E

الأمم المتحدة

Distr.
LIMITED

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

المجلس
الاقتصادي والاجتماعي

اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)

لجنة النقل واللوجستيات
الدورة الخامسة والعشرون
عمّان، 26-27 تشرين الثاني/نوفمبر 2024

البند 8 من جدول الأعمال المؤقت

حتمية تعزيز الأمن السيبراني في قطاع النقل في المنطقة العربية

موجز

يكتسب الأمن السيبراني أهميةً عالمية لا سيّما مع ازدياد الاعتماد على التكنولوجيات الرقمية في مختلف القطاعات، بما فيها قطاع النقل. ويختلف نُضج أنظمة الأمن السيبراني إلى حدٍّ بعيد بين بلدان المنطقة العربية، كما تواجه البنية التحتية للأمن السيبراني في بعض هذه البلدان تحديات جمّة، منها على سبيل المثال عدم كفاية البنية التحتية التكنولوجية، ونقص الوعي، واتّساع الفجوات التشريعية. ونتيجةً لذلك، أُطلِقت عدّة مبادرات إقليمية ووطنية للتصدي لهذه التحديات.

تسلّط هذه الوثيقة الضوء على بعض هذه المبادرات وتقدّم أمثلة على الاستراتيجيات والخطط الوطنية التي تمّ تطويرها لتعزيز أنظمة الأمن السيبراني بهدف مكافحة التهديدات السيبرانية عموماً وتلك التي تطال قطاع النقل خصوصاً. كما تستعرض مبادرات اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) السابقة وأنشطتها الحالية في مجال تعزيز الأمن السيبراني، ثم تقدّم أمثلة عن الخطط الوطنية المقترَحة في هذا المجال، وتختتم بعرض مقترحات لتعزيز الأمن السيبراني في قطاع النقل في المنطقة العربية.

وجديرٌ بالذكر أنّ إعداد هذه الوثيقة يأتي استجابةً لتوصية لجنة النقل واللوجستيات في دورتها الرابعة والعشرين (القاهرة، 10-11 كانون الثاني/يناير 2024) التي تقضي بـ"إيلاء الاهتمام لموضوع المخاطر التي تسبّبها اختراقات الأمن السيبراني على قطاع النقل وبناه التحتية، وتقديم التوصيات للتخفيف منها". ولجنة النقل واللوجسيتات مدعوّة إلى مراجعة مضمون الوثيقة وتقديم تعليقات بشأنها لتعزيز واقع الأمن السيبراني في قطاع النقل في المنطقة العربية.

المحتويات

مقدمـة

1- يشير مصطلح "الأمن السيبراني" إلى الأساليب المستخدمة لحماية الأصول الرقمية من الأذى والضرر، وتشمل هذه الأصول الأجهزة الحاسوبية والمخدّمات والأجهزة النقّالة وأنظمة المعلومات وقواعد البيانات والشبكات.

2- تستخدم أنظمة النقل الذكية[1] تكنولوجيا المعلومات والاتصالات لتحسين تدفّق حركة المرور، وتعزيز الأداء التشغيلي، وزيادة السلامة، وتزويد المستخدِمين بمعلومات النقل في الوقت الفعلي. ولكن مع الاتّكال المتزايد على هذه الأنظمة، والاستخدام المتزايد للتكنولوجيات الناشئة مثل الذكاء الاصطناعي وإنترنت الأشياء في منظومات النقل، أصبح ضرورياً ضمان أمنها لمنع الهجمات السيبرانية المحتملة التي قد تعطّل شبكات النقل وتؤدي إلى توقّف الخدمات أو حتى تُلحق الأذى الجسدي بالمستخدِمين.

3- وإدراك أهمية الأمن السيبراني في أنظمة النقل الذكية هو الخطوة الأولى نحو إيجاد بيئة نقل آمنة. وفي ما يلي بعض النقاط الرئيسية الواجب مراعاتها:

- حماية سلامة البيانات: تضمن تدابير الأمن السيبراني أن تكون البيانات ضمن أنظمة النقل الذكية دقيقة وموثوقة، وهو أمرٌ بالغ الأهمية للتشغيل الأمثل.
- ضمان إتاحة أنظمة المعلومات والمنصّات: يمكن أن يؤدي الهجوم السيبراني الناجح إلى تعطيل خدمات النقل، ممّا يسبّب التأخير وانعدام الكفاءة ومخاطر السلامة المحتملة.
- منع النفاذ غير المصرّح به: يساعد الأمن السيبراني في منع النفاذ غير المصرّح به إلى أنظمة النقل الذكية، وحماية المعلومات الحسّاسة والأنظمة من الأنشطة الضارّة.

4- تواجه المنطقة العربية تحوّلاً رقمياً متسارعاً كون الحكومات والشركات تعتمد بصورةٍ متزايدة على الخدمات الرقمية والبنية التحتية التكنولوجية. وللاستفادة من هذه القفزة الرقمية في النمو الاقتصادي وضمان استدامتها، من الضروري بناء بيئة قوية للأمن السيبراني، على نحوٍ ينسجم مع خطة عمل القمة العالمية لمجتمع المعلومات (WSIS) وأهداف الاتفاق الرقمي العالمي للأمم المتحدة (GDC).

5- ويعرّف المعهد الوطني للمعايير والتكنولوجيا (NIST) البنية التحتية الحيوية بأنها الأنظمة والأصول المادية أو الافتراضية التي قد يؤدي أيّ خلل أو تدمير فيها إلى أثر كارثي على الأمن أو الاقتصاد الوطني أو الصحة العامة أو السلامة، أو على عدّة قضايا مجتمعةً منها. ويؤكّد هذا التعريف أنّ قطاع النقل هو جزءٌ من البنى التحتية الحيوية الوطنية. فعلى سبيل المثال، قد يؤثّر تعطيل نظام النقل على إمكانية السيطرة على إشارات المرور كما قد يؤدي إلى تعطيل عمليات السكك الحديدية، فيتسبّب بحوادث خطيرة.

(1) Koenig solutions, Understanding the Importance of Cybersecurity in Intelligent Transportation Systems, May 2024.

6- مع تفاقم تعقيد التهديدات السيبرانية وانتشارها، لم يَعُد ضمان مرونة هذه الأنظمة الحيوية وأمنها مجرد ضرورة تكنولوجية فحسب، بل بات ضمانة أساسية للرفاهية واستمرارية الحياة.

أولاً- المخاطر السيبرانية في قطاع النقل

7- باتت عمليات النقل الحديثة أكثر عرضةً للهجمات المستهدفة نظراً لطبيعتها المترابطة التي تدمج الاتصالات والخدمات اللوجستية وتسديد الرسوم في أنظمة قواعد بيانات موحّدة. وفي عام 2022، احتلّ قطاع النقل[2] المرتبة التاسعة بين أكثر القطاعات استهدافاً من الهجمات السيبرانية، وهو يواجه تهديدات ملموسة بسبب ارتباطه بسلاسل التوريد والبضائع العالية القيمة والعمليات الحسّاسة للوقت. وسُجّلت زيادة كبيرة في الهجمات السيبرانية على قطاع النقل، مع ارتفاع نسبة الهجمات الناجحة بنحو 36 في المائة في عام 2023 مقارنةً بعام 2022. وتسلّط هذه الإحصائية الضوء على الضعف المتفاقم للقطاع مع اعتماده بدرجةٍ كبرى على التكنولوجيات الرقمية. بالفعل، استهدف المتسلّلون في المقام الأول أجهزة الحاسوب والمخدّمات ومعدّات الشبكة، الأمر الذي أدى إلى نجاح 87 في المائة من الهجمات. ويشير هذا الواقع إلى أنّ البنية التحتية الأساسية لتكنولوجيا المعلومات هي نقطة الدخول الرئيسية للمهاجمين، ممّا يؤكد على الحاجة إلى اعتماد تدابير حماية قوية.

