UNITED NATIONS **E**

ECONOMIC AND SOCIAL COUNCIL

Distr.
LIMITED
E/ESCWA/C.8/2024/12
16 July 2024
ORIGINAL: ENGLISH

Economic and Social Commission for Western Asia (ESCWA)

Committee on Technology for Development
Fifth session
Amman, 7-8 November 2024

Item 13 of the provisional agenda

Enhancing digital trust and cybersecurity in the Arab region

Summary

In the Arab region, the maturity of cybersecurity ecosystems varies significantly between countries. The cybersecurity infrastructure of some countries is hampered by factors such as inadequate infrastructure, lack of cybersecurity awareness, and legislative gaps. Several regional initiatives have been launched to address these problems. This document highlights various such initiatives and provides examples of national strategies developed to strengthen cybersecurity systems to combat cyberthreats.

The document begins with an overview of global developments and initiatives aimed at creating a safe, inclusive, and equitable digital environment. These include the World Summit on the Information Society and the United Nations Global Digital Compact. It also briefly describes the role of digital public infrastructure in enhancing digital trust and improving cybersecurity. It then offers regional and national perspectives and a way forward. Overall, the document emphasizes the importance of building a robust digital trust and cybersecurity framework to support the Arab region's rapid digital transformation.

The Committee on Technology for Development is invited to review the contents of the document and provide comments on the way forward for enhancing digital trust and cybersecurity in the region.

Contents

Introduction

1. "Digital trust" refers to the confidence individuals and businesses have in the security, privacy and reliability of online interactions and transactions. It essentially means a belief that the digital world is safe and operates according to ethical principles.

2. "Cybersecurity" refers to the methods used to protect digital assets from harm. Cybersecurity is the essential first step towards achieving digital trust.

3. The rapid global adoption of emerging technologies in public services and platforms presents vast opportunities for innovation. However, it also poses significant risks of misuse. For example, generative artificial intelligence can automate data collection on individuals and companies, making it easier for criminals to gather the material they need to impersonate leaders and gain unauthorized access to sensitive information. Embedding artificial intelligence into software could also create new avenues for cyberthreats, presenting new weaknesses for attackers to exploit, resulting in heightened vulnerability.

4. The Arab region is undergoing a rapid digital transformation, with Governments and businesses increasingly relying on online services and infrastructure. This digital leap presents immense opportunities for economic growth, improved governance and citizen engagement. However, for this transformation to be sustainable, it is necessary to build a robust digital trust and cybersecurity ecosystem, which aligns with the Plan of Action of the World Summit on the Information Society (WSIS) and the goals of the United Nations Global Digital Compact (GDC).

I. Global developments

A. World Summit on the Information Society

5. The first WSIS Summit took place in Geneva in 2003; the second was held in Tunis, Tunisia, in 2005. Participants established a road map for building an information society and set guidelines for bridging the global digital divide between more and less developed countries. Since then, WSIS Forums have been taking place periodically.

6. The 2024 WSIS Forum took place in Geneva from 27 to 31 May 2024. Participants focused on reviewing progress and charting a future course for the WSIS. They concluded that confidence, trust and security were key pillars of the information society, and that it was imperative to strengthen the role of regulators in digital sectors.

7. Subsequent discussions have addressed information and network security, cybercrime, spamming, and child safety online. WSIS implementation activities have contributed to building and strengthening capacities at national and regional levels to tackle various types of cybersecurity risks.

B. United Nations Global Digital Compact

8. The GDC is an initiative proposed by the United Nations aimed at creating a comprehensive framework for digital cooperation and governance. This initiative is part of a broader effort to ensure that digital technologies are used in ways that are inclusive, safe, and beneficial to all. The GDC is still in the process of being developed, with ongoing consultations and contributions being received from various stakeholders around the world. The aim is to present a finalized framework at the Summit for the Future during the seventy-ninth session of the General Assembly in September 2024.

9. The five objectives of the GDC are the following:

(a) Close digital divides and accelerate progress across the Sustainable Development Goals (SDGs);

(b) Expand opportunities for inclusion in the digital economy;

(c) Foster an inclusive, open, safe, and secure digital space;

(d) Advance equitable international data governance;

(e) Establish ways in which emerging technologies, including artificial intelligence, can be best used in the service of humanity.

10. The main goals of the GDC are the following. All relate somehow to digital trust and security:

(a) Inclusive digital economy: The GDC is intended to foster an inclusive digital economy where the benefits of digital technologies are widely shared, reducing digital divides and ensuring equitable access to digital resources and opportunities;

(b) Digital human rights: The GDC emphasizes the protection of human rights in the digital realm, addressing issues such as privacy, freedom of expression and the right to access information;

(c) Digital trust and security: The GDC is intended to enhance trust and security in the digital space, focusing on measures to protect against cyberthreats, misinformation and other online sources of harm;

(d) Global digital cooperation: The GDC encourages international cooperation on digital policy and governance, facilitating dialogue and collaboration among Governments, private sector entities, civil society and other stakeholders;

(e) The Sustainable Development Goals (SDGs): The GDC aligns with the SDGs, using digital technologies to support and accelerate progress towards achieving these Goals.

