منشورات ITU

الاتحاد الدولي للاتصالات
قطاع التنمية

تقرير نواتج المسألة 3/2 لقطاع تنمية الاتصالات

تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل تطوير ثقافة الأمن السيبراني

فترة الدراسة 2022-2025

تقرير نواتج المسألة 3/2 لقطاع تنمية الاتصالات

تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل تطوير ثقافة الأمن السيبراني

فترة الدراسة 2022-2025

تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل تطوير ثقافة الأمن السيبراني: تقرير نواتج المسألة 3/2 لقطاع تنمية الاتصالات لفترة الدراسة 2022-2025

ISBN 978-92-61-41106-0 (النسخة الإلكترونية)
ISBN 978-92-61-41116-9 (النسخة EPUB)

الاتحاد الدولي للاتصالات، Place des Nations، CH-1211 Geneva، Switzerland

شكر وتقدير

توفر لجنتا الدراسات بقطاع تنمية الاتصالات التابع للاتحاد الدولي للاتصالات (ITU-D) منصة محايدة تجمع خبراء من الحكومات والقطاع الصناعي ومنظمات الاتصالات والهيئات الأكاديمية من جميع أنحاء العالم بغية إنتاج أدوات وموارد عملية لمعالجة قضايا التنمية. وتحقيقاً لهذه الغاية، تضطلع لجنتا دراسات قطاع تنمية الاتصالات بمسؤولية إعداد التقارير والمبادئ التوجيهية والتوصيات على أساس المدخلات الواردة من الأعضاء. ويقرِّر المؤتمر العالمي لتنمية الاتصالات (WTDC) مسائل الدراسة كل أربع سنوات. واتفق أعضاء الاتحاد، الذين اجتمعوا في المؤتمر العالمي لتنمية الاتصالات لعام 2022 في كيغالي في يونيو 2022، على أن تتناول لجنة الدراسات 2 خلال الفترة 2022-2025 سبع مسائل في النطاق العام للتحول الرقمي.

أُعد هذا التقرير استجابة للمسألة 3/2: **تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل تطوير ثقافة الأمن السيبراني**، تحت التوجيه والتنسيق العامين لفريق الإدارة التابع للجنة الدراسات 2 لقطاع تنمية الاتصالات برئاسة السيد فاضل ديغم (جمهورية مصر العربية)، بدعم من نواب الرئيس التالية أسماؤهم: السيد عبد العزيز الزرعوني (الإمارات العربية المتحدة) والسيدة زينب أردو (جمهورية نيجيريا الاتحادية) والسيد جافوخير أريبوف (جمهورية أوزبكستان) والسيدة كارمن-مادالينا كلابون (رومانيا) والسيد مشفق غولوييف (جمهورية أذربيجان) والسيد هيديو إيماناكا (اليابان) والسيدة مينا سونمين جون (جمهورية كوريا) والسيد محمد لمين منتي (جمهورية غينيا) والسيد فيكتور أنطونيو مارتينيز سانشيز (جمهورية باراغواي) والسيدة ألينا مودان (رومانيا)[1] والسيد دييور رجبوف (جمهورية أوزبكستان)،[1] والسيد تونغنينغ وو (جمهورية الصين الشعبية) والسيد دومينيك فورغيس (فرنسا).

وقد أعد التقرير تحت قيادة المقرِّرات المشاركات المعنيات بالمسألة 3/2، السيدة فانيسا كوبيتي كرافو (جمهورية البرازيل الاتحادية)، والسيدة نيكول دارابيان (المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية)، والسيدة جابين فاهورا (الولايات المتحدة الأمريكية)،[1] ، بالتعاون مع نواب المقرِّرين التالية أسماؤهم: السيد دامنام ك. باغوليبي (جمهورية توغو) والسيد دانييل باتي (Access Partnership Limited)[1] والسيدة ماريا بولشاكوفا (الاتحاد الروسي)[1] والسيد توماسو دي زان (Access Partnership Limited) والسيد إدريسا ديالو (جمهورية غينيا) والسيد سيدي محمد فال (جمهورية السنغال) والسيد ألفارو غارسيا (مجموعة Axon Partners) والسيد دوغوكان عمر غور (الجمهورية التركية) والسيد براشيش كانا (جمهورية الهند) والسيد تنغ ما (المؤسسة الصينية الدولية لإنشاءات الاتصالات) والسيد رودجرز موميلو (جمهورية كينيا) والسيدة يوليانا ستولياروفا (الاتحاد الروسي) والسيد صامويل تيو (مجموعة شركاء أكسون)[1] والسيدة شينكسين وان (جمهورية الصين الشعبية) والسيدة كاسي ييروت (الولايات المتحدة الأمريكية) والسيد جاوسوك يون (جمهورية كوريا).