8- تبلغ قيمة سوق الأمن العالمية حالياً نحو 150 مليار دولار أمريكي، وهو رقم يُتوقّع أن يرتفع إلى 400 مليار دولار في عام 2026[3]. فقد أصبحت القطاعات الحيوية، مثل النقل والطاقة والصحة والتمويل، تعتمد بصورة متزايدة على التكنولوجيات الرقمية لتشغيل أعمالها الأساسية.

9- في المقابل، باتت برامج الفدية والبرامج الضارّة وهجمات التصيّد الإلكتروني الاحتيالي شائعةً، مع وجود مخاطر محتملة تطال حتى المَرْكَبات الذاتية القيادة. ويقتضي التصيّد الإلكتروني الاحتيالي خداع المستلمين للنقر فوق الروابط أو المرفقات الضارّة، ممّا يبيّن أهمية إذكاء وعي الموظفين وتدريبهم. وتمثّل عمليات التصيّد هذه 51 في المائة من الحالات[4]، وغالباً ما تؤدي إلى سرقة البيانات والابتزاز وإلحاق الضرر بسمعة العلامة التجارية. وبلغ متوسط تكلفة خرق البيانات في قطاع النقل 3.59 مليون دولار في عام 2022[5]، ومن المتوقّع أن تصل التكلفة الإجمالية للأضرار الناجمة عن مثل هذه الجرائم السيبرانية إلى 10.5 تريليون دولار بحلول عام 2025[6] في كافة المجالات.

---

(2) MarshMclennan Agency, A glitch on the road: cybersecurity trends facing the trucking and transportation industry, September 2024.

(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) MarshMclennan 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.

10- بالإضافة إلى ذلك، زاد عموماً استخدام برامج التجسّس وأحصنة طروادة للنفاذ عن بُعد (RATs). فأصبحت برامج التجسّس تمثّل 21 في المائة من حوادث البرامج الضارّة، كما تضاعفت نسبة أحصنة طروادة للنفاذ عن بُعد لتبلغ 15 في المائة. وتجدر الإشارة أنّ برامج التجسّس تجمع معلومات حسّاسة من دون موافقة المستخدِم، بينما تسمح أحصنة طروادة بالتحكّم عن بُعد بالأنظمة المصابة[7].

11- ويُعَدُّ الهجوم على شركة الشحن الدنماركية العملاقة "ميرسك" (Maersk) في عام 2017 من أبرز الأمثلة عن تأثير هذه البرامج على قطاع النقل. فقد تعرّضت هذه الشركة لهجوم برامج الفدية NotPetya، ممّا أثّر على عمليات الشحن الخاصة بها في أربعة بلدان مختلفة، وتسبّب في تأخيرات وانقطاعات استمرّت أسابيع، وتكبّدت من جرّائه الشركة أكثر من 200 مليون دولار.

12- تمثّل الهجمات المحدّدة الأهداف 83 في المائة من الهجمات السيبرانية الناجحة في المنطقة العربية[8]. وتُعَدُّ الجهات الحكومية من الأهداف الأكثر جاذبية للمهاجمين، فكانت عرضة لـ 22 في المائة من إجمالي الهجمات على المؤسسات. في المقابل، احتلت مؤسسات القطاع الصناعي، بما فيها تلك الموجودة في قطاع النقل، المرتبة الثانية بين المؤسسات الأكثر استهدافاً، فتلقّت 16 في المائة من الهجمات. وتمكّن المهاجمون من النفاذ إلى هذه الأنظمة إمّا بفضل الهندسة الاجتماعية في 33 في المائة من الحالات وإمّا باستخدام البرامج الضارّة مع أحصنة طروادة للنفاذ عن بُعد في 62 في المائة من الحالات.

13- وفي عام 2023، سجّل قطاع النقل في المنطقة العربية زيادة ملحوظة في الهجمات السيبرانية، وتحديداً باستخدام برامج الفدية. وفي هذا السياق، أشار تقرير مجموعة آي بي (IB group) إلى تعرّض قطاع النقل في المنطقة إلى ثماني هجمات سيبرانية. وكانت هذه الهجمات جزءاً من زيادةٍ بنسبة 68 في المائة في حوادث برامج الفدية في جميع أنحاء المنطقة. وكان قطاع النقل، إلى جانب قطاع الاتصالات السلكية واللاسلكية، عرضة إلى حدٍّ بعيد للتهديدات المستمرّة التي تنسّقها مجموعات معروفة بأنشطة التجسّس.

14- تزايد نشاط برامج الفدية في المنطقة العربية بنسبة 77 في المائة في الربع الأول من عام 2023 مقارنةً بالفترة نفسها من عام 2022[9]. وكانت الدول الأكثر استهدافاً في منطقة الخليج العربي هي الإمارات العربية المتحدة (33 في المائة) والمملكة العربية السعودية (29 في المائة) والكويت (21 في المائة). واستُخدمت البرامج الضارّة في نحو ثلثي الهجمات على المؤسسات، كونها تتيح للمهاجمين التحكّم في الأجهزة المخترَقة والبقاء داخل البنية التحتية. وبين أيار/مايو وحزيران/يونيو 2018[10]، استهدفت هجمات سيبرانية مؤسسات النقل والشحن في الكويت باستخدام أدوات اختراق مختلفة سمحت للمتسلّلين بمراقبة البيانات وسرقتها من الأنظمة المصابة. وفي أيار/مايو 2020، استُهدِفت وكالتا النقل الجوي في الكويت والمملكة العربية السعودية، وكان الهدف على الأرجح استكشاف البيانات الحساسّة واستخراجها. كذلك، تعرّضت شركة كريم (Careem)، وهي شركة ناشئة شهيرة

(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.

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

لتأجير السيارات في المنطقة العربية لاختراقٍ جسيمٍ لبياناتها في كانون الثاني/يناير 2018، فاستولى المخترقون على بيانات شخصية لزبائن الشركة، مثل الأسماء وعناوين البريد الإلكتروني وأرقام الهاتف وبيانات الرحلات.

ثانياً- أبرز المسارات العالمية في الأمن السيبراني

ألف- القمة العالمية لمجتمع المعلومات

15- انعقدت القمة الأولى لمجتمع المعلومات في جنيف عام 2003، والقمة الثانية في تونس عام 2005. وأعدّ المشاركون خريطة طريق لبناء مجتمع المعلومات ووضعوا إرشادات لسدّ الفجوة الرقمية العالمية بين أقلّ البلدان نموّاً من جهة وأكثرها نموّاً من جهة أخرى. ومذاك، تُعقد منتديات القمة العالمية لمجتمع المعلومات بصورة دورية.

16- عُقد منتدى القمة العالمية لمجتمع المعلومات لعام 2024 في جنيف من 27 إلى 31 أيار/مايو 2024. وركّز المشاركون فيه على استعراض التقدُّم المُحرَز ورسم مسار مستقبلي للقمة العالمية لمجتمع المعلومات. وخلصوا إلى أنّ الثقة والأمن هما من الركائز الأساسية لمجتمع المعلومات، وأنّه من الضروري تعزيز دور الجهات التنظيمية في القطاعات الرقمية.

17- وتناولت المناقشات اللاحقة أمن المعلومات والشبكات، والجرائم السيبرانية، والرسائل الاقتحامية، وسلامة الأطفال على الإنترنت. وساهمت أنشطة تنفيذ القرارات الصادرة عن القمة العالمية لمجتمع المعلومات في بناء القدرات وتعزيزها على الصعيدَين الوطني والإقليمي للتصدي لمختلف أشكال مخاطر الأمن السيبراني.

باء- الاتفاق الرقمي العالمي للأمم المتحدة

18- الاتفاق الرقمي العالمي للأمم المتحدة هو مبادرة اقترحتها الأمم المتحدة في الفترة 2023-2024، بهدف وضع إطارٍ شاملٍ للتعاون والحوكمة الرقميين. وهذه المبادرة هي جزءٌ من جهد أوسع نطاقاً لضمان استخدام التكنولوجيات الرقمية بأساليب شاملة وآمنة ومفيدة للجميع. وقُدّم الاتفاق الرقمي العالمي في مؤتمر القمّة المعني بالمستقبل الذي عُقد خلال الدورة التاسعة والسبعين للجمعية العامة في أيلول/سبتمبر 2024.

