UNITED NATIONS

E

ECONOMIC AND SOCIAL COUNCIL

Distr.
LIMITED
E/ESCWA/C.5/2024/6
9 October 2024
ENGLISH
ORIGINAL: ARABIC

Economic and Social Commission for Western Asia (ESCWA)

Committee on Transport and Logistics
Twenty-fifth session
Amman, 26–27 November 2024

Item 8 of the provisional agenda

Inevitability of enhancing cybersecurity in the transport sector in the Arab region

Summary

Cybersecurity is gaining global importance, especially with increasing reliance on digital technologies in various sectors, including transport. The maturity of cybersecurity systems varies greatly between Arab countries, and cybersecurity infrastructure in some countries faces significant challenges, including insufficient technological infrastructure, lack of awareness, and widening legislative gaps. As a result, several regional and national initiatives have been launched to address these challenges.

The present document sets out some of these initiatives, and provides examples of national strategies and plans that have been developed to enhance cybersecurity systems to combat cyberthreats in general and those affecting the transport sector in particular. It also reviews previous initiatives and current activities of the Economic and Social Commission for Western Asia (ESCWA) in the field of enhancing cybersecurity, provides examples of proposed national plans in this area, and concludes with proposals for enhancing cybersecurity in the transport sector in the Arab region.

The present document was prepared in response to the recommendation of the Transport and Logistics Committee at its twenty-fourth session (Cairo, 10–11 January 2024) to focus on the risks caused by cybersecurity breaches to the transport sector and its infrastructure, and provide recommendations to mitigate them. The Transport and Logistics Committee is invited to review the contents of the present document and comments thereon to enhance cybersecurity in the transport sector in the Arab region.

Contents

Introduction

1. The term "cybersecurity" refers to methods used to protect digital assets from harm and damage, including computers, servers, mobile devices, information systems, databases and networks.

2. Intelligent transportation systems (ITS)[1] use information and communication technologies (ICTs) to improve traffic flow, enhance operational performance, increase safety, and provide users with real-time transport information. However, with increasing reliance on these systems, and greater use of emerging technologies such as artificial intelligence (AI) and the Internet of Things in transport systems, it has become necessary to ensure their security to prevent potential cyberattacks that may disrupt transport networks, lead to service interruptions, or even cause physical harm to users.

3. Understanding the importance of cybersecurity in ITS is the first step towards creating a secure transport environment. The following are some key points to consider:

- Protecting data integrity: cybersecurity measures ensure that data within ITS is accurate and reliable, which is critical for optimal operation.
- Ensuring availability of information systems and platforms: a successful cyberattack can disrupt transport services, causing delays, inefficiencies, and potential safety risks.
- Preventing unauthorized access: cybersecurity helps prevent unauthorized access to ITS, protecting sensitive information and systems from malicious activity.

4. The Arab region is witnessing an accelerating digital transformation as Governments and companies increasingly rely on digital services and technological infrastructure. To benefit from this digital leap in economic growth and ensure its sustainability, it is necessary to build a strong cybersecurity environment, in line with the World Summit on the Information Society (WSIS) Action Plan and the goals of the United Nations Global Digital Compact (GDC).

5. The National Institute of Standards and Technology defines critical infrastructure as physical or virtual systems and assets whose incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. This definition emphasizes that the transport sector is part of the national critical infrastructure. For example, a disruption to the transport system could affect the ability to control traffic signals and could disrupt railroad operations, causing serious accidents.

6. As cyberthreats become more complex and widespread, ensuring the resilience and security of these vital systems is no longer just a technological necessity, but a fundamental guarantee for well-being and continuity of life.

I. Cyberthreats in the transport sector

7. Modern transport operations are increasingly vulnerable to targeted attacks owing to their interconnected nature, which integrates communications, logistics and payment into unified database systems. In 2022, the transport sector was the ninth most targeted sector by cyberattacks,[2] and faces significant threats due to its connection to supply chains, high-value goods, and time-sensitive operations. There has been a significant increase in cyberattacks on the transport sector, with the percentage of successful attacks rising by 36 per cent in 2023 compared with 2022. This statistic highlights the increasing vulnerability of the sector, as it relies heavily on digital technologies. Hackers primarily targeted computers, servers and network equipment,

[1] Koenig solutions, Understanding the importance of cybersecurity in intelligent transportation systems, May 2024.

[2] Marsh McLennan Agency, A glitch on the road: cybersecurity trends facing the trucking and transportation industry, September 2024.

resulting in 87 per cent of successful attacks. This fact suggests that the underlying IT infrastructure is the primary entry point for attackers, underscoring the need for robust protection measures.

8. The global security market is currently worth around $150 billion, and is expected to rise to $400 billion in 2026.[3] Vital sectors, such as transport, energy, health and finance, have become increasingly dependent on digital technologies to operate their core businesses.

