspace". A summary of each of the briefings is provided below.

14. Mr. Chengetai Masango, Senior Advisor to United Nations Secretary General High-level Panel on Digital Cooperation, gave a briefing on the 13th IGF “Internet of Trust” (Paris, November 2018), starting with a highlight on the evolution of the global process and envisaged improvements from the 2018 Paris round that has featured the participation of the UNSG and the French president who called for stronger cybersecurity and for a multidisciplinary approach that goes beyond the multi-stakeholder approach to involve all sectors and engage and include the weak or missing voices in the Forum. The aim is to promote accessibility for all people, especially the underserved, and strengthen the IGF in building trust in cybersecurity and cyberspace and in monitoring progress on its subthemes that include, among others, gender and youth. Messages from national initiatives on Internet governance considered that security and trust go hand in hand and need cross-sectoral approach to be tackled. He also indicated that the newly formed IGF multi-stakeholder advisory group includes three members from the Arab region, from Sudan, Tunisia, and United Arab Emirates; and that the 2019 IGF will be held in Berlin, while pointing that the hosting mainly relies on the offers received and it was not intended to be held in European countries. Furthermore, the efforts to go beyond messages in the outcome of the IGF was considered an important development in the IGF towards having a continuous process and a natural flow of work between annual meetings.

15. Representing the Arab IGF Secretariat, Ms. Christine Arida, Executive Director of Telecom Services and Planning, Egyptian NTRA, delivered a presentation entitled Updates on Preparations for the Fifth ArabIGF (in Arabic), in which she briefed on the main steps in the preparations, including the following: Formation of a new Advisory Group for developing a programme for the Forum; Convening of open consultations, a meeting for the Executive Bureau for Joint Coordination, and a meeting for the Multi-stakeholder Advisory Group; Identification of five thematic and two cross-cutting topics for the Forum, together with a number of potential slogans for consideration during preparations; Identifying a preliminary structure of the Forum that extends over two-three days and includes plenary sessions, workshops, and a pre-event for capacity building on Internet governance and its topics; Forming seven working groups to enable collaboration amongst the members on the various themes and preparatory efforts for the Forum; and revising the ArabIGF mailing list - list@igfarab.org, and official web site <igfarab.org>.

16. With cybersecurity and trust as a strategic theme in the Fifth ArabIGF and for which a working group was formed, Mr. Adel Abdel Sadek, the coordinator of this group has provided a briefing on cybersecurity from the global perspective and in the context of preparations for the Fifth Arab IGF. group's efforts and an intervention on the relationship between the economy and the national strategy of cybersecurity. Cybersecurity is gaining more importance in the Arab region in light of the high increase in cyber-attacks and the pressing need to protect infrastructure and private data, to address the security challenges of artificial intelligence and Internet of things, and to fight cybercrimes and cyberwars. Also, the need was raised to formulate and update legislations, increase awareness and capabilities, and guard from the different types pf cyberattacks.

17. Entitled "Under the bonnet of the Paris Call for Trust and Security in Cyberspace,” the presentation of Mr. Vladimir Radunovic, Director of e-Diplomacy and Cybersecurity Programmes, DiploFoundation, provided a briefing on the 2018 IGF, held at UNESCO in Paris, that has featured the launch by the French President of a high-level declaration on developing common principles for securing cyberspace. The "Paris Call for Trust and Security in Cyberspace" builds on the WSIS Tunis Agenda's definition of the "respective roles" of states and

other stakeholders, and resonates with the UN Group of Governmental Experts reaffirmation that international law applies to cyberspace.

18. The Paris Call invites for more regulations and security, strengthening the rules through more government engagement in work, and increased involvement of the private sector; and it was signed by many which shows willingness to cooperate with governments in the area of cybersecurity and accepting their shared responsibility. The declaration calls to support victims both during peacetime and armed conflict, reaffirms Budapest Convention as the key tool for combating cybercrime, recognises the responsibility of private sector for products security, and calls for broad digital cooperation and capacity-building. It invites signatories to, among other, prevent damaging general availability or integrity of the public core of the Internet, foreign intervention in electoral processes, ICT-enabled theft of intellectual property for competitive advantage, and non-state actors from 'hacking-back'. The Paris Call has received strong initial support from hundreds of signatories, including leading technology companies and many governments. Yet the USA, Russia, and China are missing. The declaration and its effects will be discussed again during the Paris Peace Forum in 2019, as well as during the IGF 2019 in Berlin.

19. During discussion, participants highlighted the need to build capabilities in the Arab region to have measures for protecting people and private data, and to have authentication to verify online identify through digital identification. The Paris Call was perceived as a building block for partnerships, and the topic of cybersecurity was perceived as a means for engagement of all stakeholders, especially that the major players are getting involved.

3- Legal and Regulatory Frameworks in Selected Arab Countries

20. Speakers in this session addressed the legal and regulatory frameworks of cybersecurity in their countries, and the presentations covered Lebanon, Syrian Arab Republic, Sudan, Yemen, Palestine and Algeria. Briefings on the presentations are provided below.

21. The legal aspects pertaining to cybersecurity and trust in cyberspace in Lebanon - with status, gaps, and aspirations - were addressed in a presentation by Mr. Bilal Abdallah, President of Legal Informatics Centre, Lebanese University, Lebanon. The wide use of Internet and its services was not risk-free, with misuse and use for criminal purposes, and has raised legal challenges related to security of information, private data protection, and electronic transactions. In 2018, Lebanon has adopted the law no. 81 for electronic transactions and personal data, to support cybersecurity and building trust in cyberspace. Before this law, reliance was on the clauses for technological developments in existing laws, such as laws for managing stock exchange, protection of cultural heritage, privacy of information, and financial processes through digital means. Few proposals were raised during the presentation, namely: Updating national legislations based on developments in ICTs, Strengthening cooperation towards having an Arab Agreement on Cybersecurity; Raising awareness and capabilities on cyber-risks and cybersecurity; and Forming a council for personal data protection that keeps up with technological developments.