نتوجه بشكر خاص إلى المؤلفين الرئيسيين للفصول على تفانيهم ودعمهم وخبرتهم.

وأُعد هذا التقرير بدعم من جهات الاتصال المعنية بالمسألة 3/2 لقطاع تنمية الاتصالات والمحررين وفريق إنتاج المنشورات وأمانة لجنة الدراسات 2 لقطاع تنمية الاتصالات.

[1] استقال خلال فترة الدراسة هذه.

جدول المحتويات

قائمة الأشكال والإطارات

الأشكال

الإطارات

ملخص تنفيذي

يُمثل تقرير نواتج المسألة 3/2 لقطاع تنمية الاتصالات لفترة الدراسة 2022-2025 جهداً متضافراً للاستفادة من التجارب والممارسات الوطنية في مجال الأمن السيبراني من جميع أنحاء العالم. ويُعدّ التقرير مورداً يمكن أن يساعد البلدان في صياغة استراتيجياتها الرامية إلى بناء ثقافة متينة للأمن السيبراني. ويتناول التقرير ويبرز مساهمات أعضاء الاتحاد الدولي للاتصالات، بالإضافة إلى مناقشات ورش العمل التي عُقدت خلال فترة الدراسة، مما يعكس مجموعة متنوعة من وجهات النظر والخبرات التي تهدف إلى تأمين شبكات المعلومات والاتصالات

وفي عصر تتداخل فيه التكنولوجيات الرقمية بشكلٍ كبير في نسيج الحياة اليومية وتُشكّل عصب الاقتصادات حول العالَم، يُقرّ التقرير بالهشاشة المتزايدة التي يواجهها الأفراد والمنظمات والدول في ظلّ تزايد تعقيد التهديدات السيبرانية. ولم يعد الأمن السيبراني شأناً خاصاً، بل أصبح عنصراً أساسياً في التحوّل الرقمي والتطورات الرقمية، مما يتطلب مدخلات ذات أولوية قصوى من أصحاب المصلحة كافة، بما في ذلك الحكومات والقطاع الخاص والأفراد والهيئات الأكاديمية. وعلى الصعيد العالمي، يصنَّف انعدام الأمن السيبراني على أنه رابع أشد المخاطر على المدى القصير، وفقاً لتقرير المخاطر العالمية لعام 2024 الصادر عن المنتدى الاقتصادي العالمي.[2]

وبالإضافة إلى مبادرات وموارد الاتحاد الدولي للاتصالات وأعضائه المذكورة في هذا التقرير، من المهم إدراك أن هناك أيضاً عدداً من المبادرات العالمية التي تهدف إلى تبادل المعلومات والممارسات الجيدة في مجال الأمن السيبراني. وتهدف هذه المبادرات إلى دعم البلدان ومختلف أصحاب المصلحة في رحلة تحقيق الأمن السيبراني، إذ قد يصعب على البلدان النامية، وخاصةً أقل البلدان نمواً (LDC)، العثور على معلومات الأمن السيبراني والنفاذ إليها. وفي هذا السياق، من المهم الإشارة إلى موردَين شاملَين ورد ذكرهما خلال فترة الدراسة هذه، ويُمكن للدول الأعضاء في الاتحاد الاستفادة منهما: بوابة السياسات السيبرانية التابعة لمعهد الأمم المتحدة لبحوث نزع السلاح (UNIDIR) [3]، وبوابة المعرفة لبناء القدرات السيبرانية التابعة للمنتدى العالمي للخبرات السيبرانية (GFCE).[4]