19- وتتلخص الأهداف الخمسة للاتفاق الرقمي العالمي، والتي تتعلق بطريقة أو بأخرى بالأمن السيبراني، بما يلي:

- سدّ الفجوات الرقمية وتسريع التقدّم في تحقيق كافة أهداف التنمية المستدامة.
- توسيع فرص الإدماج في الاقتصاد الرقمي.
- تعزيز مساحة رقمية شاملة ومنفتحة وآمنة ومأمونة.
- تعزيز الإدارة الدولية العادلة للبيانات.

- وضع أساليب تتيح استخدام التكنولوجيا الناشئة، بما في ذلك الذكاء الاصطناعي، على أفضل وجه في خدمة الإنسانية.

جيم- اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية

20- تركّز اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، التي تمّت المصادقة عليها في آب/أغسطس 2024، على تعزيز التعاون الدولي لمكافحة الجرائم المرتكبَة بواسطة أنظمة تكنولوجيا المعلومات والاتصالات.

21- وتشمل مجالات التركيز الرئيسية لهذه الاتفاقية ما يلي:

- **التعاون الدولي:** ينبغي أن تتعاون البلدان في ما بينها بشكلٍ أوثق للتصدي للجرائم السيبرانية، مع الاعتراف بأنّ هذا النوع من الجرائم غالباً ما يتجاوز الحدود الوطنية. ويشمل هذا التعاون المساعدة القانونية المتبادلة والتسليم والتحقيقات المنسّقة.
- **مكافحة الجرائم السيبرانية المحدّدة:** تحدّد الاتفاقية فئات الجرائم السيبرانية وتسعى إلى معالجتها، مثل الجرائم ضد سرية وسلامة وتوافر أنظمة الحاسوب والبيانات، فضلاً عن الجرائم مثل الاحتيال واستغلال الأطفال وتوزيع المحتوى غير القانوني عبر تكنولوجيا المعلومات والاتصالات.
- **تبادل الأدلة:** تقترح الاتفاقية آليات لتبادل الأدلة الإلكترونية المتعلقة بالجرائم الخطيرة بطريقة فعّالة. ويشمل ذلك إنشاء بروتوكولات للحفاظ على البيانات الإلكترونية وجمعها وتبادلها، وهو أمرٌ بالغ الأهمية في ملاحقة الجرائم السيبرانية.
- **بناء القدرات:** تسلّط الاتفاقية الضوء أيضاً على أهمية بناء القدرات في الدول الأعضاء لمعالجة الجرائم السيبرانية بفعاليّة. ويتضمن ذلك تقديم المساعدة الفنية والتدريب والموارد للدول النامية لتعزيز قدرتها على مكافحة التهديدات السيبرانية.
- **احترام حقوق الإنسان والحريات الأساسية:** يجب تحقيق التوازن بين إنفاذ الجرائم السيبرانية واحترام حقوق الإنسان والحريات الأساسية، وضمان عدم انتهاك التدابير الرامية إلى مكافحة الجرائم السيبرانية للخصوصية أو حرية التعبير أو غيرها من الحقوق.

ثالثاً- أمثلة عن خطط الأمن السيبراني من خارج المنطقة العربية

22- أصدرت وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA)[11] في عام 2020 إرشادات مفصّلة لمساعدة مشغّلي الموانئ في إدارة المخاطر السيبرانية. وتؤكد الإرشادات على اتّباع نَهجٍ قائم على المخاطر للأمن السيبراني، وتشجيع المشغّلين على تحديد أصولهم المتصلة بالإنترنت وحمايتها بشكلٍ منهجي. ويتضمن ذلك تقييم المخاطر السيبرانية المحتملة وتنفيذ تدابير أمنية مناسبة، مثل ضوابط النفاذ وتجزئة الشبكة والتحديثات المنتظمة لبروتوكولات الأمان.

(11) European Union Agency for Cybersecurity (ENISA), Cybersecurity in the Maritime Sector: ENISA Releases New Guidelines for Navigating Cyber Risk, December 2020.

23- بالإضافة إلى ذلك، أُصدِرت في الاتحاد الأوروبي في عام 2023 النسخة المحدّثة من توجيه أمن الشبكات والمعلومات (NIS2 Directive)[12]. والهدف الأساسي من هذا التوجيه تعزيز الموقف الأمني للمؤسسات من أجل التصدي للتهديدات السيبرانية الناشئة[13]، وهو تحديثٌ للإصدار الأول لتوجيه أمن الشبكات والمعلومات (NIS)[14] الذي هَدَفَ إلى تحقيق مستوى مرتفع من الأمن السيبراني عبر الدول الأعضاء. ومن شأن الإصدار الثاني من التوجيه إلزام المزيد من المؤسسات والقطاعات باتخاذ التدابير بفعاليّة، وزيادة مستوى الأمن السيبراني في أوروبا على المدى الطويل. ويركّز الإصدار الثاني عموماً على المؤسسات الأساسية في سلسلة توريد البنية التحتية الحيوية. وجرى العمل في تشرين الأول/أكتوبر 2024 على إصدارٍ بشأن المتطلبات التفصيلية سيدخل حيّز التنفيذ في كانون الثاني/يناير 2025. ويفرض الاتحاد الأوروبي، بموجب هذا التوجيه، عقوبات مالية ملموسة على المؤسسات التي تخفق في الامتثال ضمن الإطار الزمني المحدّد. وينطبق هذا التوجيه على الجهات العامة والخاصة على السّواء، وهو يغطي قطاع النقل بوصفه من القطاعات الحيوية في الاتحاد الأوروبي. وتتضمن التدابير التي ينصّ عليها التوجيه ما يلي: تحليل المخاطر وسياسات أمن المعلومات؛ والتعامل مع الحوادث؛ وأمن سلسلة التوريد؛ وأمن الموارد البشرية وسياسات التحكم في النفاذ وإدارة الأصول.

24- يقسّم الإصدار الثاني من توجيه أمن الشبكات والمعلومات الجهات المعنيّة إلى فئتين: "الفئة الأساسية" و"الفئة المهمّة". ويجب أن تمتثل الفئتان لتدابير الأمن نفسها، لكنّ مؤسسات الفئة الأساسية تخضع لإشرافٍ استباقيّ، في حين أن مؤسسات الفئة المهمّة لا تُراقَب إلاّ بعد الإبلاغ عن حادثة عدم امتثال.

25- وصدر في عام 2024 قانون المرونة السيبرانية (CRA)[15] الذي يهدف إلى حماية المستهلكين والشركات التي تشتري المنتجات والبرامج ذات المكوّنات الرقمية أو تستخدمها. ويركّز القانون على تقديم متطلبات الأمن السيبراني الإلزامية لمصنّعي هذه المنتجات والتجار الذين يبيعونها بالتجزئة، مع التركيز على ضرورة استمرار هذه الحماية طوال دورة حياة المنتجات. ودخل قانون المرونة السيبرانية حيّز التنفيذ في 10 تشرين الأول/أكتوبر 2024 ويتعيّن بموجبه على الشركات المصنّعة طرح المنتجات المتوافقة في سوق الاتحاد بحلول عام 2027. ويضمن قانون المرونة السيبرانية ما يلي:

- توفير معايير موحّدة عند طرح المنتجات أو البرامج ذات المكوّنات الرقمية في السوق.
- توفير إطار لمتطلبات الأمن السيبراني التي تنظّم التخطيط لهذه المنتجات وتصميمها وتطويرها وصيانتها، مع الالتزامات الواجب الوفاء بها في كلّ مرحلة من مراحل سلسلة القيمة.
- الالتزام بتوفير واجب الرعاية طوال دورة حياة هذه المنتجات.

(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.

(15) European Commission, EU Cyber Resilience Act, July 2024.