22. A presentation on cybersecurity legal and regulatory frameworks in the Syrian Arab Republic (in Arabic) was delivered by Ms. Fadia Soliman, General Director, Syrian National Agency for Network Services (NANS); and it covered the national cybersecurity laws, namely the laws for e-signature and network services, e-transactions, protection of intellectual property rights and other rights, and online communication and fighting cybercrime. These laws would help in facing the challenges with the transition towards a knowledge-based society. The presentation also covered the draft laws for protection of personal data, and the right to access information. Furthermore, national control systems were put in place to support law implementation. A national information security policy was prepared, a cybersecurity department was formed in the Ministry of Interior, and a centre for information security was formed in the national authority for network services. Procedures are underway for the completion of information systems for electronic documents, and a training programme was prepared for legal system on facing cybercrime, and a special court was designated for cybercrimes.

23. The experience of Morocco - from building trust in cyberspace to developing cybersecurity (in Arabic), was presented by Mr. Belaid Nouar, Head of Telecommunication Affaires, Ministry of Industry, Investment, Trade and Digital Economy, Morocco. The briefing covered the ICT use, industry and infrastructure in Morocco, the laws enacted and the governing bodies working on building capabilities and trust in cyberspace, as well as the national strategy for cybersecurity that aims at establishing the enabling environment for cybersecurity and building trust in the digital economy. The country has witnessed an increase in investments

in ICT together with the creation of more jobs and focuses on four areas of work within its national strategy for cybersecurity, namely: Assessing threats, protecting vital information systems for institutions and infrastructure, strengthening the basis for secure information systems and promoting national and international cooperation on cybersecurity.

24. A briefing on the Law for Combating Cybercrime in Sudan (in Arabic) was provided by Mr. Sudad Ismaeil, Manager of Coordination and Foreign Relations Department, National Information Centre. The presentation outlined the laws that support ICT and e-transaction and e-signature, and elaborated on the laws for fighting cybercrime and the national information security policy. The cybersecurity law was issued in 2007 and resulted in 2017 with a specialized court for cybercrime, cybercrime police, and criminal investigation laboratories for analysis and proof of information crimes.

25. A presentation on Managing Social Media Cybersecurity in Sudan (in Arabic) was delivered by Mr Tarig Alameen, Head of Digital Forensic Department, Telecom and Post Regulatory Authority, Sudan, in which the speaker overviewed the risks on security and privacy on social media platforms and outlined the main actions taken by Sudan CERT (Computer Emergency Response Team) to protect users from these risks. Activities included capacity building programmes and raising technical capabilities to respond to reports of cybercrime.

26. A briefing on Cybersecurity in Yemen – situation and prospects (in Arabic) was delivered by Mr Abduljalil Alkubati, Vice Manger of Internet, Public Telecommunications Corporation, Yemen. The country faces high risks for cyberattacks and has limited technical capabilities for facing them; and it needs to develop its infrastructure and form a CERT to respond to risks of cybersecurity and cybercrime. The first cybersecurity conference in Yemen was held in 2014, following which a national centre for cybersecurity was formed, and a number of related laws were formulated, including laws for cybercrime and for protection of personal data.

27. Cybersecurity in Palestine (in Arabic) was the subject of an intervention by Mr. Mohammed Midani, Manager of Internet and Digital Content, Ministry of Telecom and Information Technology, Palestine. The speaker highlighted the main activities of the Ministry for a safer use of the Internet by the government entities and general users, and these include the formation of a national CERT in 2015, and the monitoring and protection of public records, as well as raising awareness and enabling a legal environment that could govern the use of Internet.

28. A presentation on the Legal and Regulatory Framework of Cybersecurity in Algeria (in Arabic), was delivered by Ms. Wassila Chamekh, Deputy Director of Standardization and Information Society Watch, Ministry of Post, Telecommunications, Technologies and Digitalisation, Algeria. The speaker covered the most important cybersecurity laws and regulations, covering: Child protection, e-commerce, rules on prevention of offences through the use of ICTs, protection of personal data, electronic signature and e-certification. These include the 2009 laws for protection from use of ICTs, media and communications, the 2018 laws that govern the use of email and online commination and e-commerce, and the 2019 law that regulates the work of the national authority for protection from crimes related to use of ICTs.

4- Insights on Cybersecurity

29. Over two morning sessions, speakers gave insights on cybersecurity in conferences, programmes and conventions, and recaps were given on the 2018 Munich Cybersecurity Conference, ITU 2018 plenipotentiary conference, and regional efforts towards cybersecurity conventions.

30. The recap on Munich Cybersecurity Conference (MSC) was provided by Mr. Leonhard Simon, Project Manager, MSC Foundation, Germany. It covered the governance of cybersecurity norms and addressed the technical and political perspectives for cyberspace and highlighted the need for efforts of stakeholders to set cyber standards. The speaker put forward two recommendations, namely (i) Promoting trust in cyberspace through responding to public needs and their questions on digital life; and (ii) Establishing multilateral agreements on stability and security that would join efforts and widen trust in cyberspace.

31. The Director of ITU Arab Regional Office, Mr. Ebrahim Alhaddad, briefed the meeting on the outcome of the ITU 2018 plenipotentiary conference and highlighted the importance of the topic of Internet governance and cybersecurity in the digital transformation of societies. He further pointed to the ITU decision number 130 that aims at building confidence and security in the use of ICTs and includes proposals for raising awareness

and building capabilities to face the challenges, recognizing the roles of the private sector, technical community, individuals and organizations, and promoting cooperation between the ITU and other organizations.

32. A presentation on the regional efforts towards cybersecurity conventions was delivered by Ms. Mona Jabour, Law Professor, Lebanese University, & Founder of Pan-Arab Observatory for Cybersecurity, Lebanon. The threats in the landscape of cyberspace are both technical and legal and require changes at various levels; and the responsibility of improving security and stability of cyberspace is shared by various stakeholders and sectors, each in their roles. Reference was made to the Paris Call with emphasis on the importance of development and application of international norms and laws, and of the need for a responsible behaviour of all actors/sectors in their implementation. For the Arab region, a draft Convention for Cybersecurity is under review and it proposes the establishment of an Arab organization for cybersecurity; and this convention was prepared based on the need for a binding agreement to harmonize laws and commit countries to cooperate for the aim of cybersecurity and protection of personal information.