9. Ransomware, malware and phishing attacks are becoming more common, with potential risks even extending to self-driving vehicles. Phishing involves tricking recipients into clicking on malicious links or attachments, highlighting the importance of raising employee awareness and training. These phishing attacks account for 51 per cent of cases,[4] and often result in data theft, extortion and damage to brand reputation. The average cost of a data breach in the transport sector was $3.59 million in 2022,[5] and the total cost of damage from such cybercrimes is expected to reach $10.5 trillion by 2025 across all industries.[6]

10. Moreover, the use of spyware and remote access Trojans (RATs) has generally increased. Spyware now accounts for 21 per cent of malware incidents, and RATs have doubled to 15 per cent. Spyware collects sensitive information without the user's consent, while Trojans allow remote control of infected systems.[7]

11. The attack on the Danish shipping giant Maersk in 2017 is a major example of the impact of these programmes on the transport sector. The company was attacked by the NotPetya ransomware, which affected its shipping operations in four countries, causing delays and interruptions that lasted for weeks, and costing the company more than $200 million.

12. Targeted attacks account for 83 per cent of successful cyberattacks in the Arab region.[8] Government entities are the most attractive targets for attackers, accounting for 22 per cent of all attacks on organizations. Industrial organizations, including those in the transport sector, ranked second among the most targeted organizations, receiving 16 per cent of attacks. Attackers were able to access these systems either through social engineering in 33 per cent of cases, or by using malware with remote access Trojans in 62 per cent of cases.

13. In 2023, the transport sector in the Arab region recorded a significant increase in cyberattacks, specifically using ransomware. In this context, an IB Group report indicated that the transport sector in the region was exposed to eight cyberattacks. These attacks were part of a 68 per cent increase in ransomware incidents across the region. The transport sector, along with the telecommunications sector, was highly vulnerable to ongoing threats coordinated by groups known for their espionage activities.

14. Ransomware activity in the Arab region increased by 77 per cent in the first quarter of 2023 compared with the same period in 2022.[9] The most targeted Gulf Cooperation Council (GCC) countries were the United Arab Emirates (33 per cent), Saudi Arabia (29 per cent), and Kuwait (21 per cent). Malware was used in nearly two thirds of attacks on organizations, as it allows attackers to control compromised devices and remain within

[3] European Parliamentary Research Service, The NIS2 Directive: a high common level of cybersecurity in the EU, February 2021.

[4] IBM Security, IBM X-Force Threat Intelligence Index 2024, 2024.

[5] Marsh McLennan Agency, A glitch on the road: cybersecurity trends facing the trucking and transportation industry, September 2024.

[6] Forbes, 10.5 Trillion reasons why we need a united response to cyber risk, February 2023.

[7] Positive technologies, Analytics, 2024.

[8] Positive technologies, Cybersecurity threat scape in the Middle East, 2022-2023.

[9] Intelligent CIO, Surge in ransomware, leaks and info stealers targeting Middle East and Africa, February 2024.

the infrastructure. Between May and June 2018,[10] cyberattacks targeted transport and shipping organizations in Kuwait using various hacking tools that allowed hackers to monitor and steal data from infected systems. In May 2020, air transport agencies in Kuwait and Saudi Arabia were targeted, likely to explore and extract sensitive data. Careem, a popular car rental startup in the Arab region, also suffered a major data breach in January 2018, with hackers stealing customer personal data, such as names, email addresses, phone numbers, and trip information.

II. Top global cybersecurity processes

A. World Summit on the Information Society

15. The first WSIS was held in Geneva in 2003, and the second in Tunis in 2005. Participants prepared a road map for building the information society, and set guidelines for bridging the global digital divide between the least developed countries and the most developed countries. Since then, WSIS forums have been held periodically.

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

17. Discussions covered information and network security, cybercrime, spam and child safety online. Activities to implement WSIS decisions have contributed to building and strengthening capacities at the national and regional levels to address various forms of cybersecurity risks.

B. United Nation Global Digital Compact

18. GDC is an initiative proposed by the United Nations for the period 2023–2024, with the aim of developing 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. GDC was presented at the Summit on the Future held at the seventy-ninth session of the General Assembly in September 2024.

19. The five GDC objectives, which are largely related cybersecurity, are summarized as follows:

- Bridging digital divides and accelerating progress towards achieving all the Sustainable Development Goals.
- Expanding opportunities for inclusion in the digital economy.
- Promoting an inclusive, open, safe and secure digital space.
- Enhancing fair international data management.
- Developing methods that enable emerging technologies, including AI, to be used to their best advantage in the service of humanity.

C. United Nations Convention against Cybercrime

20. The United Nations Convention against Cybercrime, ratified in August 2024, focuses on enhancing international cooperation to combat crimes committed through ICT systems.

21. The Convention's main areas of focus include the following:

[10] Intelligent CIO, The biggest data breaches and cyberattacks in the Middle East, May 2021.