وهناك مورد آخر ذو صلة أُشير إليه عدة مرات في هذا التقرير هو الرقم القياسي العالمي للأمن السيبراني (GCI)،[5] الذي يقيس مدى التزام البلدان بالأمن السيبراني عبر خمس ركائز أساسية هي: التدابير القانونية، والتدابير التقنية، والتدابير التنظيمية، وتنمية القدرات، والتعاون. وأطلق الاتحاد الرقم القياسي العالمي للأمن السيبراني في عام 2015، وتم تحسينه باستمرار ليكون بمثابة أداة للتقييم والتوعية وبناء القدرات، تساعد البلدان في مسيرتها نحو تطوير وتنفيذ قدراتها في مجال الأمن السيبراني.

ويُعدّ هذا التقرير مورداً يُقدّم أحدث الأفكار والممارسات، المُستنيرة بمشهد التهديدات الدينامي والمتطور باستمرار، مُقدّماً لمحةً عن الوضع الراهن للأمن السيبراني، ومحدداً لمسار استراتيجي لتطوراته في المستقبل.

ويُقدم هنا هيكل التقرير، بحيث يُركّز كل فصل على جانب مُحدّد من جوانب الأمن السيبراني:

- يتناول الفصل الأول الجانب البشري المحوري للأمن السيبراني، مشدداً على الحاجة الملحة لاستثمارات كبيرة من أجل توعية المستعملين، وتثقيف وتدريب الكوادر العاملة في مجال الأمن السيبراني. ويؤكد هذا الفصل على الحاجة الماسة إلى متخصصين مهرة في مجال الأمن السيبراني قادرين على إدارة تعقيدات التهديدات الرقمية المعاصرة، ويحث الفصل أيضاً البلدان على إعطاء الأولوية للبرامج التعليمية وخطط التوظيف لإنشاء كوادر تتسم بالكفاءة والمرونة في مجال الأمن السيبراني، بالإضافة إلى إعطاء الأولوية للتوعية كعنصر أساسي لتعزيز ثقافة الأمن السيبراني.
- يُركز الفصل الثاني على ممارسات ضمان الأمن السيبراني التي تعتبر أساسية لحماية الشبكات والأنظمة والبيانات من الأنشطة الضارة. ويُقيّم هذا الفصل مختلف المنهجيات والضوابط والمبادئ التوجيهية والمعايير المُعتمدة عالمياً، والتي يُمكن أن تُساعد في منع مخاطر الهجمات السيبرانية والتخفيف من حدتها.

[2] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
[3] https://cyberpolicyportal.org/ar
[4] https://cybilportal.org/
[5] https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

- يُسلّط الفصل الثالث الضوء على الدور الحاسم لأفرقة الاستجابة لحوادث الأمن السيبراني (CIRT) في حماية البنى التحتية الحيوية. ويعرض نماذج ناجحة للاستجابة للحوادث، ويُشدّد على أهمية إنشاء أفرقة الاستجابة لحوادث الأمن السيبراني وتطويرها، بالإضافة إلى التنسيق فيما بينها.
- يُقيّم الفصل الرابع وضع وتنفيذ استراتيجيات الأمن السيبراني الوطنية. ويبين هذا الفصل بالتفصيل أهمية مواءمة هذه الاستراتيجيات مع التحوّل الرقمي الشامل، والأمن الوطني، والبرامج الاقتصادية لتعزيز الصمود الرقمي.
- يستكشف الفصل الخامس الجهود المبذولة لتأمين شبكات الجيل الخامس. وفي خضمّ التحديات العالمية المتمثلة في نشر شبكات الجيل الخامس، يُسلّط هذا الفصل الضوء على السياسات والأطر التنظيمية والإجراءات الاستباقية التي تتخذها الصناعة للمساعدة في التخفيف من تهديدات الأمن السيبراني لشبكات الجيل الخامس.
- يبحث الفصل السادس في الاستخدام المتزايد لتكتيكات التصيد الاحتيالي المتطورة التي يستخدمها مرتكبو الجرائم السيبرانية لخداع المستعملين عبر خدمة الرسائل القصيرة (SMS)، مما يؤكد على ضرورة اتباع نهج جماعي يشمل اللوائح التنظيمية الحكومية ومبادرات الصناعة والتوعية العامة المتزايدة لحماية المستهلكين والحفاظ على اعتمادية شبكات الاتصالات.