5- Cybersecurity and Trust in the Arab Region

33. This session has tackled the topic of Cybersecurity and Trust in the Arab Region and included presentations on the legal framework for cybersecurity, cybersecurity efforts and programmes, counter cybercrime and digital forensics efforts, and cybersecurity threats in the age of big data and fourth industrial revolution. Briefings from this session are provided below.

34. The legal framework for cybersecurity in the Arab region was outlined by Ms. Janane el-Khoury, Chief of Legal Department, Legal Informatics Centre, Lebanese University, Lebanon. In the digital age, the Arab people have the right to benefit from technologies within a legal framework that protects their basic and human rights. The presentation covered the benefits and challenges facing the Arab region in the area of cybersecurity and profiled the existing legal frameworks that showed few countries having specialized legislations for e-transactions, e-commerce, intellectual property rights, protection of personal data and cybercrime. It also addressed cybersecurity contracts, national sovereignty and cross-border security challenges, and proposed the application of best practices and the development of legal, executive and capacity building programmes.

35. The perspective of the League of Arab States on cybersecurity and its related regional initiatives was outlined by Mr. Khaled Fouda, Director for ICT Development, League of Arab States, Egypt. A briefing was made on the various activities, initiatives and projects that were approved by the Arab Council of Ministers of ICT and include the establishment of the Arab Regional Cybersecurity Centre (ARCC) in Oman in collaboration with the ITU. The steps taken for promoting cybersecurity and trust in cyberspace was also outlined, together with the main achievements be selected Arab countries that can be extended to other countries.

36. A presentation on the cybersecurity programme at the ITU was delivered by Ms. Rouda Alamir Ali, Programme officer, ITU Arab Regional Office, Egypt, which outlined ITU mandate and coordinated response on cybersecurity, the 2018-2021 plan of action on the Arab Regional Initiatives that include an initiative aimed at promoting confidence and security in the use of telecommunications and ICTs, child online protection, and combatting cyberthreats and misuse of ICTs. It also covered the ITU global cybersecurity index (GCI) and the way countries can improve their positions, and the 2018 ITU guide to develop national cybersecurity strategies[1].

37. On Supporting Counter Cybercrime and Digital Forensics Efforts in the Middle East and North Africa, Mr. Patrick Boismenu, Cybercrime Expert, United Nations Office on Drugs and Crime (UNODC), Tunisia, briefed participants on the regional experience of UNODC that supports fighting cybercrime. The problem lies when national legislations cannot respond cybercrimes that goes beyond borders; and this needs cooperation between countries to face the challenges of cybercrime and take counteractions. National law enforcement systems need to investigate and respond to cybercrimes using digital forensics, and countries need to go up the ladder to address cybercrime challenges online. A practical demo was run for a 2019 project that shows how law enforcement agencies communicate using simple least significant bit techniques.

38. In a presentation on cybersecurity threats in the age of big data and fourth industrial revolution, Mr. Fadi Salem, Director of Research and Advisory, Mohammed Bin Rashid (MBR) School of Government, UAE, briefed on the main findings from a regional survey and various research reports covering digital transformation in the Arab region, on cybersecurity, smart cities, use of social media, and public services. The region has

[1] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

societal datafication with wider penetration of Internet, broadband, mobiles, and social media, and growing Internet of things devices; and this creates a hybrid ecosystem of data that feeds into algorithms and tools and enables more options for cybersecurity threats. The region has weakness in awareness and behaviours related to these threats and their conceptualization; and people face cyberthreats and are concerned about digitization, yet most do not follow secure behaviours online. The speaker outlined the main public concerns about the Internet, Internet of things and artificial intelligence in the region, with the highest concerns going for cyber-terrorism, cyber-crimes and cyber-bullying as well as for privacy and safety. The policy responses to threats from public perspective was in three dimensions: transparency of data and data use, personal control of data, and regulation of data.

39. Discussions tackled a number of areas related to cybersecurity and responding to cyberthreats, covering, among others: The role of Arab IGF in the linkages between cybersecurity and Internet governance and the potential engagement in international cybersecurity processes; and this needs more engagement of experts from the legal dimension of cybersecurity in the Internet governance dialogue. Participants raised the need for supporting countries in fighting cyberthreats and facing the cross-border challenges and not only through capacity-building programmes.

6- Cybersecurity and Internet Economy

40. This session examined cybersecurity and Internet economy causality and correlations, and included presentations on the governance of digital money, trust and security in the adoption of emerging technologies and Internet economy, economic and social impact of information technology security, legal framework for electronic transactions and trust, and cybersecurity and Internet economy. Briefings on this session are provided below.

41. A presentation on governance of digital money, with focus on stability of next generation financial sectors, was given by Mr. Michael Palage, CEO, Pharos Global, USA. It covered the evolution of "digital money" and the history of other forms of payment that are not based on physical currency. The significant changes in financial services with the Internet, mobile payments, and other new technologies, have significantly impacted the financial sector and its supporting ecosystems. The new technologies of blockchain/ distributed ledger technology (DLT) allow financial services to extend to the unbanked and provide new approaches to digital identity that improve security and privacy. However, these technologies are not risk-free and would need a proactive public-private collaboration to ensure protection of consumers financial services.

42. The topic of trust and security implications in the adoption of emerging technologies and Internet economy was covered by Mr Hafedh Yahmadi, Professor, Tunisia Business School, Tunisia. While the world connectivity is expected to grow beyond imagination, people and devices would be leaving traces of information in many places; and this would widen the scope of data collection and challenge the implementation of data collection policies. Threats to privacy and data security would also be vast and require responses from the social and economic angles rather than the technical ones. Covering trust, privacy and security effects of emerging technologies, corporate management, digital transformation and cyber-risks, and the corporate governance of data, the presenter stressed the importance of public-private partnerships in managing cybersecurity, and the institutionalization of data governance coupled with new data reforms.