- **International cooperation:** countries should cooperate more closely to combat cybercrime, recognizing that this type of crime often transcends national borders. This cooperation includes mutual legal assistance, extradition and coordinated investigations.
- **Combating specific cybercrimes:** the Convention identifies and seeks to address categories of cybercrimes, such as crimes against the confidentiality, integrity and availability of computer systems and data, and crimes such as fraud, child exploitation, and the distribution of illegal content via information and communications technologies.
- **Evidence sharing:** the Convention proposes mechanisms for the effective exchange of electronic evidence relating to serious crimes, including establishing protocols for the preservation, collection and exchange of electronic data, which is crucial in the prosecution of cybercrime.
- **Capacity-building:** the Convention highlights the importance of building capacity in member States to effectively address cybercrime. This includes providing technical assistance, training and resources to developing countries to enhance their capacity to combat cyberthreats.
- **Respect for human rights and fundamental freedoms:** tackling cybercrime must be balanced with respect for human rights and fundamental freedoms, ensuring that measures to combat cybercrime do not infringe on privacy, freedom of expression or other rights.

III. Examples of cybersecurity plans from outside the Arab region

22. In 2020, the European Union Agency for Cybersecurity (ENISA)[11] issued detailed guidance to help port operators manage cyberthreats. The guidance emphasizes a risk-based approach to cybersecurity, and encourages operators to systematically identify and protect their internet-connected assets. This includes assessing potential cyberthreats and implementing appropriate security measures, such as access controls, network segmentation, and regular updates to security protocols.

23. In addition, the updated version of the Network and Information Security Directive (NIS2)[12] was issued for the European Union in 2023. The main objective of this directive is to strengthen the security of organizations so as to address emerging cyberthreats.[13] It is an update of the first version of NIS,[14] which aimed to achieve a high level of cybersecurity across member States. The second version requires more organizations and sectors to take effective measures, and aims to strengthen cybersecurity in Europe in the long term. NIS2 generally focuses on key organizations in the critical infrastructure supply chain. In October 2024, detailed requirements were developed that will enter into force in January 2025. Under NIS2, the European Union will impose significant financial penalties on organizations that fail to comply within the specified timeframe. NIS2 applies to both public and private entities, and covers the transport sector as a vital sector in the European Union. It covers risk analysis and information security policies, incident management, supply chain security, human resources security, access control and asset management policies.

24. NIS2 divides stakeholders into two categories: an essential category, and an important category. Both categories must comply with the same security measures, but essential category organizations are subject to proactive supervision, while important category organizations are only monitored after a non-compliance incident is reported.

[11] ENISA, Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk, December 2020.

[12] KPMG, Network & Information Security Directive (NIS2), May 2023.

[13] Centraleyes, NIS2 Framework: Your Key to Achieving Cybersecurity Excellence, January 2024.

[14] Think Tank-European Parliament, The NIS2 Directive: A high common level of cybersecurity in the EU, February 2023.

25. In 2024, the Cyber Resilience Act[15] was enacted to protect consumers and businesses that purchase or use products and software with digital components. It focuses on introducing mandatory cybersecurity requirements for manufacturers of these products and retailers who sell them, with an emphasis on the need for such protection to continue throughout the life cycle of the products. The Act entered into force on 10 October 2024, and requires manufacturers to have compatible products on the European Union market by 2027. The Act ensures the following:

- Setting out uniform standards for products or software with digital components that are on the market.
- Providing a framework for cybersecurity requirements that regulate the planning, design, development and maintenance of these products, with obligations to be met at each stage of the value chain.
- Committing to a duty of care throughout the life cycle of these products.

26. In the United States, the Transportation Security Administration[16] issued new security guidelines in 2021 to enhance cybersecurity resilience within the transport sector. These guidelines specifically target high-risk areas, such as freight and passenger rail. Key measures include requiring owners and operators to appoint a cybersecurity coordinator responsible for overseeing cybersecurity practices and responding to threats. Moreover, they must report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency within 24 hours to ensure a rapid response to potential threats. These guidelines require owners and operators to develop and implement a comprehensive cybersecurity incident response plan to mitigate the risk of operational disruptions caused by cyber incidents. They also require them to complete a cybersecurity vulnerability assessment to identify potential vulnerabilities in their system.

27. In Canada, the Vehicle Cybersecurity Strategy of Transport Canada sets future vehicle cybersecurity goals and priorities to enhance the cyber resilience of land transport.[17] The strategy helps the department achieve its vision of continuing to be a leader in ensuring a safe and resilient vehicle cybersecurity environment. The strategy includes the following three overarching objectives for land transportation cybersecurity:

- Objective 1: Integrate vehicle cybersecurity considerations into policy and regulatory frameworks. This objective includes a number of priorities, such as providing guidance, tools and non-regulatory policies, and updating regulatory and policy frameworks to ensure a flexible and responsive regulatory environment that fosters autonomous vehicle innovation and provides the necessary flexibility.
- Objective 2: Raise awareness and promote a modern and innovative approach to vehicle cybersecurity. This includes a number of priorities, such as active participation in federal and regional forums, research, testing and verification, and public awareness and education on vehicle cybersecurity.
- Objective 3: Address emerging issues in vehicle cybersecurity. This includes protecting privacy and managing personal information, ensuring digital infrastructure security, and ensuring supply chain security.