26- وفي الولايات المتحدة الأمريكية، أصدرت إدارة أمن النقل (TSA)[16] في عام 2021 توجيهات أمنية جديدة لتعزيز مرونة الأمن السيبراني داخل قطاع النقل. وتستهدف هذه التوجيهات تحديداً المناطق الأخطر مثل السكك الحديدية للشحن والركاب. وتشمل التدابير الأساسية إلزام المالكين والمشغّلين بتعيين منسّق للأمن السيبراني ليكون مسؤولاً عن الإشراف على ممارسات الأمن السيبراني والاستجابة للعوامل المهدِّدة. بالإضافة إلى ذلك، يتعيّن عليه الإبلاغ عن حوادث الأمن السيبراني إلى وكالة الأمن السيبراني وأمن البنية التحتية (CISA) في غضون 24 ساعة لضمان الاستجابة السريعة للتهديدات المحتملة. وتُلزِم هذه التوجيهات أيضاً المالكين والمشغّلين بتطوير وتنفيذ خطة شاملة للاستجابة لحوادث الأمن السيبراني بهدف الحدّ من مخاطر الاضطرابات التشغيلية الناجمة عن الحوادث السيبرانية. كما تُلزِمهم بإتمام تقييم لمَواطن الضعف في الأمن السيبراني في سبيل تحديد الثغرات المحتملة في نظامهم.

27- أمّا في كندا، فتحدّد استراتيجية الأمن السيبراني للمَرْكَبات التابعة لوزارة النقل الكندية أهدافاً وأولويات مستقبلية للأمن السيبراني للمَرْكَبات بهدف تعزيز المرونة السيبرانية للنقل البرّي[17]. وتساعد الاستراتيجية الوزارة على تحقيق رؤيتها المتمثلة في الاستمرار في كونها رائدة في ضمان بيئة آمنة ومرنة للأمن السيبراني للمَرْكَبات. وتتضمن الاستراتيجية ثلاثة أهداف شاملة للأمن السيبراني للنقل البرّي، وهي:

- الهدف 1: دمج اعتبارات الأمن السيبراني للمَرْكَبات في أُطُر السياسات والأُطُر التنظيمية. ويشمل هذا الهدف عدداً من الأولويات، مثل توفير الإرشادات والأدوات والسياسات غير التنظيمية، وتحديث الأُطُر التنظيمية وأُطُر السياسات لضمان بيئة تنظيمية مرنة وسريعة الاستجابة تعزّز ابتكار المَرْكَبات الذاتية القيادة وتوفّر المرونة اللازمة.
- الهدف 2: نشر الوعي وتعزيز نَهج حديث ومبتكر للأمن السيبراني للمَرْكَبات. ويشمل ذلك عدداً من الأولويات، منها المشاركة النشطة في المنتديات الفيدرالية والإقليمية، والبحث والاختبار والتحقّق، والتوعية العامة والتثقيف بشأن الأمن السيبراني للمَرْكَبات.
- الهدف 3: معالجة القضايا الناشئة في مجال الأمن السيبراني للمَرْكَبات. ويتضمن ذلك حماية الخصوصية وإدارة المعلومات الشخصية، وضمان أمن البنية التحتية الرقمية، وضمان أمن سلسلة التوريد.

رابعاً- الأمن السيبراني في المنطقة العربية

ألف- نظرة عامة

28- يختلف نُضج أنظمة الأمن السيبراني إلى حدٍّ بعيد بين بلدان المنطقة العربية. فيحتلّ بعضها المراتب الأعلى على مستوى العالم من حيث أدائه في هذا المجال بينما يقع البعض الآخر في الربع الأقلّ تقدّماً. ومن المتوقع أن ينمو سوق الأمن السيبراني في المنطقة العربية بنحو 20 في المائة سنوياً على مدى السنوات السبع

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

(17) Department of Transport Canada, Transport Canada's Vehicle Cyber Security Strategy, 2021.

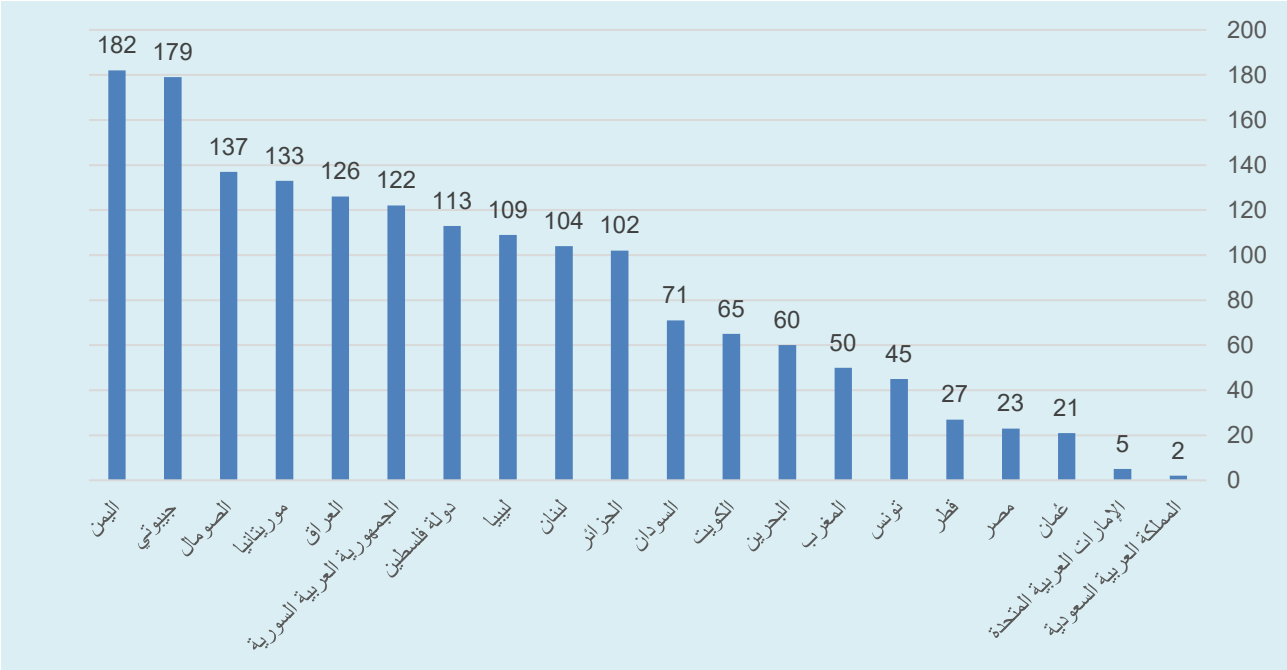
المقبلة[18]. وسيتركّز هذا النموّ في البلدان ذات الصناعات القوية في مجال الأمن السيبراني والسياسات الحكومية، ممّا يجعلها الوجهات المفضّلة للصناعة والأكاديميين والشركات والبحث والابتكار.

29- ويقدّم مؤشر الأمن السيبراني العالمي لعام 2021 رؤية كميّة عن أداء المنطقة العربية في مجال الأمن السيبراني. ويقيس هذا المؤشر الصادر عن الاتحاد الدولي للاتصالات خمسة أبعاد هي: الجوانب القانونية، والجوانب الفنية، والجوانب التنظيمية، وبناء القدرات، والتعاون[19].

30- وبحسب هذا المؤشر، تحتلّ سبعة بلدان عربية مراتب بين أعلى 50 بلداً، بينما تَشْغل ثلاثة بلدان عربية أخرى مراتب بين 51 و100، وتقع عشرة بلدان عربية بين المراتب 101 و182 (الشكل 1).

31- ويبلغ متوسط الدرجات التي سجّلتها بلدان المنطقة العربية 49.86 في المائة، وهو أقلّ من متوسط الدرجات التي سجّلتها كلّ الاقتصادات النامية (59.18 في المائة) وأقلّ بكثير من متوسط الدرجات التي سجّلتها كلّ الاقتصادات المتقدّمة (91.8 في المائة).