C. Digital public infrastructure

11. The United Nations Roadmap for Digital Cooperation, released in 2020, addresses the growing importance of digital technologies and their societal impacts. The road map invites all stakeholders to collaborate in creating a safer and more equitable digital world.

12. The key priorities of digital cooperation included in the road map are the following:

(a) Achieving universal connectivity by 2030;
(b) Promoting digital public goods to create a more equitable world;
(c) Ensuring digital inclusion for all, including the most vulnerable;
(d) Strengthening digital capacity-building;
(e) Ensuring the protection of human rights in the digital era;
(f) Supporting global cooperation on artificial intelligence;
(g) Promoting trust and security in the digital environment;
(h) Building a more effective architecture for digital cooperation.

13. Within this framework, one aspect of digital transformation has recently been receiving particular attention: digital public infrastructure. Digital public infrastructure is an umbrella term for the building blocks which enable the various processes of digital inclusive development. It is recognized as being crucial for managing services, resources, and information responsibly. According to one definition shared by the United Nations Development Programme and the International Telecommunications Union, these building blocks are digital identity systems, payments systems, and data exchange systems.[1] Digital public infrastructure is also important in other domains such as climate action, health care, and artificial intelligence.

[1] See United Nations Development Programme (UNDP), Digital public infrastructure, 2024; and International Telecommunications Union (ITU), https://www.itu.int/cities/digitaltransformationdialogues/digital-public-infrastructure/.

14. Digital public infrastructure can be used to promote several key goals:

(a) Inclusive access: Ensure everyone can participate in the digital world, regardless of socioeconomic background or location. This means bridging the digital divide and providing the tools and resources necessary for people to access essential services and opportunities online;

(b) Economic growth: Foster innovation and entrepreneurship by creating a robust digital foundation. Digital public infrastructure allows businesses to develop new services and reach wider markets, ultimately stimulating economic activity;

(c) Efficient service delivery: Improve the way Governments deliver public services. Digital public infrastructure streamlines processes and makes them more accessible to citizens, saving time and resources;

(d) Social development: Support the achievement of social goals such as education, health care and environmental sustainability. Digital public infrastructure can be used to deliver educational resources, improve health care access in remote areas, and promote green initiatives;

(e) Security and privacy: Protect user data and ensure the safe and secure use of digital systems. Strong safeguards are built into digital public infrastructure to prevent misuse and uphold individual privacy.

15. Overall, the road map emphasizes the need for deliberate and comprehensive trust-building measures in the design, regulation, governance, and implementation of digital public infrastructure to ensure the equitable and safe delivery of digital services.

16. Trust is crucial for the acceptance and effective implementation of digital public infrastructure, ensuring that people's rights are upheld and that they are treated fairly in digital interactions. Building trust must be a deliberate part of the design, regulation, governance, and implementation of digital public infrastructure. Safety, which underpins trust, includes technical measures such as end-to-end encryption and cybersecurity, as well as addressing organizational vulnerabilities. Beyond technology, trust also depends on stakeholders' perceptions and experiences with the system.

17. Digital public infrastructure must be safe, and it must be perceived as being so. It must have responsive mechanisms for addressing issues. Frameworks governing transparency, grievance redressal, human rights, due diligence and privacy can enhance safety and predictability, thus increasing public trust. Involving people in the design and governance of digital public infrastructure further boosts trust in the system.

18. While digital public infrastructure offers tremendous potential for development, there are also risks. Digital Public Infrastructure Safeguards (DPI Safeguards) is a United Nations initiative led by the Office of the Secretary-General's Envoy on Technology which is aimed at mitigating the risks associated with digital public infrastructure by establishing safeguards to ensure that it is developed and used responsibly.

19. The initiative is developing a comprehensive safeguards framework which will establish principles and best practices for designing, implementing and operating digital public infrastructure in a way that:

(a) Protects human rights (such as freedom of expression and privacy);
(b) Promotes inclusion (by ensuring everyone has access);
(c) Advances sustainable development (by contributing to the SDGs).

20. Launched in September 2023, the initiative is still evolving. Here are some key milestones:

(a) Multistakeholder working groups were established in March 2024 to bring together experts from Governments, civil society, and the private sector to develop the safeguards framework;

(b) An interim report was released in April 2024 for public comment, outlining initial ideas for the framework.[2]

[2] DPI Safeguards interim report, available at https://safedpi.gitbook.io/safeguards/working-group-documents/reports.