[15] European Commission, EU Cyber Resilience Act, July 2024.

[16] Transportation Security Administration, DHS announces new cybersecurity requirements for surface transportation owners and operators, December 2021.

[17] Transport Canada, Transport Canada's Vehicle Cyber Security Strategy, 2021.

IV. Cybersecurity in the Arab region

A. Overview

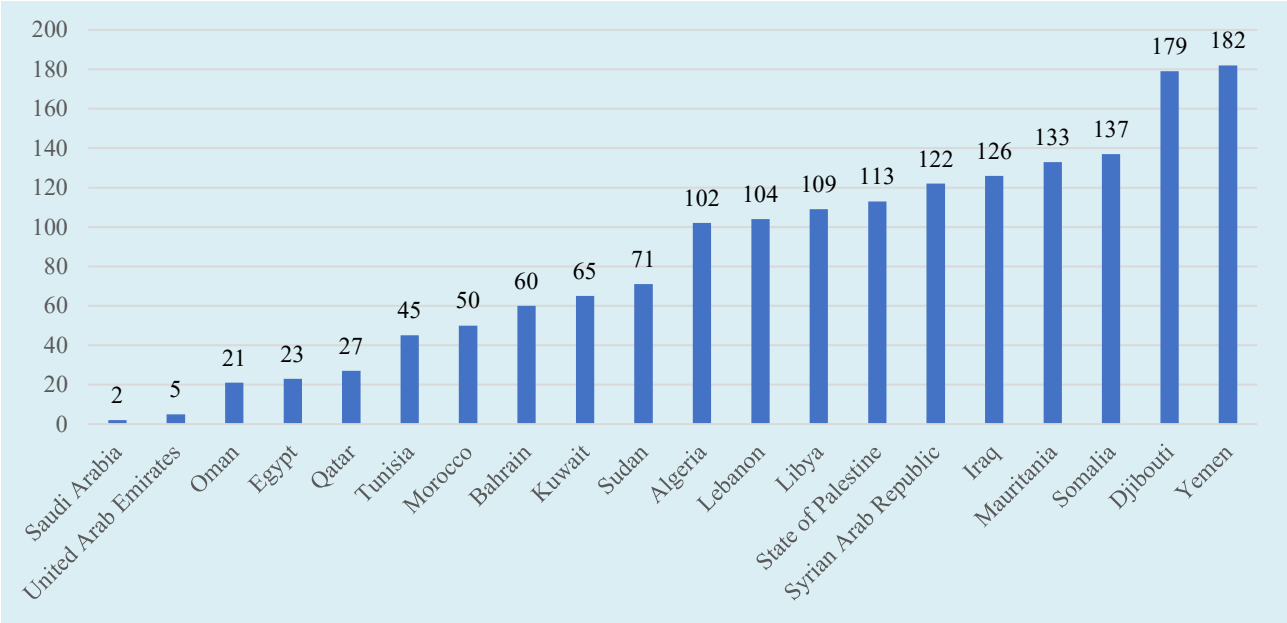
28. The maturity of cybersecurity systems varies greatly between Arab countries. Some rank among the highest worldwide in terms of their performance in this area, while others fall into the least advanced quartile. The cybersecurity market in the Arab region is expected to grow by about 20 per cent annually over the next seven years.[18] This growth will be concentrated in countries with strong cybersecurity industries and government policies, making them the preferred destinations for industry, academia, companies, research and innovation.

29. The Global Cybersecurity Index 2021 provides a quantitative view of the Arab region's performance in the field of cybersecurity. This index, issued by the International Telecommunication Union (ITU), measures the following five dimensions: legal aspects, technical aspects, regulatory aspects, capacity-building, and cooperation.[19]

30. According to this index, seven Arab countries occupy ranks among the top 50 countries, while three occupy ranks between 51 and 100, and 10 are between ranks 101 and 182 (figure 1).

31. The average score recorded by Arab countries is 49.86 per cent, which is lower than the average score recorded by all developing economies (59.18 per cent) and much lower than the average score recorded by all advanced economies (91.8 per cent).

Figure 1. Global ranking of Arab countries in the Global Cybersecurity Index, 2021



Source: ESCWA calculations based on the Global Cybersecurity Index 2021.