الشكل 1- الترتيب العالمي للبلدان العربية في مؤشر الأمن السيبراني العالمي (2021)



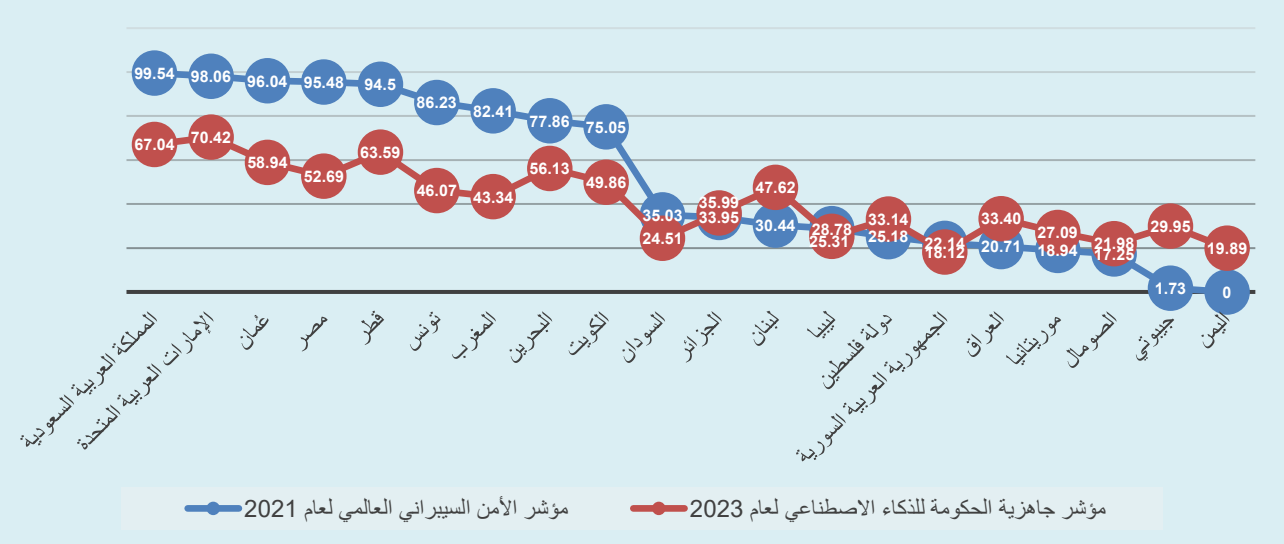
المصدر: تجميع الإسكوا استناداً إلى مؤشر الأمن السيبراني العالمي لعام 2021 الصادر عن الاتحاد الدولي للاتصالات. متاح على الموقع: https://www.itu.int/pub/D-STR-GCI.01-2021 (تموز/يوليو 2024).

(18) PWC, Digital Trust Insights – Middle East findings, 2024.

(19) ITU, Global Cybersecurity Index, 2021.

32- وتسجّل المنطقة العربية اتساقاً كبيراً بين ترتيب بلدٍ ما في مؤشر الأمن السيبراني العالمي وترتيبه في مؤشر جاهزية الحكومة للذكاء الاصطناعي الذي يقيس مدى الاستعداد الحكومي لتطبيقات الذكاء الاصطناعي، على الرغم من استثناءاتٍ في بعض البلدان. ويبلغ معامل الترابط بين مؤشر الأمن السيبراني العالمي لعام 2021 ومؤشر جاهزية الحكومة للذكاء الاصطناعي لعام 2023 نسبة 95.27 في المائة، ممّا يشير إلى أنّ البلدان التي تتمتّع بنظام قوي للأمن السيبراني هي عموماً في وضع أفضل لنشر تطبيقات الذكاء الاصطناعي في القطاع العام.

الشكل 2- مقارنة بين مؤشر جاهزية الحكومة للذكاء الاصطناعي ومؤشر الأمن السيبراني العالمي



المصدر: تجميع الإسكوا استناداً إلى مؤشر الأمن السيبراني العالمي لعام 2021 التابع للاتحاد الدولي للاتصالات ومؤشر جاهزية الحكومة للذكاء الاصطناعي المتاح على الموقع: https://oxfordinsights.com/ai-readiness/ai-readiness-index/.

باء- التحديات في المنطقة العربية

33- تعيق تحديات عدّة تطوير بيئة رقمية آمنة وموثوقة في المنطقة العربية، ممّا يُبرز المخاوف التي يتناولها الاتفاق الرقمي العالمي للأمم المتحدة. وتشمل هذه التحديات ما يلي:

(أ) **نقص الوعي:** يفتقر العديد من المواطنين إلى المعرفة الأساسية بالأمن السيبراني، ممّا يجعلهم عُرضة لهجمات التصيّد الإلكتروني الاحتيالي والبرامج الضارّة وعمليات الاحتيال عبر الإنترنت. ويتجلّى ذلك في تركيز الاتفاق الرقمي العالمي على الأمن الرقمي؛

(ب) **البنية التحتية التكنولوجية غير الكافية:** تتفاوت مستويات تطوير البنية التحتية الرقمية في المنطقة. وتفتقر بعض البلدان إلى مراكز البيانات الآمنة الكافية أو شبكات الاتصالات المتقدّمة بما فيه الكفاية. وتمّ إبراز ذلك في الاتفاق الرقمي العالمي الذي أكّد على أهمية سدّ الفجوة الرقمية؛

(ج) **الثغرات التشريعية:** لا تكون قوانين الجرائم السيبرانية واللوائح التنظيمية لحماية البيانات محدّدة جيداً أو متناغمة في كافة البلدان العربية، ممّا يعيق نَهج أصحاب المصلحة المتعدّدين الذي يدعو إليه الاتفاق الرقمي العالمي. ولا تزال بعض البلدان العربية تفتقر إلى استراتيجيات وطنية محدّثة؛

(د) **التعاون المحدود:** برزت الحاجة إلى المزيد من التعاون الإقليمي والدولي في تبادل المعلومات الاستخباراتية والاستجابات المنسّقة لتهديدات الأمن السيبراني.

خامساً- مبادرات إقليمية لتعزيز الأمن السيبراني

ألف- الاستراتيجية العربية للأمن السيبراني

34- في عام 2022، قدّمت المنظمة العربية لتكنولوجيات الاتصال والمعلومات[20] الاستراتيجية العربية للأمن السيبراني للفترة 2023-2027 التي توفّر خريطة طريق يمكن أن تتبعها البلدان العربية لتقوية أمنها السيبراني. وتحدّد هذه الاستراتيجية المبادرات التي ستنفّذها الحكومات العربية على مدى السنوات الخمس المقبلة لتعزيز اعتماد وتطوير ضوابط للأمن السيبراني معترَف بها عالمياً. وترمي الاستراتيجية إلى رفع مستوى نُضج الأمن السيبراني في جميع أنحاء المنطقة العربية، وتحصين الفضاء السيبراني في وجه التهديدات الرقمية المتطوّرة باستمرار.

35- وتنصّ رؤية الاستراتيجية العربية للأمن السيبراني على ما يلي: "نحو مجتمع عربي آمن وشامل ومتكامل في الاقتصاد الرقمي العالمي، وحلول وخبرات مكتفية ذاتياً تدعم الثقة الرقمية داخل الفضاء السيبراني العربي". وتتمثل أهدافها في ما يلي:

(أ) إنشاء آليات تشاركية تشمل سوق الأمن السيبراني في المنطقة؛

(ب) تطوير القدرات المتخصّصة في مجال الأمن السيبراني، وتعزيز المشاركة المهنية والطلابية، وبناء القدرات، وإنشاء نظام تدريب متكامل للأمن السيبراني؛

(ج) تعزيز الوعي المجتمعي بالأمن السيبراني والمخاطر المتعلقة بالإنترنت، والدعوة إلى ممارسات رقمية آمنة، وتشجيع المؤسسات على تعزيز الوعي بالأمن الرقمي بصورة فعّالة؛

(د) تنظيم مسابقات تدعم التميّز في مجال الأمن السيبراني عن طريق برامج الجوائز، وتشجيع المؤسسات على إطلاق مبادرات الأمن السيبراني، والحثّ على الابتكار في مجال ريادة الأعمال، ودعم البحوث الإبداعية في المؤسسات الأكاديمية، وإشراك الطلاب في مجال الأمن السيبراني؛

(ه) تنظيم آليات الكشف عن حوادث الأمن السيبراني والإبلاغ عنها؛

(و) وضع منهجية موحّدة لتقييم مدى خطورة حوادث الأمن السيبراني بهدف تقديم الدعم المناسب؛

---

(20) المنظمة العربية لتكنولوجيات الاتصال والمعلومات هي منظمة حكومية عربية تعمل تحت راية جامعة الدول العربية، وتساهم في تطوير تكنولوجيات المعلومات والاتصال في البلدان العربية وتوفير الآليات الضرورية لدعم التعاون والتكامل في هذا المجال بين أعضاء المنظمة. كما تسعى إلى تطوير سياسات واستراتيجيات مشتركة لتحقيق النفاذ العادل والمستدام إلى التكنولوجيا وتطويعها لخدمة أهداف التنمية الاقتصادية.