21. The initiative is expected to culminate in the release of a final digital public infrastructure safeguards framework at the Summit of the Future in September 2024. This framework will serve as a guide for countries around the world as they build and use their digital infrastructure.

D. Digital public infrastructure, digital trust and cybersecurity

22. Digital public infrastructure, digital trust and cybersecurity are closely linked:

(a) Foundation for trust:

- Security: Strong digital public infrastructure acts as the secure foundation for digital interactions. Its core components, such as digital identity and data sharing, are built with robust security measures in place. This helps establish trust among users and organizations engaging in online activities.
- Transparency: Interoperable and standardized digital public infrastructure fosters transparency. Users can understand how their data is collected, used, and protected. This transparency builds trust in the digital ecosystem.

(b) Enhancing cybersecurity:

- Reduced scope for attack: Well-designed digital public infrastructure minimizes the scope for cybercriminals to attack. By standardizing core services and implementing strong security protocols, vulnerabilities are minimized, making it harder for attackers to exploit weaknesses.
- Improved incident response: Digital public infrastructure facilitates a coordinated approach to cybersecurity threats. Standardized systems and data sharing mechanisms enable faster and more efficient responses to cyberattacks.

(c) Building a secure digital environment:

- Empowering users: Digital public infrastructure empowers users to participate securely in the digital world. Secure digital identity systems allow users to control their online identities and data access.
- Fostering innovation: A secure digital environment built on strong digital public infrastructure encourages innovation. Businesses and individuals are more likely to develop and use new digital technologies when they trust the underlying infrastructure.

23. However, there are also challenges:

- Vulnerability of components: Security breaches within any core component of digital public infrastructure can have a cascading effect, affecting the entire digital ecosystem.
- Balancing security and convenience: Striking the right balance between robust security and user convenience is crucial. Overly complex security measures can discourage user adoption.

24. Overall, digital public infrastructure plays a critical role in building a digital environment where trust and cybersecurity are paramount. By providing a secure foundation and fostering transparency, digital public infrastructure empowers users, strengthens cybersecurity, and paves the way for a more secure and prosperous digital future.

E. The Global Digital Compact, digital trust and cybersecurity

25. Enhancing digital trust and cybersecurity is a vital element of the GDC. The GDC is focused on creating a safer and more trustworthy digital environment for individuals, businesses and Governments. The key elements include:

(a) Cybersecurity measures:

- Strengthening defences through robust cybersecurity strategies.
- Encouraging international cooperation to combat cybercrime.

(b) Data privacy and protection:

- Establishing and enforcing privacy regulations.
- Implementing strong data-security measures.

(c) Combating misinformation and disinformation:

- Supporting fact-checking and verification initiatives.
- Enhancing media literacy for identifying credible sources.

(d) Ethical artificial intelligence and algorithmic transparency:

- Ensuring ethical development and use of artificial intelligence.
- Promoting transparency in algorithmic decision-making.

(e) Protection from online harm:

- Implementing measures against online harassment and abuse.
- Enhancing online safety for children.

(f) Secure digital infrastructure:

- Building resilient and reliable digital infrastructure.
- Safeguarding critical infrastructure from cyberattacks.

(g) Digital identity and authentication:

- Developing secure authentication methods.
- Promoting interoperable digital identity systems.

(h) Legal and regulatory frameworks:

- Working towards harmonized laws across countries.
- Ensuring accountability and redress mechanisms.

II. Regional perspectives

A. Overview

26. In the Arab region, the maturity of cybersecurity ecosystems varies significantly between countries. Some countries are among the top performers globally; others fall into the least advanced quartile. The risks of cyberattacks are significant and potentially very costly. Globally, the percentage of organizations reporting that their most serious cybersecurity breach in the previous three years had cost them $1 million or more has risen from 27 per cent in 2023 to 36 per cent in 2024. In the Arab region, the corresponding figure for 2024 is 29 per cent.[3]

27. The cybersecurity market in the Arab region is projected to grow by nearly 20 per cent each year over the next seven years.[4] This growth will be concentrated in countries with robust cybersecurity industries and government policies, making them preferred destinations for industry, academics, businesses, and research and innovation.

[3] PWC, Digital Trust Insights – Middle East findings, 2024.