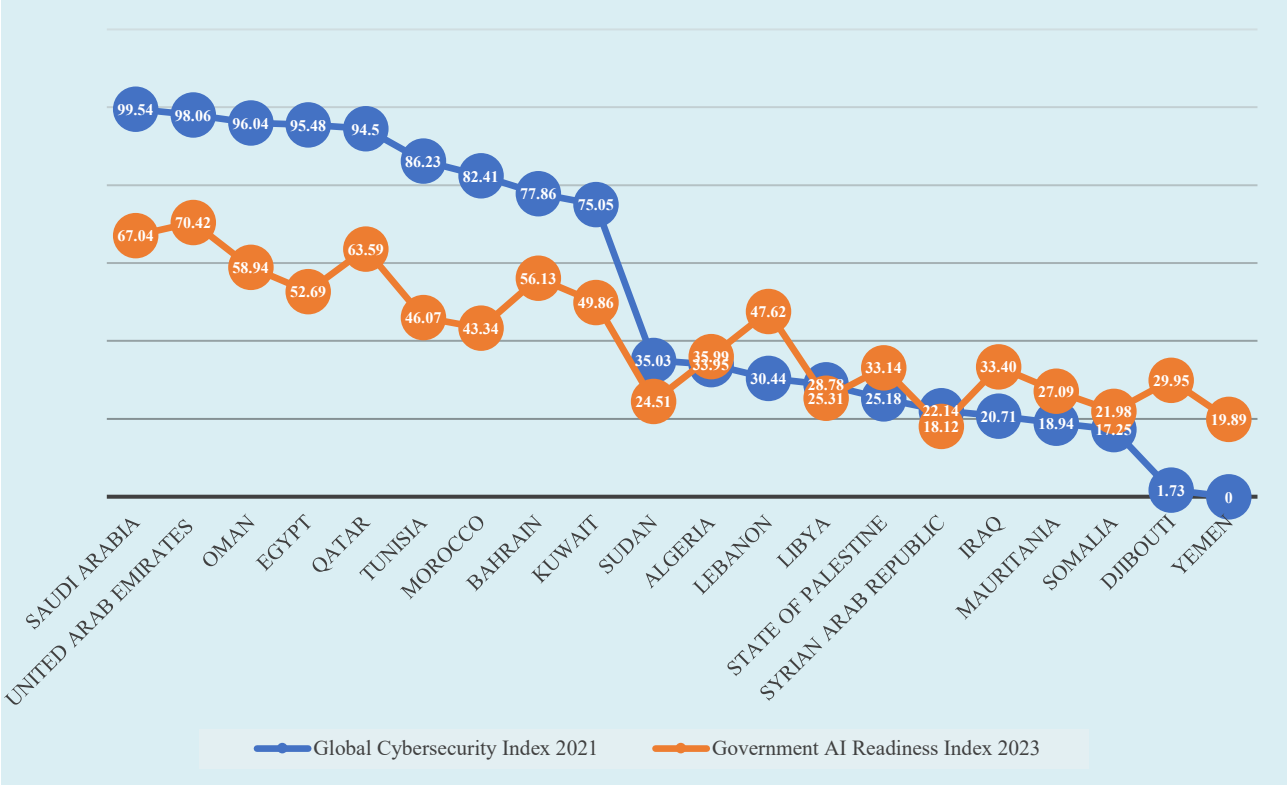
32. The Arab region records a high degree of consistency between a country's ranking in the Global Cybersecurity Index and its ranking in the Government AI Readiness Index, which measures government readiness for AI applications, despite exceptions in some countries. The correlation coefficient between the Global Cybersecurity Index 2021 and the Government AI Readiness Index 2023 is 95.27 per cent, indicating

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

[19] ITU, Global Cybersecurity Index, 2021.

that countries with a strong cybersecurity system are generally better positioned to deploy AI applications in the public sector.

Figure 2. Comparison between the Government AI Readiness Index and the Global Cybersecurity Index



Source: ESCWA calculations based on the Global Cybersecurity Index 2021 and the Government AI Readiness Index.

B. Challenges in the Arab region

33. Several challenges hinder the development of a safe and reliable digital environment in the Arab region, highlighting the concerns addressed by the United Nations Global Digital Compact (GDC). These challenges include the following:

(a) **Lack of awareness:** many citizens lack basic cybersecurity knowledge, making them vulnerable to phishing attacks, malware, and online fraud. This is reflected in the GDC focus on digital security;

(b) **Inadequate technological infrastructure:** the level of digital infrastructure development in the region varies. Some countries lack sufficient secure data centres or sufficiently advanced communications networks. This was highlighted in GDC, which emphasizes the importance of bridging the digital divide;

(c) **Legislative gaps:** cybercrime laws and data protection regulations are not well-defined or harmonized in all Arab countries, hindering the multi-stakeholder approach advocated by GDC. Some Arab countries still lack updated national strategies;

(d) **Limited cooperation:** there is a need for stronger regional and international cooperation in intelligence sharing and coordinated responses to cybersecurity threats.

V. Regional initiatives to enhance cybersecurity

A. Arab Cyber Security Strategy

34. In 2022, the Arab Information and Communication Technologies Organization (AICTO)[20] presented the Arab Cybersecurity Strategy 2023–2027, which provides a road map for Arab countries to strengthen their cybersecurity. This strategy sets out the initiatives that Arab Governments should implement over the next five years to promote the adoption and development of globally recognized cybersecurity controls. The strategy aims to raise the level of cybersecurity maturity across the Arab region, and to fortify cyberspace against ever-evolving digital threats.