ويُكمِّل هذا التقرير ملحقان يوفران موارد إضافية، بما في ذلك مساهمات مُفصَّلة من أعضاء الاتحاد عُرِضَت في دورة الدراسة هذه، ومُلخَّص لمشاريع وبرامج الأمن السيبراني الجارية في قطاع تنمية الاتصالات. ويقدِّم هذان الملحقان رؤىً قيّمة ويشكلان موادَّ أساسيةً لأصحاب المصلحة الذين يسعون إلى تعميق فهمهم للأمن السيبراني ودوره الحاسم في العصر الرقمي.

وفي جوهره، يُمثِّل التقرير النهائي للمسألة 3/2 لدى قطاع تنمية الاتصالات لفترة الدراسة 2022-2025 مُخطَّطاً استراتيجياً لبناء مستوى عالٍ من الأمن السيبراني بين أعضاء الاتحاد. وهو دعوةٌ للعمل من أجل نهج مُوحَّد لتأمين مُستقبلنا الرقمي، مُؤكِّداً على أهمية التوعية والتثقيف وتطوير الاستراتيجيات وقدرات أفرقة الاستجابة لحوادث الأمن السيبراني والسياسات والاستراتيجيات والتعاون الدولي للتعاطي مع تعقيدات تحديات الأمن السيبراني والتخفيف من حدتها سعياً نحو تحقيق التحوّل الرقمي.

الاختصارات والأسماء المختصرة

الاختصار	المصطلح
2G	تكنولوجيا الاتصالات المتنقلة من الجيل الثاني (*second generation mobile technology*)
3G	تكنولوجيا الاتصالات المتنقلة من الجيل الثالث (*third generation mobile technology*)
3GPP	مشروع شراكة الجيل الثالث (*Third Generation Partnership Project*)
4G	تكنولوجيا الاتصالات المتنقلة من الجيل الرابع (*fourth generation mobile technology*)
5G	تكنولوجيا الاتصالات المتنقلة من الجيل الخامس[6] (*fifth generation mobile technology*)
CI	البنية التحتية الحرجة (*critical infrastructure*)
CIRT	أفرقة الاستجابة لحوادث الأمن السيبراني (*cybersecurity incident response team*)
CISA	وكالة الأمن السيبراني وأمن البنى التحتية (*Cybersecurity and Infrastructure Security Agency*)
COP	حماية الأطفال على الإنترنت (*child online protection*)
ENISA	وكالة الاتحاد الأوروبي للأمن السيبراني (*European Union Agency for Cybersecurity*)
ETSI	المعهد الأوروبي لمعايير الاتصالات (*European Telecommunications Standards Institute*)
EU	الاتحاد الأوروبي (*European Union*)
FIRST	المنتدى العالمي لأفرقة الاستجابة لحوادث وأمن المعلومات (*Forum of Incident Response and Security Teams*)
GCI	الرقم القياسي العالمي للأمن السيبراني (*global cybersecurity index*)
GFCE	المنتدى العالمي للخبرات السيبرانية (*Global Forum on Cyber Expertise*)
GSMA	رابطة النظام العالمي للاتصالات المتنقلة (*GSM Association*)
ICT	تكنولوجيا المعلومات والاتصالات (*information and communication technologies*)
IoT	إنترنت الأشياء (*Internet of Things*)
ITU	الاتحاد الدولي للاتصالات (*International Telecommunication Union*)
ITU-D	قطاع تنمية الاتصالات بالاتحاد الدولي للاتصالات (*ITU Telecommunication Development Sector*)
ITU-R	قطاع الاتصالات الراديوية بالاتحاد الدولي للاتصالات (*ITU Radiocommunication Sector*)
ITU-T	قطاع تقييس الاتصالات بالاتحاد الدولي للاتصالات (*ITU Telecommunication Standardization Sector*)
LDC	أقل البلدان نمواً (*least developed countries*)
NESAS	خطة ضمان أمن معدات الشبكة (*Network Equipment Security Assurance Scheme*)