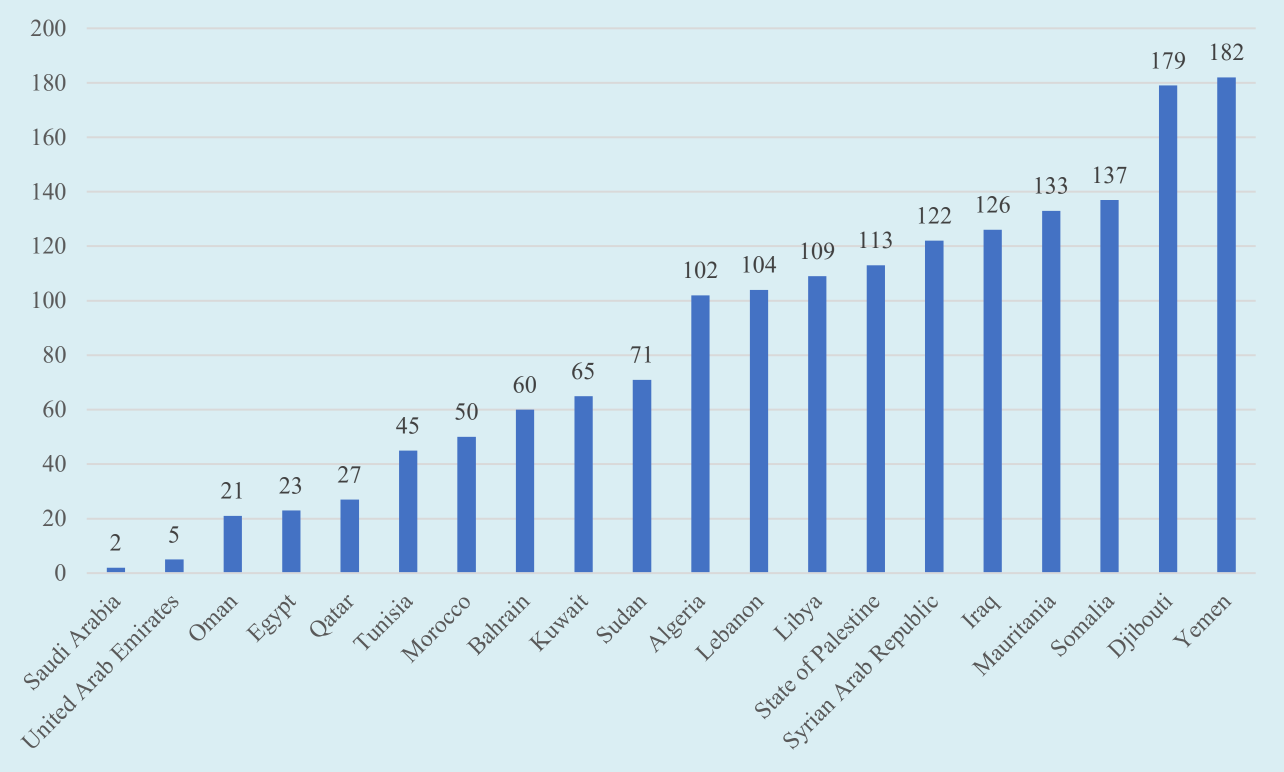
[4] Ibid.

28. To provide quantitative insights into the region's performance in cybersecurity, this document will rely on the 2021 Global Cybersecurity Index (GCI), the most recent edition of an index produced by the International Telecommunication Union (ITU). The GCI measures five dimensions: legal aspects, technical aspects, organizational aspects, capacity-building and cooperation.

29. Seven Arab countries are among the 50 highest-ranked countries in the GCI. Three others are ranked between 51 and 100. Ten Arab countries are ranked between 101 and 182 (figure 1).

30. The average score of countries in the Arab region (49.86 per cent) is lower than the average score of all developing economies (59.18 per cent) and significantly below the average score of all developed economies (91.8 per cent).