35. The vision of the Arab Cybersecurity Strategy states the following: "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 of Arab cyberspace." Its objectives are as follows:

(a) Creating participatory mechanisms by taking advantage of the region›s cybersecurity market;

(b) Developing the capacity of cybersecurity specialists, encouraging professionals and students to get involved, building capacity and developing an integrated cybersecurity training system;

(c) Increase community awareness of cybersecurity and Internet-related risks, promoting safe digital practices and encouraging institutions to spread cyber awareness effectively;

(d) Organizing competitions that support cybersecurity excellence through Arab award programs, encouraging institutions to launch cybersecurity programs, inspiring entrepreneurs to innovate in the field, supporting creative research in academic institutions and encouraging students to be involved in cybersecurity;

(e) Regulating the cybersecurity incident detection and reporting mechanism;

(f) Establishing a standardized methodology for assessing the degree of gravity of cyber incidents to provide appropriate support;

(g) Building Arab capacities at a global level to respond to all types of cyber accidents;

(h) Designing a comprehensive legal and regulatory framework for cybersecurity to address all types of cybercrimes, building a regulatory framework to protect current and emerging technologies, and developing supportive systems to empower small and medium-sized enterprises and protect them from cyber threats.

B. Arab Regional Cybersecurity Centre

36. The ITU Arab Regional Cybersecurity Centre was established in December 2012 following collaboration between ITU and Oman, represented by the Ministry of Transport, Communications and Information Technology. The Centre aims to provide a safer and more collaborative cybersecurity environment in the Arab region. It was officially launched on 3 March 2013, and is hosted and managed by the Oman National Computer Emergency Readiness Team.

37. The following are the objectives of the Arab Regional Cybersecurity Centre are:

(a) Promoting the adoption of the ITU Global Cybersecurity Agenda throughout the Arab region;
(b) Providing assistance to and meeting the cybersecurity needs of the Arab least developed countries.

[20] AICTO is an Arab governmental organization operating under the banner of the League of Arab States. It contributes to the development of information and communication technologies in Arab countries, and provides the necessary mechanisms to support cooperation and integration in this field among the organization's members. It also seeks to develop joint policies and strategies to achieve fair and sustainable access to technology, and harness it to serve the goals of economic development.

38. The Arab Regional Cybersecurity Centre undertakes the following tasks:

(a) **Cybersecurity strategy and governance:** the Centre's experts work closely with Governments and public sector entities to formulate national cybersecurity strategies, and clearly define responsibilities. These strategies include programmes and initiatives to enhance cybersecurity capabilities and address gaps in the cybersecurity system;

(b) **Technical aspect in the field of cybersecurity:** the Centre's experts use recognized technical standards and international standards (such as ISO 27001) to assist ITU member States in improving their cybersecurity capabilities;

(c) **Capacity-building in the field of cybersecurity:** the Centre implements initiatives to build institutional capacity in the field of cybersecurity. It also seeks to raise awareness of cybersecurity through community campaigns, forums, and training and development programmes at the national level;

(d) **Incident management:** the Centre collaborates with its partners to support ITU member States in establishing national cybersecurity incident response teams that act as central cybersecurity coordination points. Its incident response service assesses the capabilities of government and public sector response teams, identifies gaps, and proposes improvements.

C. Council of Arab Ministers of Cybersecurity

39. The Economic and Social Council of the League of Arab States established the Council of Arab Ministers of Cybersecurity in 2023, based on a proposal from Saudi Arabia.[21] The Council seeks to enhance cooperation between Arab countries on all aspects of cybersecurity, and to stimulate growth and prosperity by ensuring that the digital infrastructure in the Arab region is safe and reliable.

40. The Council's main objectives can be summarized as follows:

(a) Developing and enhancing collaboration in the field of cybersecurity, and facilitating the exchange of knowledge and expertise;

(b) Protecting the interests of member States in international cybersecurity organizations by defining a unified Arab position;

(c) Contributing to establishing the security and reliability of Arab digital infrastructure in a manner that leads to the growth and prosperity of all member States;

(d) Coordinating efforts between Arab countries in all areas related to cybersecurity.

D. ESCWA activities in cybersecurity

41. ESCWA began to focus on enhancing the cybersecurity environment over 10 years ago. In 2011, it issued the ESCWA Directives for the Regional Harmonization of Cyber Legislation. In 2020, it issued a publication entitled Technology and Innovation for the Development of Land Transport in Arab Countries, following collaboration between the Transport Group and the Information and Technology Group. The publication addressed data and information security in several of its sections. In 2024, ESCWA issued a report on digital trust and emerging technologies.

42. ESCWA also provides technical support to government agencies in Arab countries to develop their national and sectoral plans in the field of cybersecurity.

[21] فوربس، جامعة الدول العربية تنشئ مجلس وزراء الأمن السيبراني العرب، أيلول/سبتمبر 2023.

VI. Examples of national cybersecurity plans in the Arab region

43. Many Arab countries have issued national strategies to improve the cybersecurity environment, which has had a positive impact on enhancing cybersecurity and protecting vital infrastructure, including the transport sector.