43. The economic and social impact of information technology security was addressed by Mr. Qusai AlShatti, Board Member, Kuwait Information Technology Society. The presentation covered the conduct in cyberspace, types of cyberthreats and their impact on society, authorship of cyber-attacks, statistics of cybercrimes and their occurrences, major risks of information technology security, new trends in cybercrime. It also included a number of proposed remedies that include sharing information, reporting on incidents, making security the responsibility of all, training and educating on it, keeping up with security developments and best practices, apply security regulations and culture with frequent security testing.

44. A presentation on the legal framework for electronic transactions and trust was delivered by Mr Wassim Hajjar, Judge Supervisor of the Information Technology Unit, Ministry of Justice, Lebanon. The speaker overviewed the legal-economic linkages and the importance of verification of online identity in the digital economy. An example was the use of credit cards online for e-transactions that entails a risk of un-rightful access to the databases that keep records. The recommendations include, among others: updating legislations to suit the digital economy, facilitating access to law enforcement to respond to conflicts, setting international

legal agreements aimed at coordinating efforts, harmonizing legislations, and responding to threats, raising awareness of users, and maintaining technical neutrality of legislations and updating it regularly.

45. The conception of a paper on cybersecurity and Internet economy (in Arabic) was presented by Mr Adel Abdel Sadek, coordinator of the Arab IGF Working Group on Cybersecurity and Trust, in which he overviewed the relationship between economy and security in light of digital transformation and the motives for developing national strategies for cybersecurity. The tendency of practicing sovereignty on cyberspace resources was addressed, together with application of cybersecurity economies in the context of national cybersecurity strategies (NCCSs). The paper would also cover the challenges facing governments in setting policies for cybersecurity; and it would address the efficiency of investments in cybersecurity and its economic impact on national cybersecurity strategies. These strategies would contribute to enhancing confidence and securing a digital environment that enables growth and progress. The importance of integrating the economic and political dimensions in addressing cybersecurity was stressed, towards having effective national public cybersecurity policies.

46. Participants stressed the importance of education, skills, and the existing financial sector in the linkages between cybersecurity and Internet economy, where emerging technologies are disruptive and transformative. A key aspect linking cybersecurity to economic development is the trust between users and products, and citizens and the government. Furthermore, data governance and the balance between control and openness in economy are important aspects affecting development and allowing new dynamism in the economy.

7- Citizen's Trust in Fintech and Digital Transactions

47. This session included a number of interventions under the overall title of Citizen's Trust in Fintech and Digital Transactions, and covered the following: the Arab cybersecurity landscape, cybersecurity and cryptocurrencies from the Lebanese perspective, digital financial inclusion and digital fiat currencies, cybersecurity concerns in the Arab region, Internet of things security and consumer trust, and the digital identity and trust frameworks. Briefings from this session are provided below.

48. The challenges and opportunities in the Arab cybersecurity landscape were overviewed by Mr. Amro Moussa, Advisor to the Minister of Communication and Information Technology, Egypt, in which it was emphasized that the challenges of cybersecurity are multi-disciplinary and need an ongoing operational risk management framework to face its threats. The challenges are related to information security and cybersecurity strategy, awareness and education, collaboration, corruption, legal and regulatory ecosystem, and leadership; and the opportunities are related to job creation, trusted online platforms for digital economy, security protection, trusted services and a security digital society.

49. A presentation on cybersecurity and cryptocurrencies from the Lebanese perspective was delivered by Mr. Ali Nahle, Senior Executive Director, Banque Du Liban, Lebanon, in which he pointed to the increased threats on Internet with the widespread of networks, which necessitates continuous coordinated efforts for ensuring security of systems that would support the laws, such as the Lebanon e-transaction law. The Central Bank has recently prepared a roadmap for digital transformation with a digital bank identify coupled with a digital currency that runs in parallel and complements the Lebanese pound. The Lebanese digital currency is expected to allow instant payments and help a faster and safe use of the currency; and it requires authentication together with a category of management of the payment process.

50. Addressing digital financial inclusion and digital fiat currencies, Mr. Ahmed Said, Consultant, ITU Arab Regional Office, Egypt, delivered a presentation that stressed the need for digital financial inclusion and the roles of telecommunication and financial regulators in coordinating their efforts towards facing the various security challenges in expanding the use of mobile banking. The speaker covered the regulatory and security challenges in the use of digital fiat currencies together with the underlying opportunities, and has further shed light on the conceptualization of a study that will address digital financial inclusion in the Arab region.

51. An overview of a planned survey on Consumer Perceptions on Trust in e-transaction in the Arab region was delivered by Mr Fadi Salem, Director of Research and Advisory, MBR School of Government, UAE. Collaboration on this survey is open and it needs a unified definition of e-transactions and commitment of partners to distribute and solicit responses to the survey.

52. The subject of critical advances in Internet of things Security and Consumer Trust was addressed in a presentation by Mr Hosein Badran, Consultant, Canada, which started by stressing the importance of protection of privacy in the use of smart devices as they are subject to hacking. The speaker briefed on the outcome of a 2018 survey by the Internet Society on policy in Asia-Pacific, and listed the clear risks that include consumer security, privacy and safety that are undermined by the vulnerability of devices, and the rising risks in wider economy and increased use of insecure devices. Furthermore, the different certifications for consumer security and the key considerations for smart devices and their labels. Few recommendations were proposed for the Arab region to be ready for higher cybersecurity risks, and these include: establishing the role of privacy commissioner to protect and promote privacy rights; strengthening consumer protection agencies; raising awareness and capabilities on Internet of things device testing and certification.

53. In a presentation on digital identity and trust frameworks, Mr Michael Palage, CEO, Pharos Global, USA, shared foundational documents and stressed the need for increased digital identify and trust, and the protection of consumers from fraud and identify theft. With various initiatives related to digital identity there are significant challenges in the technical and governance interoperability, which requires a global framework for governance of digital identity systems. Few ideas were raised for the Arab region, which include, among others: securing the rights to operate the. arab Top Level Domains (TLDs) and using it as a platform for cross-border use of digital identities in conjunction with regional ccTLD managers; establishing digital identify framework and credentials for both natural and legal persons, with natural persons being anonymized.