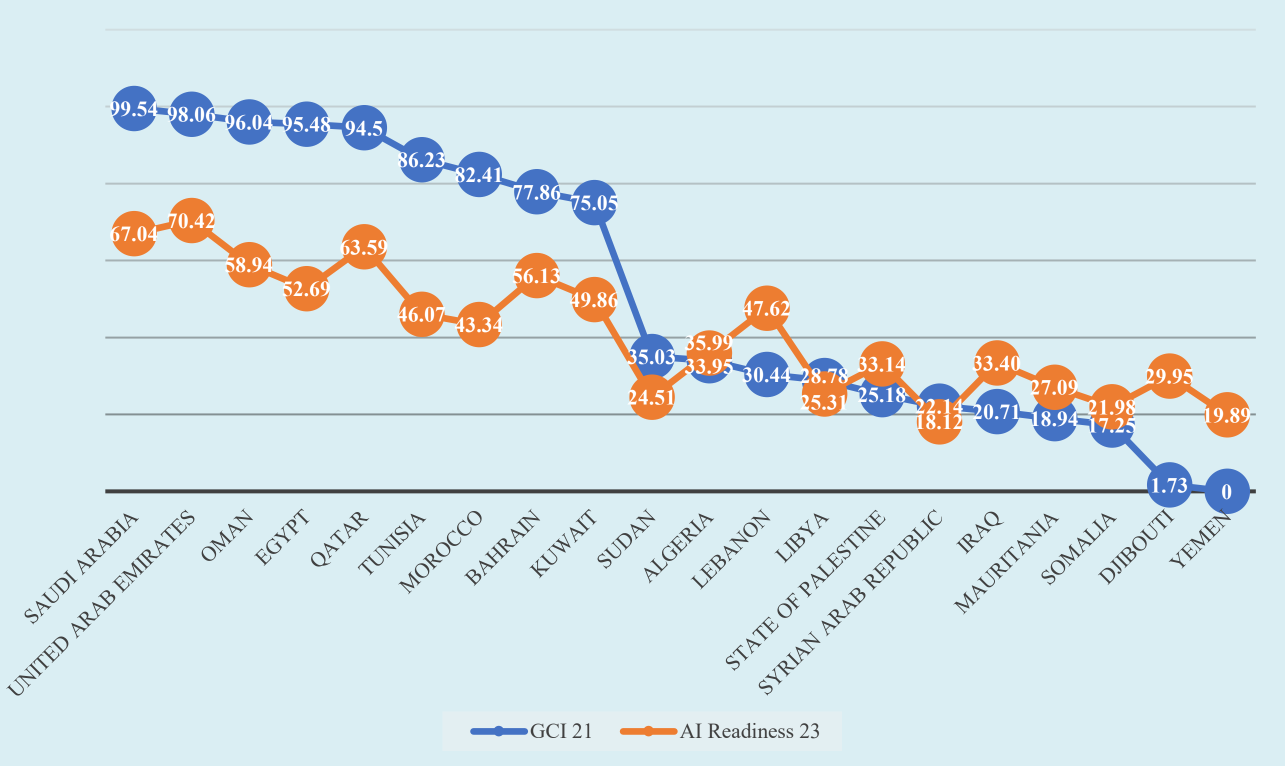
Figure 1. Global ranking of Arab States in the Global Cybersecurity Index (2021)



Source: ESCWA compilation based on ITU CGI 2021. Available at https://www.itu.int/pub/D-STR-GCI.01-2021 (accessed on July 2024).

31. In the Arab region, there is significant coherence between a country's rank on the GCI and its Government's preparedness for artificial intelligence applications, albeit with exceptions in certain countries. The correlation factor between the 2021 GCI and the 2023 AI Government Readiness Index is 95.27 per cent, indicating that countries with a robust cybersecurity ecosystem are generally better positioned to deploy artificial intelligence applications in the public sector.

Figure 2. Comparison of GCI and artificial intelligence readiness indicators



Source: Oxford Insights Government AI Readiness Index (2023). Available at https://oxfordinsights.com/ai-readiness/ai-readiness-index/.

B. Challenges and threats in the Arab region

32. Several challenges hinder the development of a secure and trusted digital environment in the Arab region, echoing concerns being addressed by the United Nations Global Digital Compact:

(a) Lack of awareness: Many citizens lack basic cybersecurity knowledge, making them susceptible to phishing attacks, malware, and online scams. This is reflected in the GDC’s focus on digital security;

(b) Inadequate infrastructure: The region has varying levels of digital infrastructure development. Some countries do not have adequate secure data centres or sufficiently advanced communication networks. This is reflected in the GDC's emphasis on closing the digital divide;

(c) Legislative gaps: Cybercrime laws and data protection regulations are not always well defined or harmonized across Arab States, hindering the multi-stakeholder approach advocated by the GDC. Updated national strategies are still lacking in certain Arab countries;

(d) Limited collaboration: There is a need for more regional and international collaboration in intelligence-sharing and coordinated responses to cybersecurity threats, in line with the call made in the GDC for international cooperation.

C. Regional initiatives

1. *Council of Arab Cybersecurity Ministers*

33. The Council of Arab Cybersecurity Ministers was established in 2023 by the Economic and Social Council of the League of Arab States on a proposal from Saudi Arabia. It seeks to strengthen cooperation

among Arab countries in all aspects related to cybersecurity, working to foster growth and prosperity by ensuring that digital infrastructure in the Arab region is safe and reliable.

34. The council’s objectives are to:

(a) Develop and reinforce cooperation in cybersecurity, facilitating the exchange of knowledge and experiences;

(b) Safeguard the interests of member States in international cybersecurity organizations through unified Arab position-setting;

(c) Contribute to the establishment of the security and reliability of Arab digital infrastructure in a way which is conducive to the growth and prosperity of all member States;

(d) Coordinate efforts among Arab countries across all cybersecurity-related domains.

35. The council’s tasks are to:

(a) Address cybersecurity issues and advancements across the security, economic, developmental and legislative spheres;

(b) Formulate recommendations and decisions on cybersecurity matters;

(c) Foster cooperation and integration of cybersecurity projects and initiatives;

(d) Develop overarching policies, strategies, and priorities to enhance collective Arab action on cybersecurity.