(ز) زيادة قدرات البلدان العربية على الاستجابة لشتّى أنواع حوادث الأمن السيبراني؛

(ح) تصميم إطار قانوني وتنظيمي شامل للأمن السيبراني لمكافحة الجرائم السيبرانية، وحماية التكنولوجيات الحالية والناشئة، وتطوير أنظمة داعمة لحماية الشركات الصغيرة والمتوسطة من تهديدات الأمن السيبراني.

باء- المركز العربي الإقليمي للأمن السيبراني

36- أُنشئ المركز العربي الإقليمي للأمن السيبراني التابع للاتحاد الدولي للاتصالات في كانون الأول/ديسمبر 2012 نتيجةً للتعاون بين الاتحاد الدولي للاتصالات وعُمان، ممثلةً بوزارة النقل والاتصالات وتقنية المعلومات. ويهدف المركز إلى توفير بيئة أكثر أماناً وتعاوناً للأمن السيبراني في المنطقة العربية. وأُطلق المركز العربي الإقليمي للأمن السيبراني رسمياً في 3 آذار/مارس 2013، ويستضيفه ويديره المركز الوطني للسلامة المعلوماتية.

37- وتتمثّل بعض أهداف المركز العربي الإقليمي للأمن السيبراني التابع للاتحاد الدولي للاتصالات في ما يلي:

(أ) الحثّ على اعتماد البرنامج العالمي للأمن السيبراني الخاص بالاتحاد الدولي للاتصالات في جميع أنحاء المنطقة العربية؛

(ب) تقديم المساعدة وتلبية الاحتياجات في ما يتعلق بالأمن السيبراني لأقلّ البلدان نموّاً في المنطقة.

38- ويضطلع المركز العربي الإقليمي للأمن السيبراني بالمهام التالية:

(أ) **استراتيجية الأمن السيبراني والحوكمة:** يعمل خبراء المركز العربي الإقليمي للأمن السيبراني بشكل وثيق مع الحكومات وهيئات القطاع العام لصياغة استراتيجيات وطنية للأمن السيبراني، وتحديد المسؤوليات بوضوح. وتشمل هذه الاستراتيجيات برامج ومبادرات تهدف إلى تعزيز قدرات الأمن السيبراني ومعالجة الثغرات في نظام الأمن السيبراني؛

(ب) **الجانب الفني في مجال الأمن السيبراني:** يستخدم خبراء المركز العربي الإقليمي للأمن السيبراني معايير فنية معترف بها ومعايير دولية (مثل معيار ISO 27001) لمساعدة الدول الأعضاء في الاتحاد الدولي للاتصالات في تحسين قدراتها في مجال الأمن السيبراني؛

(ج) **بناء القدرات في مجال الأمن السيبراني:** ينفِّذ المركز العربي الإقليمي للأمن السيبراني مبادرات لبناء قدرات المؤسسات في مجال الأمن السيبراني. ويسعى أيضاً إلى زيادة الوعي بالأمن السيبراني عن طريق الحملات المجتمعية والمنتديات وبرامج التدريب والتطوير على المستوى الوطني؛

(د) **إدارة الحوادث:** يتعاون المركز العربي الإقليمي للأمن السيبراني مع شركائه لدعم الدول الأعضاء في الاتحاد الدولي للاتصالات في إنشاء فِرق وطنية للاستجابة لحوادث السلامة المعلوماتية تعمل كنقاط تنسيق

مركزية للأمن السيبراني. وتقوم خدمة الاستجابة للحوادث في المركز العربي الإقليمي للأمن السيبراني بتقييم قدرات فِرق الاستجابة الخاصة بالحكومة والقطاع العام، وتحديد الثغرات، واقتراح التحسينات.

جيم- مجلس وزراء الأمن السيبراني العرب

39- أنشأ المجلسُ الاقتصادي والاجتماعي لجامعة الدول العربية مجلسَ وزراء الأمن السيبراني العرب في عام 2023، بناءً على اقتراحٍ من المملكة العربية السعودية[21]. ويسعى المجلس إلى تعزيز التعاون بين البلدان العربية في كافة الجوانب المتعلقة بالأمن السيبراني، والعمل على تحفيز النموّ والازدهار من خلال ضمان أن تكون البنية التحتية الرقمية في المنطقة العربية آمنة وموثوقة.

40- ويمكن إيجاز أهم أهداف المجلس بما يلي:

(أ) تطوير وتعزيز التعاون في مجال الأمن السيبراني، وتيسير تبادل المعرفة والخبرات؛

(ب) حماية مصالح الدول الأعضاء في منظمات الأمن السيبراني الدولية عن طريق تحديد موقف عربي موحّد؛

(ج) المساهمة في إرساء أمن وموثوقية البنية التحتية الرقمية العربية على نحوٍ يفضي إلى نموّ جميع الدول الأعضاء وازدهارها؛

(د) تنسيق الجهود بين البلدان العربية في كافة المجالات المتعلقة بالأمن السيبراني.

دال- أنشطة الإسكوا في مجال الأمن السيبراني

41- بدأت الإسكوا بالاهتمام بتعزيز البيئة المحيطة بالأمن السيبراني منذ أكثر من 10 سنوات. فأصدرت في عام 2011 إرشادات الإسكوا لتنسيق التشريعات السيبرانية في المنطقة العربية. وفي عام 2020 أصدرت تقريراً بعنوان التكنولوجيا والابتكار من أجل تطوير النقل البرّي في البلدان العربية، الذي جاء ثمرة تعاونٍ بين مجموعة النقل ومجموعة المعلومات والتكنولوجيا، وتطرّق إلى أمن البيانات والمعلومات في عددٍ من فقراته. وأخيراً في عام 2024 أصدرت الإسكوا تقريراً عن الثقة الرقمية والتكنولوجيات الناشئة.

42- بالإضافة إلى ذلك، تعمل الإسكوا على تقديم الدعم الفني للجهات الحكومية في الدول العربية لتطوير خططها الوطنية والقطاعية في مجال الأمن السيبراني.

سادساً- أمثلة عن الخطط الوطنية للأمن السيبراني في المنطقة العربية

43- أصدر العديد من بلدان المنطقة العربية استراتيجيات وطنية لتحسين البيئة المحيطة بالأمن السيبراني، ممّا يؤثر إيجاباً في تعزيز الأمن السيبراني وحماية البنى التحتية الحيوية، بما في ذلك قطاع النقل.

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

ألف- المغرب

44- تحدّد الاستراتيجية الوطنية للأمن السيبراني التي وضعتها المديرية العامة لأمن نُظُم المعلومات في عام 2012 بوصفها سلطة وطنية تشرف على الأمن السيبراني، المجالات التي يستلزم فيها إطار الأمن السيبراني في البلد تحسيناً عاجلاً، وهي:

(أ) **تقييم المخاطر:** تقييم المخاطر التي تؤثر على أنظمة المعلومات في المؤسسات الحكومية والعامة والبنى التحتية الحيوية؛

(ب) **الحماية والدفاع:** تنفيذ التدابير اللازمة لحماية أنظمة المعلومات والدفاع عنها؛

(ج) **أُسس أمن تكنولوجيا المعلومات:** تحسين الجوانب الأساسية لأمن تكنولوجيا المعلومات عبر مختلف القطاعات، بما في ذلك الأُطُر القانونية وبرامج التوعية ومبادرات بناء القدرات والبحث والتطوير؛

(د) **التعاون:** تعزيز التعاون الوطني والدولي لتحسين قدرات الأمن السيبراني عموماً.