B. Arab Regional Dialogue Meeting of the Arab Multi-stakeholder Programmmme Advisory Committee

54. A meeting for the Arab IGF multi-stakeholder programme advisory committee (AMPAC) was held jointly with the meeting on Internet governance and cybersecurity, in an effort to engage the committee members in the thematic dialogue that covers the strategic priority areas identified in the Second Arab Roadmap for Internet Governance[2]. The committee that was formed during the previous meeting (Beirut, July 2018) has continued the efforts on preparations for the Fifth Arab IGF, planned to be held in 2019. The AMPAC meeting was held over three sessions and has reviewed the progress made on hosting the Forum and on the efforts of the thematic and operational working groups from the previous meeting. A briefing on the main content of this meeting is provided below, and the Committee's report (in Arabic)[3] is available through the Arab IGF website.

55. The importance of participation in the forums that contribute to developing the ICT sector in the Arab region, including the Arab IGF, was emphasized considering their open dialogue and non-binding nature of their resulting messages on the issues of priority for the region. The importance lies in the envisaged role of these forums in advocating for policies and strategies in the region and promoting collaboration on the areas of priority. The Forum messages get presented to the technical secretariat of the Arab Council of Ministers of ICT and its specialized working groups and would support regional efforts on policy- and strategy-making in the Arab region; and this contribution was recognized in the outcomes of the 21st and 22nd rounds[4] of the Council in 2017 and 2018.

56. The coordinators of thematic working groups briefed the committee on the progress made in the preparations for the plenary sessions of the Forum; and these covered the five main themes and three cross-cutting topics listed below, which were identified in the previous committee meeting:

Main themes

(1) Meaningful access for inclusion and diversity;
(2) Cybersecurity, privacy, trust and peace;
(3) Digital transformation and Internet economy;
(4) Institutional empowerment and engagement in Internet public policy-making at global and regional levels;
(5) Social and human impact.

Cross-cutting topics

(i) Gender equality and women empowerment
(ii) Human development and capacity-building
(iii) Legislative frameworks

[2] Arab Roadmap for Internet Governance – Second edition

[3] Report can be accessed through the link: http://igfarab.org/UploadedFiles/News/Images/meeting-report-2019.pdf

[4] Report of the 22nd Round, page 26, and Report of the 21st Round, page 31, of the Arab Council of Ministers of ICT.

57. The working groups conducted side meetings to continue their efforts on the thematic plenary sessions and to fine-tune the sub-themes of each; and the members agreed to postpone the identification of speakers for these sessions until the host is identified, in order to include potential speakers from the hosting country. Furthermore, emphasis was put on the need to consider the representation of all stakeholder groups, and to increase the participation of women and youth in the speakers in order to have an added value and diversity in addressing the various themes. A list of potential speakers from the Arab region and beyond, on the themes of the event, would be prepared in order to later assist on the identification of speakers.

58. The operational working groups covered the community workshops, fellowship programme and the capacity building pre-event of the Fifth Arab IGF; and the work of these groups is dependent on the identification of the host country and dates, following which their related work processes can be initiated and the hosting entity can be engaged in the preparations.

59. For hosting the Forum, the umbrella organizations, ESCWA and League of Arab States, are contacting the entities that has expressed interest in hosting the Fifth Arab IGF, and a proposal was raised to convene the annual meetings in either of their premises in either Beirut or Cairo. Furthermore, the role of committee members was considered important in inviting national sectors to participate in the Forum and potentially encouraging various stakeholders to host the event.

C. Consultations on the Way Forward

60. The last session of the meeting was dedicated to consultations on the way forward, in which the organizers and participating experts discussed the sustainability of the Arab IGF, the Arab perspective on the Paris Call for Trust in Cyberspace and reviewed the compiled recommendations for the meeting.

61. Reflections on Arab IGF and its relationship with the Paris Call considered that the latter as a call by countries to develop regulations for cyberspace to avoid cyberwars. The Arab region have a similar situation to the global one and need to cooperate on cybersecurity to resolve conflicts in the cyber domain. While the Paris Call is taken as a white paper without precautions and the reactions of governments and other stakeholders to it are not clear, the 13-year IGF process relies on the multi-stakeholder and multi-sectoral approach; and it was advised not to have a fast stand on the call, but rather read and seek clarifications on its overall path that would be addressed in the 14th IGF planned for Berlin in 2019.

62. A list of 40 recommendations (in Arabic) were gathered from the participating experts and were reformulated after the meeting to allow categorization and avoid duplications; and the revised list was shared with participants for further input before finalization and inclusion in Annex I of this report.

D. PARTICIPATION

63. The meeting was attended by 47 experts, 23 per cent of them women, from 14 countries in the Arab region and beyond, and participants were from various stakeholders - Governments, Business Sector, Civil Society Organizations, Technical Community and Academia, and International and regional organizations. The participants from the Arab region included representatives from Algeria, Egypt, Iraq, Jordan, Kuwait, Lebanon, Morocco, Oman, Palestine, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen.

Annex 1:

Outcome - Recommendations (in Arabic)

التوصيات من اجتماع الحوار الإقليمي العربي واجتماع الخبراء حول ترابط حوكمة الإنترنت والأمن السيبراني – تعزيز الثقة في الفضاء السيبراني (بيروت، 4-7 كانون الأول/ديسمبر 2018)

خلال جلسات الحوار الإقليمي العربي وضمن اجتماع الخبراء حول ترابط حوكمة الإنترنت والأمن السيبراني - تعزيز الثقة في الفضاء السيبراني الذي عقدته الاسكوا في مقرها في بيروت من 4 إلى 7 كانون الأول/ديسمبر 2018، عملت منظمتي جامعة الدول العربية والإسكوا على استشراف مدخلات المشاركين للمساهمة في جمع هذه التوصيات. ولما كان من الصعب مناقشة هذه المدخلات خلال الاجتماع، فقد عكفت المنظمتين على جمعها وتنقيحها وإخراجها بالشكل المناسب، ومن ثم تعميمها على المشاركين وأخذ الملاحظات بشأنها لإخراجها في صيغتها هذه. تعتبر هذه التوصيات جزء لا يتجزأ من هذا التقرير ومكمل له:

تطوير الإطار التشريعي في الدول العربية:

1. وضع إطار استرشادي إقليمي للتشريعات الخاصة بمكافحة الجريمة الالكترونية.
2. تعزيز الأطر القانونية ومراجعة القوانين الخاصة بأمن نظم المعلومات ومكافحة الجريمة الالكترونية وإدارة الأدلة الرقمية في المنطقة من أجل مواءمتها /توحيدها في الدول العربية، وبهدف تعزيز التعاون الدولي في هذا المجال
3. سن القوانين والتشريعات اللازمة لتنظيم العلاقة مع الشركات العالمية (الشركات متعددة الجنسيات).
4. النظر في إنشاء محاكم وطنية وإقليمية متخصصة لسرعة البت في جرائم المعلوماتية.
5. انشاء هيئة أو مرجعية عربية (Regional Center) فيما يخص (Cyber Security) يناط بها وضع الأنظمة والتشريعات والقوانين ذات العلاقة وتنسيقها في البلدان العربية لمعالجة التفاوت الموجود بين البنود والنصوص فيما بين البلدان العربية (مما قد يؤثر على حرية التعبير أحيانا).
6. إنشاء مرصد (افتراضي) ليكون بمثابة مرجع واف للقوانين الوطنية والقرارات الرسمية في مجال الأمن السيبراني ومكافحة الجرائم باستخدام تقنية المعلومات، وكذلك الاتفاقيات الإقليمية العربية والدولية في هذا الشأن.
7. وضع الأطر التشريعية المناسبة لحماية بيانات المواطنين والأفراد، والنظر في إطلاق الحوار حول دور الذي يلعبه "مفوض الخصوصية" المستقل.

التعاون الإقليمي والدولي:

1. ضرورة وضع استراتيجية عربية موحده للأمن السيبراني، والترويج لثقافة عربية للامن السيبران، تتضمن:
   - انشاء منظومة عربية لتوحيد أطر تصنيف Data classification framework
   - انشاء منظومة عربية لتوحيد أطر واجراءات و ضوابط "آليات التسجيل و اكتشاف الاختراقات
   - انشاء منظومة عربية موحدة ل تحديد معايير أمن المعلومات و معايير الأمن السيبراني الواجب الالتزام بها في كل قطاع من قطاعات البنية التحتية الحرجة " Compliance framework " و انشاءلائحة ترتيب عربية " Compliance Scoreboard
   - انشاء منظومة عربية لتحليل وادارة المخاطر التشغيلية لتكنولوجيا المعلومات " IT Operational Risk Framework " و توحيد الأطر والضوابط و الاجراءات المستخدمة
   - رسم أطر عربية ل مكافحة عمليات "النصب الرقمي" و تحديد أطر تحديد "المسؤولية الرقمية" وتحديد المنظومة المؤسسية وفصل السلطات لاستخراج "الدليل الرقمي العربي" و أطر استخراجه و تداوله و ذلك باستخدام هوية رقمية وطنية لكل دولة في اطار عربي متكامل
   - اهمية التعاون الإقليمي والدولي من اجل تعزيز الحماية والامن في الفضاء السيبراني والنظر في إنشاء لجنة عربية للأمن السيبراني تضم خبراء من قطاعات الداخلية والعدل والاتصالات والإعلام
   - توحيد كل ما سبق ذكره في منظومة عربية متكاملة لل " الالتزام وادارة المخاطر والحوكمة " GRC Governance, Risk and Compliance"
2. تعزيز التعاون الإقليمي والدولي، بغية تعزيز الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، من أجل تخفيف المخاطر والتهديدات
3. إنشاء مراكز للأمن السيبراني على المستوى الأقليمي من أجل الكشف على الهجمات والتصدي لها بالإضافة إلى توفير بناء القدرات على المستوى السياسي لزيادة الوعي بقضايا الأمن السيبراني الدولي
4. من خلال المنتدى العربي لحوكمة الانترنت، إنشاء آلية فعالة ودقيقة ومتقنة للمراقبة والتحقق وضمان الامن السيبراني.
5. دعم المبادرات الدولية والإقليمية بشأن الأمن السيبراني، بما في ذلك مؤشر الأمن السيبراني العالمي (GCI)، من أجل تعزيز الاستراتيجيات الحكومية وتبادل المعلومات بشأن الجهود المبذولة في مختلف القطاعات.
6. تبني مسابقات عربية لمحاكاة عمليات الاختراق والدفاع السيبراني.
7. الطلب من الإسكوا بالاشتراك مع جامعة الدول العربية العمل على جمع المعلومات وإنشاء خارطة للمؤسسات المعنية بتعزيز الثقة والأمن في الفضاء السيبراني والعاملة في المنطقة العربية (بما في ذلك المؤسسات الوطنية، والمنظمات الدولية والإقليمية، وشبكات التنسيق الإقليمية، مراكز الأبحاث والجامعات المختصة، ومؤسسات تنمية القدرات ذات الصلة)، وتشمل هذه الخارطة معلومات أساسية حول دور كل من هذه المؤسسات ومعلومات مرجعية حول نطاق عملها.
8. أهمية تعزيز دور الأمم المتحدة في مجال الأمن السيبراني ، وإعداد وتطوير مجموعة من المبادئ الأساسية وتدوينها بوثيقة دولية/إقليمية خاصة بالأمن السيبراني من أجل حصر استخدام شبكة الأنترنت في الأغراض السلمية .
9. دعوة ITU لتوسيع نطاق حماية الأطفال على الإنترنت (COP) وتضمين المبادرة حماية الأطفال من المخاطر المحتملة من الأجهزة الذكية بما في ذلك الألعاب الذكية.
10. إعطاء دور للمنظمة العربية في التنسيق بين الدول العربية بخصوص الأمن السيبراني.