2. *Arab Cybersecurity Strategy*

36. In 2022, the Arab Information and Communication Technologies Organization introduced the Arab Cybersecurity Strategy (ACSS) for the 2023-2027 period. The ACSS serves as a road map for action; it outlines the initiatives Arab Governments will carry out over the next five years to foster the adoption and development of globally recognized, efficient and cost-effective cybersecurity controls. Its overarching objective is to cultivate uniform growth in cybersecurity maturity across the Arab region, fortifying cyberspace against ever-evolving digital threats.

37. The vision of the ACSS is set out as follows: "Towards a safe, inclusive Arab society integrated into the global digital economy, and self-sufficient solutions and expertise supporting digital confidence and trust within the Arab cyberspace." Its objectives are:

(a) Creating participatory mechanisms involving the region's cybersecurity market;

(b) Developing specialist cybersecurity capacity, nurturing professional and student involvement, building capacity, and establishing an integrated cybersecurity training system;

(c) Enhancing community awareness of cybersecurity and Internet-related risks, advocating safe digital practices, and encouraging institutions to promote digital security awareness effectively;

(d) Organizing competitions supporting cybersecurity excellence through award programmes, fostering the launch of cybersecurity initiatives by institutions, inspiring entrepreneurial innovation, supporting creative research in academic institutions, and engaging students in cybersecurity;

(e) Regulating cybersecurity incident detection and reporting mechanisms;

(f) Establishing a standardized methodology for assessing the severity of cybersecurity incidents to provide appropriate support;

(g) Increasing the capacities of Arab countries to respond to all types of cybersecurity incidents;

(h) Designing a comprehensive legal and regulatory framework for cybersecurity to combat cybercrimes, safeguard current and emerging technologies, and develop supportive systems to shield small and medium-sized enterprises from cybersecurity threats.

38. The focus areas of the ACSS are:

(a) Drawing up national cybersecurity strategies;
(b) Supporting research and development work;
(c) Conducting training and awareness-raising initiatives;
(d) Promoting security standards;
(e) Facilitating joint Arab cooperation and initiatives;
(f) Establishing national incident response centres;
(g) Promoting market-oriented cybersecurity training;
(h) Modernizing cybersecurity governance frameworks.

3. *Arab Regional Cybersecurity Centre*

39. In December 2012, the Arab Regional Cybersecurity Centre of the International Telecommunication Union (ITU-ARCC) was established through collaboration between ITU and Oman, represented by the Ministry of Transport, Communications, and Information Technology. With a vision of fostering a safer and more cooperative cybersecurity environment in the Arab region, ITU-ARCC is intended to bolster ITU's role in instilling confidence and security in the use of information and communications technologies across the Arab region. Hosted and operated by the Oman National Computer Emergency Readiness Team, ITU-ARCC was officially launched on 3 March 2013.

40. The objectives of ITU-ARCC are:

(a) Driving the adoption of the ITU Global Cybersecurity Agenda throughout the Arab region;

(b) Assisting and responding to the cybersecurity needs of least developed countries in the region;

(c) Serving as a management centre and implementation platform for regional cybersecurity objectives;

(d) Providing a platform for member States to oversee regional cybersecurity programmes and initiatives;

(e) Developing regional or national information security frameworks and policies through regional studies and workshops.

41. The roles of ITU-ARCC are:

(a) Cybersecurity strategy and governance: ITU-ARCC experts work closely with Governments and public sector bodies to craft national cybersecurity strategies, setting clear accountabilities and responsibilities. These strategies encompass robust programmes aimed at enhancing cybersecurity capabilities and addressing gaps in the cybersecurity landscape;

(b) Cybersecurity technical and assurance: ITU-ARCC experts employ recognized technical benchmarks and international standards such as ISO 27001 to assist ITU member States in improving their cybersecurity capabilities;

(c) Cybersecurity capacity-building: ITU-ARCC conducts cybersecurity capacity-building initiatives for institutions. It also seeks to raise cybersecurity awareness through community campaigns, forums and national-level training and development programmes;

(d) Incident management: Collaborating with partners, ITU-ARCC supports ITU member States in establishing national computer incident response teams which serve as central cybersecurity coordination points. The ITU-ARCC incident response service assesses the capabilities of government and public sector response teams, identifies gaps, and proposes improvements.

D. National cybersecurity plans

42. Several countries in the Arab region have issued national strategies to improve their cybersecurity ecosystems.

1. *Morocco*

43. The National Cybersecurity Strategy, devised by the General Directorate of Information Security Systems in 2012, identifies areas where the country's cybersecurity framework requires urgent improvement:

(a) Risk assessment: evaluating risks affecting information systems across government agencies, public organizations and critical infrastructure;

(b) Protection and defence: implementing measures to safeguard and defend these information systems;

(c) IT security foundations: improving fundamental aspects of IT security across sectors, including legal frameworks, awareness programmes, capacity-building initiatives, and research and development;

(d) Cooperation: fostering both national and international cooperation to improve overall cybersecurity capabilities.