[6] وفي حين حُرِص في هذه الوثيقة على استخدام التعريف الرسمي لأجيال الاتصالات المتنقلة الدولية والإشارة إليها على النحو الصحيح (انظر القرار ITU-R 56، "*التسمية الخاصة بالاتصالات المتنقلة الدولية*")، فإن أجزاء من هذه الوثيقة تتضمن مواد قدمها الأعضاء تشير إلى أسماء الأسواق المستعملة بكثرة لأجيال الاتصالات المتنقلة "xG". ولا يمكن بالضرورة إقامة تقابل لهذه المواد مع جيل معين من الاتصالات المتنقلة الدولية، لأن المعايير الأساسية لدى الأعضاء غير معروفة، ولكن بشكل عام، تعرَّف الاتصالات المتنقلة الدولية-2000 والاتصالات المتنقلة الدولية-المتقدمة والاتصالات المتنقلة الدولية-2020 والاتصالات المتنقلة الدولية-2030 بالجيل الثالث (3G)/الجيل الرابع (4G)/الجيل الخامس (5G)/الجيل السادس (6G) على التوالي.

(تابع)

الاختصار	المصطلح
NIST	المعهد الوطني للمعايير والتكنولوجيا (*National Institute for Standards and Technology*)
OECD	منظمة التعاون والتنمية في الميدان الاقتصادي (*Organisation for Economic Co-operation and Development*)
RAN	شبكة نفاذ لاسلكي (*radio access network*)
SDN	الشبكات المُعرّفة بالبرمجيات (*software-defined network*)
SDO	منظمة معنية بوضع المعايير (*standards development organization*)
SG17	لجنة الدراسة 17 بقطاع تقييس الاتصالات (*Study Group 17 of ITU-T*)
SMS	خدمة الرسائل القصيرة (*short message service*)
UNIDIR	معهد الأمم المتحدة لبحوث نزع السلاح (*United Nations Institute for Disarmament Research*)

الفصل الأول - التشجيع على إذكاء وعي المستعملين وعلى بناء القدرات في مجال الأمن السيبراني

يُعدّ تطبيق مهارات وبرامج توعية فعّالة في مجال الأمن السيبراني أمراً بالغ الأهمية لضمان استمرار جني ثمار الرقمنة بأمان. فمبادرات الأمن السيبراني لا تُسهم فقط في الحد من المخاطر المرتبطة بالتصيّد الاحتيالي وغيره من التهديدات السيبرانية، بل تُسهم أيضاً في بناء قوى عاملة ماهرة قادرة على مواجهة التحديات المعقدة للعصر الرقمي. ويستكشف هذا الفصل العناصر الرئيسية والأمثلة البارزة، مُقترحاً سبيلاً للمضي قدماً للبلدان الراغبة في اتباع المسار نفسه.

1.1 إذكاء الوعي بالأمن السيبراني

لا يزال الخطأ البشري عاملاً رئيسياً في خروقات الأمن السيبراني، إذ تشير الدراسات إلى أن أكثر من 88 في المائة من هذه الحوادث تنطوي على شكل من أشكال الأخطاء البشرية.[7] وهذا يؤكد الحاجة إلى برامج توعية شاملة تتجاوز الحلول التقنية وتتناول العنصر البشري في الأمن السيبراني.

تشير التوعية بالأمن السيبراني إلى النهج الاستراتيجي لتثقيف الأفراد والمنظمات والمجتمعات بشأن المخاطر السيبرانية والممارسات الجيدة لحماية الأصول والمعلومات الرقمية. ويتمثل الهدف الرئيسي من مبادرات زيادة التوعية بالأمن السيبراني في ترسيخ ثقافة أمنية واعية، وتمكين الأشخاص من التعرف على مخاطر الأمن السيبراني والوقاية منها والاستجابة لها بفعالية. وقد تشمل برامج التوعية أساليب وأدوات متنوعة (مثل برامج التدريب، وتمارين محاكاة التصيد الاحتيالي، والألعاب الإلكترونية، ووحدات التعلم الصغرية). وتتراوح الموضوعات الرئيسية التي غالباً ما تغطيها هذه المبادرات بين الهندسة الاجتماعية والتوعية بالتصيد الاحتيالي، وإدارة كلمات المرور، وحماية البيانات، والاستخدام الآمن للأجهزة المتنقلة ووسائل التواصل الاجتماعي.