11. دعم اعتماد معاهدات واتفاقيات إقليمية ملزمة لإدارة قضايا الأمن السيبراني.
12. الموافقة على الاتفاقية العربية للأمن السيبراني.
13. اعداد اتفاقية عربية لتبادل المعلومات في مجال الأدلة الرقمية
14. تفعيل التعاون العربي من أجل مساعدة الدول العربية الواقعة تحت طائلة العقوبات بالحصول على أجهزة تسهل عمليات التحقيقات الرقمية والأمن السيبراني.
15. إنشاء صندوق أبحاث في مجال الأمن السيبراني (مدعوم من الشركات الخاصة الناشطة في مجال تكنولوجيا المعلومات والاتصالات) لتمويل المبادرات البحثية في المؤسسات الأكاديمية والتدريسية في المنطقة العربية (دعم البحث والتطوير المحلي في مجال الأمن السيبراني في المنطقة) ، ويعتمد في نظام حوكمته وآلياته أسس البحوث الوطنية في أوروبا وأمريكا الشمالية.
16. إصدار دعوة لـ "الهدنة السيبرانية" و "مدونة السلوك" في المنطقة العربية، لكي تلتزم الدول بوقف الأنشطة العدوانية في الفضاء السيبراني ضد بعضها البعض. مما يكون خطوة أولى وأساس "للتعاون" المستقبلي في مجال الأمن السيبراني في المنطقة العربية.
17. مناشدة جميع الدول العربية على الحرص على المشاركة فى اجتماعات وحوارات المنتدى العربى لحوكمة الانترنت حرصا على الفائدة العامة والانتفاع من المواضيع والقضايا المطروحة وخاصة المتعلقة منها بالأمن السيبراني.
18. دعوة الدول العربية إلى التأسيس لدور "مفوض خصوصية" يقدم تقاريره إلى البرلمان، تتمثل مهمته في حماية وتعزيز حقوق الخصوصية."
19. إعداد دليل عربي لتقديم الطلبات إلى الشركات المختصة في مجالات الاتصالات والإنترنت
20. اعداد قاعدة بيانات للشركات والمؤسسات والافراد التي تقوم بالتشجيع علي الجرائم الالكترونية عبر توفير البرمجيات الخاصة بالاختراقات والتجسس وإيجاد قوانيين ضد هذه الشركات والمؤسسات. ولربما تكون هذه الخطوة علي مستوى الأمم المتحدة وعلي مستوى الحكومات العربية

تطوير الأطر الوطنية:

1- تشجيع الشراكة بين القطاعين العام والخاص "PPP" من أجل استراتيجية فعالة في مجال الأمن السيبراني، وزيادة الوعي بين جميع أصحاب المصلحة، بما في ذلك المؤسسات والأفراد، بأهمية تعزيز الأمن السيبراني وتنفيذ الضمانات الأساسية، ومشاركة المعلومات حول الهجمات والتهديدات بين كافة أصحاب المصلحة والحكومة.
2- الطلب إلى الحكومات القيام بحملات توعية تهدف الى زيادة الوعي حول الجرائم السيبرانية واهمية الحفاظ على المعلومات والبيانات الرقمية للمواطنين وكيفية التعامل مع البرامج، وبناء القدرات في مجال الامن السيبراني
3- حث المؤسسات الإعلامية من فضائيات وغيرها أيضا بالقيام بدروها الفعال في نشر الوعي في المجتمعات في مجال الامن السيبراني
4- حث المؤسسات التعليمية دمج مواضيع الامن السيبراني في مناهج التعليم مما يسمح للطلاب التعامل مع المجمتع الرقمي آمن ومنتج وحر
5- المساهمة في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات على المستويات الوطنية، بما يضمن تنفيذ مخرجات ونتائج القمة العالمية لمجتمع المعلومات.
6- تشجيع الحكومات لزيادة الاستثمار في مجال الامن السيبراني
7- تحسين كفاءة الدول في استخدام خدمات مختبرات التحقيقات الرقمية ودمج واستخدام قواعد البيانات في التحقيقات الوطنية والإقليمية والدولية.
8- تحديث الاستراتيجيات الوطنية للامن السيبراني لتأخذ في اعتبارها الإبعاد الاقتصادية، وتطوير آليات العمل لمواجهة التحديات أمام نمو سوق الأمن السيبراني، وأدخال القطاع الخاص في تنفيذ هذه الاستراتيجيات واعتماد مؤشرات لقياس الكفاءه الاقتصاديه للاستراتيجيات
9- زيادة التعاون بين الأكاديميين والصناعات والحكومات للتمكن من إجراء بحوث دقيقة حول السوق السيبراني.
10- تقديم حوافز من جانب الدولة لتشجيع الاستثمارات في الأمن السيبراني.
11- أهمية تدخل الدولة ودورها في تنظيم سوق الأمن السيبراني وعدم تركه لحريه السوق.
12- مواجهة نقص البيانات حول سوق الأمن السيبراني بتشكيل هيئة مختصة.
13- العمل على دمج السياسة الصناعية في الأمن السيبراني في الاستراتيجيات الوطنية.
14- خلق ثقافة الالتزام بالقواعد الدولية للإنترنت واتباع الدول لهيئة واحدة تابعة للأمم المتحدة والتغلب على الانقسامات القائمة في العملية الدولية لوضع القواعد.
15- تضمين القواعد الدولية لبنود تمنع الجهات الفاعلة الحكومية وغير الحكومية العبث بالمنتجات والخدمات خلال عمليات التطوير والإنتاج، إذا كان ذلك قد يضعف إلى حد كبير استقرار الفضاء السيبراني.
16- ضمان أن تستطيع مراكز الاستجابات الوطنية في المنطقة العربية الاستجابة للممارسات السيبرانية الأوسع نطاقاً المتعلقة بالممارسات الناشئة للبيانات الضخمة والذكاء الاصطناعي على وجه التحديد.
17- تعزيز أدوار وكالات حماية المستهلك وتوفير وظائف تثقيف المستهلك والتوعية لأجهزة المستهلكين في إنترنت الأشياء ووضع ونشر "مدونة أفضل الممارسات لأمن إنترنت الأشياء في الوطن."
18- تطوير القدرات الوطنية والقومية في اختبار أجهزة إنترنت الأشياء (IoT) وإصدار الشهادات لها، والاستفادة من الجهود الدولية المستمرة (الاتحاد الأوروبي، المملكة المتحدة، كندا، أستراليا).
19- توفير المصادقة واستخدام التوقيع الإلكتروني وغيرها من التقنيات من أجل ضمان حماية محتوى البيانات والبريد الإلكتروني وضمان المعاملات والتصدي للأخطار التي تواكب استخدام التكنولوجيات الحديثة كإنترنت الأشياء، و Blockchain.