A. Morocco

44. The National Cybersecurity Strategy, developed by the General Directorate of Information Systems Security in 2012 as the national authority overseeing cybersecurity, identifies the following areas where the country's cybersecurity framework requires urgent improvement:

(a) **Risk assessment:** assessing risks affecting information systems in government and public institutions and critical infrastructure;

(b) **Protection and defence:** implementing measures to protect and defend information systems;

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

(d) **Cooperation:** enhancing national and international cooperation to improve overall cybersecurity capacity.

45. The strategy applies the principle of "security by design" by integrating security measures at the beginning of the systems and services development process. The strategy also includes awareness programmes and training workshops on best practices for combating cybercrime.

46. The General Directorate of Information Systems Security issued a new version of the country's National Cybersecurity Strategy in 2024. The updated strategy emphasizes enhancing the security and resilience of cyberspace, especially as new threats emerge. The strategy's vision states: For a reliable, secure and resilient national cyberspace, capable of supporting the Kingdom's digital transformation, enhancing economic prosperity and ensuring the well-being of citizens.

47. The updated strategy is based on the following pillars: developing national coordination mechanisms; updating and strengthening the legal and normative framework; supporting the decision-making process and adopting data-based policies; strengthening national capacity in the field of prevention, management and response to cyber incidents and crises; enhancing the protection of vital infrastructure information systems against risks; developing a culture of cybersecurity within society; supporting the national cybersecurity system; encouraging innovation; and strengthening and enhancing national presence at the regional and international levels in cybersecurity issues.

B. Egypt

48. The Egyptian Supreme Cybersecurity Council recently unveiled the National Cybersecurity Strategy 2023–2027. The strategy's vision is to make the country's digital infrastructure secure, resilient and conducive to economic prosperity, and its main focus areas include the following:

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

(b) **Changing the culture of society around cybersecurity:** promoting awareness and education programmes to instil a culture of cybersecurity awareness and responsibility among Egyptian citizens;

(c) **Strengthening national partnerships:** strengthening collaboration between government agencies, the private sector, academia and civil society to collectively enhance cybersecurity measures;

(d) **Building strong and resilient cyber defences:** implementing robust cybersecurity measures to defend and establish a solid infrastructure to protect against cybersecurity threats and ensure the resilience of critical systems;

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

(f) **Promoting international cooperation:** connecting with partners and international organizations to exchange best practices, expertise and information for collective efforts in the field of cybersecurity.

C. Jordan

49. The latest Jordanian National Cyber Security Strategy 2018–2023 outlines a comprehensive approach to cybersecurity, including the following five pillars:

(a) **Protecting critical infrastructure:** the Government committed itself to protecting critical infrastructure, including physical facilities such as transport, power plants, and water treatment facilities, and cyberinfrastructure such as the Internet and telecommunications networks;

(b) **Building a resilient digital environment:** efforts were directed towards promoting a resilient digital environment by encouraging the adoption of secure practices and technologies. Strengthening the capacity of the public and private sectors to respond to cyberattacks is a key aspect of this pillar;

(c) **Enhancing international cooperation:** the Government enhanced international cooperation in the field of cybersecurity by exchanging information and best practices. Priority was given to collaborative efforts with other countries to respond effectively to cybersecurity threats;

(d) **Assisting citizens and businesses:** initiatives were taken to help citizens and businesses defend themselves against cyberattacks. This included raising awareness of cybersecurity risks and providing resources and support to enhance resilience;

(e) **Building a strong cybersecurity workforce:** the Government fostered a strong cybersecurity workforce by providing education and training opportunities in the field. It also created additional job opportunities in the cybersecurity sector.

50. The transport sector is vital for the Jordanian economy. The Ministry of Transport's strategic plan for 2024–2026 includes the following vision: A safe and modern transport sector that contributes to making Jordan a pivotal transport hub. The strategy's pillars emphasize the inclusion of innovative technologies on the one hand, and maintaining security and safety on the other.

D. Syrian Arab Republic

51. The Cybersecurity Strategy of the Syrian Arab Republic, developed in collaboration with ESCWA in 2023, seeks to achieve the following vision: A secure and reliable cyberspace in all areas, contributing to protecting national interests and enhancing confidence in digital transformation.

52. The strategy includes the following six main programmes: promoting infrastructure security, developing the legal and regulatory framework, disseminating a culture of cyber awareness, building capacity and knowledge, strengthening regional and international partnerships and cooperation, and developing specialised functional structures.

53. The Higher Committee for Digital Transformation supervises the implementation of the strategy. A national cybersecurity committee coordinates with each national entity on the implementation of cybersecurity projects, ensuring effective coordination and collaboration between government entities.