45- وتطبّق الاستراتيجية مبدأ "الأمن في التصميم" من خلال دمج التدابير الأمنية في بداية عملية تطوير الأنظمة والخدمات. وتتضمن هذه الاستراتيجية برامج توعية وورش عمل تدريبية بشأن أفضل الممارسات لمكافحة الجرائم السيبرانية.

46- وأصدرت المديرية العامة لأمن نُظُم المعلومات نسخة جديدة من الاستراتيجية الوطنية للأمن السيبراني في البلد في عام 2024. وتؤكد الاستراتيجية المحدّثة على تعزيز الأمن ومرونة الفضاء السيبراني، لا سيّما مع ظهور تهديدات جديدة. وتتصدّر رؤية هذه الاستراتيجية على ما يلي: "من أجل فضاء سيبراني وطني موثوق وآمن وصامد، قادر على دعم التحوّل الرقمي في المملكة وتعزيز الازدهار الاقتصادي وضمان رفاهية المواطنين".

47- وتقوم الاستراتيجية المحدّثة على المحاور التالية: تطوير آليات التنسيق الوطنية، وتحديث وتعزيز الإطار القانوني والمعياري، ودعم عملية صنع القرار واعتماد سياسات قائمة على البيانات، وتعزيز القدرات الوطنية في مجال الوقاية والإدارة والاستجابة للحوادث والأزمات السيبرانية، وتعزيز حماية أنظمة معلومات البنى التحتية ذات الأهمية الحيوية أمام المخاطر، وتطوير ثقافة الأمن السيبراني داخل المجتمع، ودعم المنظومة الوطنية للأمن السيبراني، وتشجيع الابتكار، وتقوية وتعزيز الحضور الوطني على المستويَين الإقليمي والدولي في قضايا الأمن السيبراني.

باء- مصر

48- كَشَفَ مؤخراً المجلس الأعلى للأمن السيبراني في مصر عن الاستراتيجية الوطنية للأمن السيبراني 2023-2027. وتتمثّل رؤية هذه الاستراتيجية في جعل البنية التحتية الرقمية للبلد آمنة ومرنة ومواتية للازدهار الاقتصادي، وتشمل مجالات تركيزها الرئيسية ما يلي:

(أ) **بناء إطار تشريعي متكامل:** صياغة قوانين ولوائح تنظيمية شاملة للتصدي بفعاليّة للمخاوف المرتبطة بالأمن السيبراني؛

(ب) **تغيير ثقافة المجتمع حول الأمن السيبراني:** تعزيز برامج التوعية والتعليم لغرس ثقافة الوعي بالأمن السيبراني والمسؤولية بين المواطنين المصريين؛

(ج) **تعزيز الشراكة الوطنية:** تعزيز التعاون بين الجهات الحكومية، والقطاع الخاص، والأوساط الأكاديمية، والمجتمع المدني للتعزيز الجماعي لتدابير الأمن السيبراني؛

(د) **بناء دفاعات سيبرانية قوية وقادرة على الصمود:** تنفيذ تدابير قوية في مجال الأمن السيبراني للدفاع وإقامة بنية تحتية صلبة للحماية من تهديدات الأمن السيبراني وضمان مرونة الأنظمة الحيوية؛

(هـ) **تشجيع البحث العلمي وتعزيز الابتكار والنموّ:** دعم المبادرات البحثية وتعزيز الابتكار في تكنولوجيات وممارسات الأمن السيبراني لدفع النموّ الاقتصادي؛

(و) **تعزيز التعاون الدولي:** التواصل مع الشركاء والمنظمات الدولية لتبادل أفضل الممارسات والخبرات والمعلومات لبذل جهود جماعية في مجال الأمن السيبراني.

جيم- الأردن

49- حدّدت أحدث وثيقة للاستراتيجية الوطنية للأمن السيبراني 2018-2023 في الأردن نَهجاً شاملاً للأمن السيبراني، وهي تتضمن الركائز الخمس التالية:

(أ) **حماية البنى التحتية الحيوية:** التزمت الحكومة بحماية البنية التحتية الحيوية. وشمل هذا الالتزام المرافق المادية مثل النقل ومحطات توليد الطاقة ومرافق معالجة المياه بالإضافة إلى البنية التحتية السيبرانية مثل الإنترنت وشبكات الاتصالات؛

(ب) **بناء بيئة رقمية مرنة:** وُجِّهت الجهود نحو تعزيز بيئة رقمية مرنة عن طريق تشجيع تبنّي الممارسات والتكنولوجيات الآمنة. وكان تعزيز قدرات القطاعَين العام والخاص على التصدي للهجمات السيبرانية جانباً رئيسياً من جوانب هذه الركيزة؛

(ج) **تعزيز التعاون الدولي:** هدفت الحكومة إلى تعزيز التعاون الدولي في مجال الأمن السيبراني بتبادل المعلومات وأفضل الممارسات. وأُعطِيَت الأولوية للجهود التعاونية مع الدول الأخرى للاستجابة بفعاليّة لتهديدات الأمن السيبراني؛

(د) **مساعدة المواطنين والشركات:** اتُّخِذت مبادرات لمساعدة المواطنين والشركات على الدفاع عن أنفسهم ضد الهجمات السيبرانية. وشمل ذلك زيادة الوعي بمخاطر الأمن السيبراني وتوفير الموارد والدعم لتعزيز القدرة على الصمود؛

(هـ) **بناء قوة عاملة قوية في مجال الأمن السيبراني:** سعت الحكومة إلى رعاية قوة عاملة قوية في مجال الأمن السيبراني عن طريق تقديم فرص التعليم والتدريب في هذا المجال. كما سعت إلى استحداث فرص عمل إضافية في قطاع الأمن السيبراني.

50- ويُعَدُّ قطاع النقل قطاعاً حيوياً للاقتصاد الأردني. وتضمّنت الخطة الاستراتيجية لوزارة النقل 2024-2026 في الأردن الرؤية التالية: "قطاع نقل مواكِب للتطوّرات وآمن يساهم في جعل الأردن مركزاً محورياً للنقل". وشدّدت ركائز الاستراتيجية على تضمين التكنولوجيات الابتكارية من جهة، والحفاظ على الأمن والسلامة من جهة أخرى.

دال- الجمهورية العربية السورية

51- تسعى استراتيجية الأمن السيبراني للجمهورية العربية السورية، التي تمّ تطويرها بالتعاون مع الإسكوا في عام 2023، إلى تحقيق الرؤية التالية: "فضاء سيبراني آمن وموثوق في جميع المجالات، بما يسهم في حماية المصالح الوطنية ويعزِّز الثقة في التحوّل الرقمي".

52- وتشمل الاستراتيجية ستة برامج رئيسية هي: أمن البنية التحتية، وتطوير الإطار القانوني والتنظيمي، ونشر ثقافة الوعي السيبراني، وبناء القدرات والمعرفة، والشراكات والتعاون الإقليمي والدولي، وتطوير هياكل وظيفية متخصّصة.

53- وتشرف اللجنة العليا للتحوّل الرقمي على تنفيذ الاستراتيجية. وتنسّق لجنة وطنية للأمن السيبراني مع كلّ هيئة وطنية بشأن تنفيذ مشاريع الأمن السيبراني، ممّا يضمن التنسيق والتعاون الفعّالين بين الهيئات الحكومية.