44. The strategy applies the principle of “security by design”, integrating security measures from the beginning of the system development process. It encompasses awareness programmes, training workshops, and best practices to combat cybercrime effectively. Additionally, the cybersecurity practices of Morocco are reinforced by various laws and regulations. For instance, Law 07-03 addresses cybercrime, while Law 53-05 governs electronic transactions, seeking to provide a secure and reliable basis for digital activity.

45. The General Directorate of Information Systems Security, which serves as the national authority overseeing cybersecurity, issued a new version of the country’s national cybersecurity strategy in 2024. The updated strategy emphasizes enhancing security and bolstering cyberspace resilience, particularly as new threats emerge.

2. *Egypt*

46. In Egypt, the Supreme Cybersecurity Council recently unveiled the country’s National Cybersecurity Strategy for 2023-2027. The vision of this strategy is to make the country’s digital infrastructure secure, resilient, and conducive to economic prosperity. Key focus areas include:

(a) Building an integrated legislative framework: drawing up comprehensive laws and regulations to address cybersecurity concerns effectively;

(b) Strengthening national partnership: fostering collaboration between government agencies, private sector entities, academia, and civil society to collectively enhance cybersecurity measures;

(c) Encouraging scientific research and promoting innovation and growth: supporting research initiatives and fostering innovation in cybersecurity technologies and practices to drive economic growth;

(d) Cultural change around cybersecurity: promoting awareness and education programmes to instill a culture of cybersecurity awareness and responsibility among Egyptian citizens;

(e) Building strong and resilient cybersecurity defences: implementing robust cybersecurity measures and infrastructure to defend against cybersecurity threats and ensure the resilience of critical systems;

(f) Strengthening international cooperation: engaging with international partners and organizations to share best practices, expertise, and information for collective cybersecurity efforts.

3. *Jordan*

47. The latest National Cybersecurity Strategy document for Jordan, which covered the period from 2018 to 2023, outlined a comprehensive approach to cybersecurity. It was structured around five pillars:

(a) Protecting critical infrastructure: The Government was committed to safeguarding critical infrastructure. This commitment covered physical facilities such as power plants and water treatment facilities as well as cyberinfrastructure such as the Internet and communication networks;

(b) Building a flexible electronic environment: Efforts were directed towards fostering a flexible digital environment by promoting the adoption of secure practices and technologies. Enhancing the response capabilities of both public and private sectors to electronic attacks was a key aspect of this pillar;

(c) Strengthening international cooperation: The Government aimed to bolster international cooperation in cybersecurity through the exchange of information and best practices. Collaborative efforts with other nations were prioritized to respond effectively to cybersecurity threats;

(d) Assisting citizens and companies: Initiatives were undertaken to help citizens and companies to defend themselves against cyberattacks. This involved raising awareness about cybersecurity risks and providing resources and support to enhance resilience;

(e) Building a strong cybersecurity workforce: The Government sought to nurture a robust cybersecurity workforce by offering education and training opportunities in the field. It also sought to promote job creation in the cybersecurity sector.

48. The strategy's action plans were categorized into four main areas: protection, detection, response, and development. Additionally, a proposal was made to establish a supreme cybersecurity council to oversee strategy implementation, set up a national cybersecurity centre, and form an emergency cybersecurity response team. These initiatives underscored the commitment of Jordan to enhancing its cybersecurity capabilities and improving its readiness in the face of evolving cybersecurity threats.

4. *Saudi Arabia*

49. The Cybersecurity Strategy of Saudi Arabia (2023-2027), which was launched in 2022, has five pillars:

(a) Cybersecurity protection and defence: developing cybersecurity defence capabilities to safeguard the stability of the country’s Government and economic systems. This involves strengthening technical, legal, and organizational capacities to deal effectively with cybersecurity threats;

(b) Development of cybersecurity infrastructure: focused on bolstering public and private sector cybersecurity infrastructure across Saudi Arabia. This entails drawing up cybersecurity standards and programmes and reinforcing existing legislation;

(c) Cooperation: fostering cooperation between the private sector, government entities, and international institutions to improve cybersecurity. Objectives include facilitating the exchange of information and experiences, fostering cooperation in combating cybercrimes, and enhancing national capabilities;

(d) Awareness and training: increasing cybersecurity awareness among institutions and individuals in Saudi Arabia. These measures include training and awareness programmes, as well as initiatives to increase technical skills in the cybersecurity domain;

(e) Legislation: strengthening legislation pertaining to cybersecurity and ensuring that it is aligned with international standards. Emphasis is placed on developing a robust legal framework and effective enforcement mechanisms to combat cybercrime while safeguarding sensitive data and privacy.

50. Saudi Arabia has earned recognition as one of the most cybersecure countries in the world by several organizations. The Government seeks to maintain the reputation of Saudi Arabia as a cybersecure environment for residents, businesses and investors.