Annex 2:
List of participants

Algeria

Ms. Wassila Chamekha
Deputy Director on Standardization and Information Society, Ministry of post, Telecom, Technologies and Digitalization

Canada

Mr. Hosein Badran
Consultant

Mr. Patrick Boismenu
Cybercrime Programme Officer, UNODC

Egypt

Mr. Adel Abdel-Sadek Algakha
Founder & CEO, Arab Centre for Cyberspace Research

Mr. Ahmed Farag
Sr. Coordinator, ArabIGF Secretariat, National Telecom Regulatory Authority (NTRA)

Mr Ahmed Said
Consultant, ITU ARO

Ms. Christine Arida
Executive Director, Telecom Services and Planning, NTRA

Mr. Hazem Hezzah
IT Expert, League of Arab States

Mr. Hisham Aboulyazed
Sr. Manager, Information Society Affairs, NTRA

Germany

Mr. Leonhard Simon
Project Manager, Munich Security Conference Foundation

Iraq

Mr. Abdulilah Al-Dewachi
Former Regional Advisor on ICT, ESCWA

Jordan

Mr. Abdelhamid Al Rahamneh
Director General, Al Monsifoon Trading

Mr. Charles Shaban
Executive Director, Abu-Ghazaleh Intellectual Property

Lebanon

Mr. Ali Awdeh
Union of Arab Banks

Mr. Ali Nahle
Executive Director, Head of Information Technology, Banque Du Liban

Mr. Bilal Osman Abdallah
President of the Legal Informatics Centre, Lebanese University

Ms. Jeanane El Khoury
Chief of Legal Department at CIJ, Lebanese University

Ms. Manal Shihab
Senior Software Engineer, TRA

Ms. Mona Al-Achkar Jabbour
Head of Research Department, Lebanese University

Mr. Salah Rustum
CIEL/GlobalSign

Mr. Wassim Hajjar
Judge Supervisor of the IT Unit, Lebanese Ministry of Justice

Ms. Yvonne Sleiman
Head of International Relations & Maintenance Services, Ministry of Telecommunications

Ms. Zeina Bou Harb
Head of International Cooperation, OGERO

Morocco

Mr. Belaid Nouar
Head of Telecom Affairs, Ministry of Industry, Investment, Trade & Digital Economy

Ms. Fatna El Farsi
General Engineer Ministry of Administrative Reform and Civil Servant

Palestine

Mr. Allan Salahaldeen
Director of Projects & Technical Development, Ministry of Telecom and IT

Mr. Mohammed Midani
Manager of Internet & Digital Content Management, Ministry of Telecom and IT

Sudan

Mr. Sudad Mahmoud Hussein Ismaeil
Manager of Coordination & Foreign Relations, National Information Centre

Mr. Tarig Mohammed
Manage security in social media, Sudan Telecom and Post Regulatory Authority

Syria

Mr. Fadi Salem
Director of Research and Advisory, Mohammed Bin Rashid School of Government

Ms. Fadia Souliman
General Manager, NANS

Mr. Ibaa Oueichek
Expert, Syrian Virtual University

Ms. Rouda Alamir Ali
Programme Officer, ITU ARO

Tunisia

Mr. Faycal Bayouli
Director in International Cooperation & External Relations, Ministry of Communication Technologies & Digital Economy

Mr. Hafedh Gharbi Yahmadi
Professor Expert in ICT technologies, Tunisia Business School

Mr. Ridha Guellouz
President, Tunisian ICT Association

USA

Mr. Michael Palage
CEO, Pharos Global

Yemen

Mr. Abduljalil Saleh Alkubati
Vice Manager of Internet, Public Telecommunications Corporation, Yemen Net

Mr. Abdulrahman Mutahar Ahmed
Vice President, Internet Society Yemen Chapter

Remote Participants

Mr. Amro Moussa
Minister Advisor, Ministry of Communication and Information Technology, Egypt

Mr Chengetai Masango, Senior Advisor to UNSG High-level Panel on Digital Cooperation, United Nations

Mr. Ebrahim AlHaddad
Director, ITU Arab Regional Office

Mr Nabil Alkhamery
Care Project Manager, ERSAL Telecom, Yemen

Mr. Qusai AlShatty
Director, Central Agency for IT, Kuwait

Mr Vladimir Radunovic, Director of e-Diplomacy & Cybersecurity, Diplo Foundation

League of Arab States

Mr. Khaled Fouda
Director for ICT Development, League of Arab States

United Nations Economic and Social Commission for Western Asia (ESCWA)

Ms. Roula Majdalani
Acting Deputy ES, ESCWA

Mr. Haidar Fraihat
Director, Technology for Development Division (TDD)

Mr. Ayman El-Sherbiny
Chief of ICT Policies Section (ICTPS), TDD

Mr. Fouad Mrad
Chief of Section, TDD

Ms. Nibal Idlebi
Chief of Innovation Section, TDD

Mr Mohamad Nawar Alawa
Inter-Regional Adviser, TDD

Ms. Mirna El-Hajj Barbar
Programme Management Officer, ICTPS, TDD

Ms. Lize Denner
Associate Programme Management Officer, Innovation Section, TDD

Ms. Zahr Bou-Ghanem
Research Assistant, ICTPS, TDD

Ms. Mona Al-Kayali
Team Assistant, ICTPS, TDD