هاء- المملكة العربية السعودية

54- تقوم الاستراتيجية الوطنية للأمن السيبراني في المملكة العربية السعودية (2023-2027)، التي أُطلقت في عام 2022، على الركائز الخمس التالية:

(أ) **حماية الأمن السيبراني والدفاع عنه:** تطوير قدرات الدفاع عن الأمن السيبراني لحماية استقرار حكومة البلد والأنظمة الاقتصادية. وينطوي ذلك على تعزيز القدرات الفنية والقانونية والتنظيمية للتعامل بفعاليّة مع تهديدات الأمن السيبراني؛

(ب) **تطوير البنية التحتية للأمن السيبراني:** التركيز على تعزيز البنية التحتية للأمن السيبراني في القطاعَين العام والخاص في جميع أنحاء المملكة العربية السعودية. ويستلزم هذا الأمر وضع معايير وبرامج للأمن السيبراني وتعزيز التشريعات القائمة؛

(ج) **التعاون:** تعزيز التعاون بين القطاع الخاص والجهات الحكومية والمؤسسات الدولية لتحسين الأمن السيبراني. ويتضمن ذلك تسهيل تبادل المعلومات والخبرات، وتعزيز التعاون في مجال مكافحة الجرائم السيبرانية، وتمتين القدرات الوطنية؛

(د) **التوعية والتدريب:** زيادة الوعي بالأمن السيبراني بين المؤسسات والأفراد في المملكة العربية السعودية. وتشمل هذه التدابير برامج التدريب والتوعية، فضلاً عن المبادرات الرامية إلى زيادة المهارات الفنية في مجال الأمن السيبراني؛

(هـ) **التشريعات:** تعزيز التشريعات المتعلقة بالأمن السيبراني وضمان توافقها مع المعايير الدولية. ويتمّ التركيز على تطوير إطار قانوني قوي وآليات إنفاذ فعّالة لمكافحة الجرائم السيبرانية، وفي الوقت نفسه حماية البيانات الحسّاسة والخصوصية.

55- ووضعت الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية أُطُراً وإرشادات شاملة لتعزيز الأمن السيبراني عبر مختلف القطاعات، بما في ذلك قطاع النقل[22]. وتُجري الهيئة الوطنية للأمن السيبراني عمليات تدقيق وتقييمات أمنية منتظمة لتحديد مَواطن الضعف في البنى التحتية الحيوية. كما يجري تنفيذ تقنيات وحلول الأمن السيبراني المتقدّمة لحماية هذه البنى التحتية، ويتمّ توفير برامج تدريبية مكثّفة للموظفين لتعزيز قدرتهم على اكتشاف التهديدات السيبرانية والاستجابة لها. وتهدف هذه الجهود إلى زيادة مرونة الأمن السيبراني لقطاع النقل في البلد وحماية بنيته التحتية الحيوية من التهديدات السيبرانية المحتملة.

واو- عُمان

56- طوّرت وزارة النقل والاتصالات وتقنية المعلومات في عُمان أُطُراً شاملة للأمن السيبراني لحماية البنية التحتية، بما في ذلك النقل[23]. وتُجرى تقييمات منتظمة للمخاطر لتحديد التهديدات السيبرانية المحتملة، وتطوير وتنفيذ سياسات وإجراءات الأمن السيبراني المصمّمة خصيصاً لمعالجة هذه التهديدات.

57- وفي السياق نفسه، أطلق المركز العربي الإقليمي للأمن السيبراني في عُمان وحدة نضج استراتيجية تطوير صناعة الأمن السيبراني (CIDSMM) لتعزيز الأمن السيبراني في المنطقة العربية. ويوفّر هذا البرنامج للسلطات التنظيمية وأصحاب المصلحة في مجال الأمن السيبراني دليلاً شاملاً يتيح لهم تقييم قدراتهم في هذا المجال وتحسينها. كما يركّز على زيادة مرونة البنية التحتية الحيوية، بما في ذلك قطاع النقل، عن طريق المراقبة المستمرّة وتقييم المخاطر وتنفيذ أفضل الممارسات في مجال الأمن السيبراني.

سابعاً- المقترحات الختامية

58- تتّسم المنطقة العربية بالقدرة على أن تصبح رائدة في العصر الرقمي عن طريق توجيه جهود التحوّل الرقمي نحو القطاعات الأساسية، وأهمّها قطاع النقل. وبإعطاء الأولوية للأمن السيبراني وتعزيز الثقة والتعاون الإقليمي، يمكن للدول العربية إنشاء بيئة رقمية آمنة ومزدهرة تعود بالنفع على جميع المواطنين والمؤسسات العامة والخاصة.

59- يمكن للمقترحات التالية أن تساعد، إن نُفِّذت، في بناء فضاء رقمي أكثر أماناً وثقةً في المنطقة العربية:

(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.

- تطوير خطة عمل قطاعية لتعزيز الأمن السيبراني في مجال النقل، بما يتوافق مع الاستراتيجيات الوطنية للأمن السيبراني التي تمّ (أو يجري) تطويرها في كلّ دولة عربية.
- رفع الوعي للعاملين في مجال النقل بشأن أهمية الأمن السيبراني والمخاطر التي تتهدّده، لا سيّما مع التبنّي المتزايد للتكنولوجيات الناشئة. ومن الضروري أن يشمل ذلك أيضاً التوعية بالإجراءات الاحترازية الممكن اتباعها للحدّ من هذه المخاطر.
- تعزيز البنية التحتية للأمن السيبراني: ينبغي للحكومات والجهات الخاصة الاستثمار في البنية التحتية للأمن السيبراني، بما في ذلك مراكز البيانات الآمنة، وتطبيق الحوسبة السحابية الحكومية، وتقنيات التشفير، وأنظمة الكشف عن التهديدات المتقدّمة.
- إجراء تقييمات شاملة للمخاطر، لا سيّما في القطاعات الحيوية مثل قطاع النقل، وتطوير خطط فاعلة للاستجابة للحوادث، وضمان الامتثال لمعايير الأمن السيبراني وأنظمته الحالية.
- تطوير إطار قانوني ملائم: من الضروري أن يكون لدى الدول العربية قوانين شاملة لمكافحة الجرائم السيبرانية وحماية البيانات، تعالج التهديدات الناشئة وتحمي خصوصية المستخدِم، بما يتماشى مع مبادئ الاتفاق الرقمي العالمي واتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية. ومن الضروري أيضاً توفير نَهج شامل للأمن السيبراني في قطاع النقل، وضمان دمج التكنولوجيات الرقمية والتشغيلية بصورة آمنة، وتحسين تبادل معلومات التهديدات، وتعزيز الشراكات بين القطاعَين العام والخاص.
- الاستثمار في التعليم عن الأمن السيبراني: ينبغي للدول العربية تنظيم حملات توعية وطنية وبرامج تعليمية لتزويد المواطنين بالمهارات الأساسية للأمن السيبراني للتنقُّل في العالم الرقمي بأمانٍ، وتمكينهم من الاستخدام الآمن للمنصّات والخدمات الرقمية في كافة القطاعات، بما في ذلك قطاع النقل.
- إشراك القطاع الخاص: تُعَدُّ الشراكات بين القطاعَين العام والخاص أمراً بالغ الأهمية لبناء بيئة رقمية مرنة. وينبغي للحكومات أن تتعاون مع شركات التكنولوجيا لتطوير خدمات وبنية تحتية رقمية آمنة، بالتعاون بين أصحاب المصلحة المتعدّدين.
- تعزيز التعاون الإقليمي: ينبغي للدول العربية استخدام الآليات الإقليمية الراسخة لتسهيل تبادل المعلومات، وتنسيق الاستجابة للهجمات السيبرانية، ووضع برامج تدريبية مشتركة للمهنيين في مجال الأمن السيبراني.
- الاستخدام الأخلاقي للتكنولوجيا: ينبغي للحكومات أن تضمن الاستخدام المسؤول للتكنولوجيات الناشئة، وتجنّب التحيّزات والتمييز والممارسات غير الأخلاقية.

60- ويمكن للإسكوا، بفضل برنامجها للتعاون الفني، الاستمرار بمساعدة الدول الأعضاء في تحسين الأمن السيبراني لديها، والعمل مع الجهات المعنيّة على وضع الخطط الوطنية للأمن السيبراني، ورفع مستوى الوعي بين المسؤولين الوطنيين بشأن تأثير التكنولوجيات الناشئة على الأمن السيبراني في مختلف القطاعات، بما في ذلك قطاع النقل، وتيسير تبادل المعرفة بين الدول الأعضاء في المجالات ذات الصلة.