5. *State of Palestine*

51. In 2023, the Ministry of Telecommunications and Information Technology of the State of Palestine, in collaboration with ESCWA, drew up a National Cybersecurity Strategy. The forthcoming strategy pursues the following vision: Towards a digital State of Palestine that is secure, confident in its systems, and capable of building and developing in cyberspace. The strategy focuses on five tracks:

(a) Infrastructure and services: improving digital infrastructure and services to ensure the stability and safety of networks, systems and applications;

(b) Regulatory and institutional environment: developing effective organizational structures and mechanisms for managing cybersecurity, enhancing coordination between institutions, and improving administrative mechanisms and standards;

(c) Capacity-building, awareness, research, and development: improving cybersecurity capacity, encouraging research and development for innovation, and developing advanced cybersecurity protection technologies;

(d) National, regional and international cooperation: boosting cooperation and coordination with local, regional, and international bodies with the aim of combating common cybersecurity threats;

(e) Innovation and entrepreneurship: encouraging innovation and entrepreneurship in cybersecurity by supporting emerging companies, promoting digital transformation and developing new solutions to confront cybersecurity challenges.

52. To ensure effective governance, the Supreme National Cybersecurity Committee oversees and monitors the cybersecurity strategy at national level. Sectoral cybersecurity committees operate at various levels to implement and coordinate cybersecurity efforts, enhancing cooperation in implementing cybersecurity programmes across the Government, the private sector and other vital institutions.

6. *Syrian Arab Republic*

53. The National Cybersecurity Strategy of the Syrian Arab Republic, which was developed in cooperation with ESCWA in 2023, pursues the following vision: To achieve a safe and reliable cyberspace in all fields, contributing to protecting national interests and fostering confidence in digital transformation.

54. The strategy encompasses six key programmes: infrastructure security, development of the legal and regulatory framework, promotion of cybersecurity awareness, capacity- and knowledge-building, regional and international partnerships and cooperation, and development of specialized organizational structures.

55. The implementation of the strategy is overseen by the Higher Committee on Digital Transformation. Additionally, a National Committee on Cybersecurity coordinates with each national body on the implementation of cybersecurity projects, ensuring effective coordination and collaboration across government bodies.

III. The way forward

56. The Arab region has the potential to become a leader in the digital age by aligning its digital transformation efforts with the GDC. By prioritizing cybersecurity, fostering trust and promoting regional cooperation, Arab States can create a secure and thriving digital ecosystem that benefits all citizens, businesses

and Governments. This will pave the way for a more prosperous, inclusive, and secure digital future for the region, contributing to the overall goals of the GDC.

57. Several key recommendations could, if implemented, help to build a more secure and trusted digital space in the Arab region:

(a) Strengthening cybersecurity infrastructure: Governments and private entities should invest in robust cybersecurity infrastructure, including secure data centres, encryption technologies, and advanced threat-detection systems, building on the digital resilience envisioned in the GDC;

(b) Developing a robust legal framework: Arab countries should have comprehensive and harmonized cybercrime laws and data protection regulations that address emerging threats and protect user privacy, aligning with the GDC's principles of human rights and legal frameworks;

(c) Investing in cybersecurity education: Arab countries should run national awareness campaigns and educational programmes to equip citizens with essential cybersecurity skills to navigate the digital world safely, supporting the GDC's focus on digital safety;

(d) Engaging the private sector: Public-private partnerships are crucial for building a resilient digital ecosystem. Governments should cooperate with technology companies to develop secure digital services and infrastructure, aligning with the GDC's focus on multi-stakeholder collaboration;

(e) Promoting regional cooperation: Arab States should use established regional mechanisms to facilitate information-sharing, coordinate responses to cyberattacks, and develop joint training programmes for cybersecurity professionals, following the multi-stakeholder approach of the GDC;

(f) Arab Governments should work to build trust with citizens and stakeholders to foster positive engagement and the effective delivery of services;

(g) Security and privacy: As technology advances, so do cyber threats. Governments should therefore prioritize robust cybersecurity measures, data protection, and privacy safeguards to ensure that citizens' information is secure and confidential;

(h) Ethical use of technology: Governments should ensure that emerging technologies are employed responsibly, avoiding biases, discrimination, and unethical practices. Efforts to achieve this may include legislation and education. Promoting transparency and collaboration is also likely to be effective;

(i) Citizen-centric design: Digital public services should be designed in a way which prioritizes citizens' needs and expectations. User-friendly, accessible and responsive services enhance citizen satisfaction and trust.

58. Through its technical cooperation programme, ESCWA can assist member States in improving digital trust and developing their cybersecurity ecosystems. It can provide support in drawing up national cybersecurity strategies or action plans, raising awareness among national officials about the impact of emerging technologies on cybersecurity, and facilitating the exchange of knowledge among member States in related areas.