E. Saudi Arabia

54. The National Cybersecurity Strategy of Saudi Arabia (2023-2027), launched in 2022, is based on the following five pillars:

(a) **Protecting and defending cybersecurity:** developing cybersecurity defence capabilities to protect the stability of the country's government and economic systems. This involves strengthening technical, legal and organizational capabilities to effectively deal with cybersecurity threats;

(b) **Developing cybersecurity infrastructure:** focusing on strengthening the cybersecurity infrastructure in the public and private sectors across Saudi Arabia. This entails developing cybersecurity standards and programmes, and strengthening existing legislation;

(c) **Strengthening collaboration:** enhancing collaboration between the private sector, government agencies, and international institutions to improve cybersecurity. This includes facilitating the exchange of information and expertise, enhancing cooperation in combating cybercrime, and strengthening national capacity;

(d) **Raising awareness and offering training:** raising awareness of cybersecurity among institutions and individuals in Saudi Arabia. These measures include training and awareness programmes, and initiatives to increase technical skills in the field of cybersecurity;

(e) **Strengthening legislation:** strengthening cybersecurity legislation and ensuring its compliance with international standards. Emphasis is placed on developing a strong legal framework and effective enforcement mechanisms to combat cybercrime, while protecting sensitive data and privacy.

55. The National Cybersecurity Authority of Saudi Arabia has developed comprehensive frameworks and guidelines to enhance cybersecurity across various sectors, including the transport sector.[22] It conducts regular security audits and assessments to identify vulnerabilities in critical infrastructure. Advanced cybersecurity technologies and solutions are being implemented to protect this infrastructure, and intensive training programmes are being provided to employees to enhance their ability to detect and respond to cyberthreats. These efforts aim to increase the cybersecurity resilience of the country's transport sector, and protect its critical infrastructure from potential cyberthreats.

F. Oman

56. The Ministry of Transport, Communications and Information Technology of Oman has developed comprehensive cybersecurity frameworks to protect infrastructure, including transport.[23] Regular risk assessments are conducted to identify potential cyberthreats, and cybersecurity policies and procedures specifically designed to address these threats have been developed and implemented.

57. The Arab Regional Cybersecurity Centre in Oman launched the Cybersecurity Industry Development Strategy Maturity Module (CIDSMM) to enhance cybersecurity in the Arab region. This programme provides regulatory authorities and cybersecurity stakeholders with a comprehensive guide that allows them to assess and improve their capabilities in the field. It also focuses on increasing the resilience of critical infrastructure, including the transport sector, through continuous monitoring, risk assessment, and implementation of best practices in the field of cybersecurity.

VII. Final proposals

58. The Arab region has the potential to become a leader in the digital age by directing digital transformation efforts towards key sectors, most notably transport. By prioritizing cybersecurity and enhancing trust and

[22] ENISA, Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk, December 2020.

[23] Sultanate of Oman- Information Technology Authority, Basic Security Controls, July 2017.

regional cooperation, Arab countries can create a safe and prosperous digital environment that benefits all citizens and public and private institutions.

59. The following proposals, if implemented, can help build a safer and more reliable digital space in the Arab region:

- Develop a sectoral action plan to enhance cybersecurity in the field of transport, in line with the national cybersecurity strategies that have been (or are being) developed in each Arab country.
- Raise awareness among transport workers on the importance of cybersecurity and the risks that threaten it, especially with the increasing adoption of emerging technologies. This should also include awareness of the precautionary measures that can be taken to reduce these risks.
- Strengthen cybersecurity infrastructure: Governments and private entities should invest in cybersecurity infrastructure, including secure data centres, the application of government cloud computing, encryption technologies, and advanced threat detection systems.
- Conduct comprehensive risk assessments, especially in vital sectors such as transport, develop effective incident response plans, and ensure compliance with existing cybersecurity standards and regulations.
- Develop an appropriate legal framework: it is essential for Arab countries to have comprehensive anti-cybercrime and data protection laws that address emerging threats and protect user privacy, in line with the principles of GDC and the United Nations Convention against Cybercrime. It is also essential to provide a comprehensive approach to cybersecurity in the transport sector, ensure the safe integration of digital and operational technologies, improve threat intelligence sharing, and strengthen public-private partnerships.
- Invest in cybersecurity education: Arab countries should organize national awareness campaigns and educational programmes to equip citizens with basic cybersecurity skills to navigate the digital world safely, and enable them to safely use digital platforms and services in all sectors, including the transport sector.
- Engage the private sector: public-private partnerships are crucial to building a resilient digital environment. Governments should work with technology companies to develop secure digital services and infrastructure, in collaboration with multiple stakeholders.
- Strengthen regional cooperation: Arab countries should use established regional mechanisms to facilitate information exchange, coordinate responses to cyberattacks, and develop joint training programmes for cybersecurity professionals.
- Use technology ethically: Governments should ensure the responsible use of emerging technologies, avoiding bias, discrimination and unethical practices.

60. Through its technical cooperation programme, ESCWA can continue to assist member States in improving their cybersecurity, work with stakeholders to develop national cybersecurity plans, raise awareness among national officials about the impact of emerging technologies on cybersecurity in various sectors, including the transport sector, and facilitate knowledge exchange among member States in relevant areas.