وقد يكون لبرامج التوعية بالأمن السيبراني المُطبقة جيداً تأثيرٌ بالغ.[8] فالمنظمات التي تُولي أولوية للتدريب على التوعية غالباً ما تشهد انخفاضاً ملحوظاً في هجمات التصيد الاحتيالي الناجحة، وتحسيناتٍ عامة في وضعها الأمني، حيث تُظهر الدراسات انخفاضاً في الهجمات الناجحة يصل إلى نسبة 70 في المائة.[9] كما يُحقق الاستثمار في التوعية بالأمن السيبراني عائداً استثمارياً (ROI) مرتفعاً، حيث تُشير الدراسات إلى أنه حتى أكثر البرامج التدريبية بساطةً يمكن أن تُحقق عائداً استثمارياً يصل إلى سبعة أضعاف.[10] وعلاوةً على ذلك، تُساهم هذه البرامج في بناء ثقافة أمن سيبراني تتجاوز نطاق مكان العمل، مما يُساعد الأفراد أيضاً على أن يصبحوا "مواطنين سيبرانيين" مسؤولين في حياتهم الشخصية. وعلاوةً على ذلك، تُعدّ التوعية بالأمن السيبراني أمراً أساسياً للامتثال للوائح التنظيمية للصناعة وقوانين حماية البيانات، مثل توجيه أمن الشبكات وأنظمة المعلومات (NIS2) المنقح في الاتحاد الأوروبي. وتُلزم العديد من القطاعات المنظمات بتنفيذ برامج تدريب أمني للامتثال للمعايير التنظيمية وتجنب الغرامات أو العواقب القانونية المحتملة.[11]

وتشير بيانات الرقم القياسي العالمي للأمن السيبراني (GCI) إلى أن 152 بلداً نظمت حملات توعية بالأمن السيبراني استهدفت عامة السكان بين عامي 2021 و2024 [12] وقد نفذت الدول الأعضاء في الاتحاد العديد من

[7] https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error
[8] https://www.sciencedirect.com/science/article/pii/S0167404823004959
[9] https://keepnetlabs.com/blog/2024-security-awareness-training-statistics؛
https://www.knowbe4.com/press/knowbe4-analysis-finds-security-awareness-training-and-simulated-phishing-effective-in-reducing-cybersecurity-risk
[10] https://blog.usecure.io/does-security-awareness-training-work؛
https://ostermanresearch.com/wp-content/uploads/2021/01/ORWP_0313-The-ROI-of-Security-Awareness-Training-August-2019.pdf
[11] https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/
[12] https://www.itu.int/epublications/ar/publication/global-cybersecurity-index-2024

المبادرات لزيادة الوعي بتهديدات الأمن السيبراني. وتشمل هذه المبادرات برامج شاملة تستهدف مختلف شرائح السكان. وتركز بعض المشاريع تحديداً على منع الجرائم السيبرانية والاحتيال، بينما تستخدم مشاريع أخرى مجموعة متنوعة من الوسائط الإلكترونية للنهوض بممارسات النظافة السيبرانية بين السكان.

ومن الأمثلة على البرامج الشاملة المصممة خصيصاً لمختلف شرائح السكان **الاتحاد الروسي**، "برنامج النظافة السيبرانية" الذي أُطلق في أغسطس 2022، وهو مبادرة شاملة مدتها ثلاث سنوات، بهدف تعزيز الوعي بالأمن السيبراني بين مواطني الاتحاد الروسي. ولتمكين اتصالات أكثر استهدافاً وفعالية، قسّم البرنامج السكان إلى ثلاث فئات عمرية: الأطفال والمراهقون (12-18 عاماً)، والبالغون (18-45 عاماً)، والبالغون (45 عاماً فأكثر). فبالنسبة للفئة العمرية 12-18 عاماً، والتي تحظى باهتمام خاص نظراً لهشاشتها أمام التهديدات السيبرانية، تم تنفيذ مشروعين رئيسيين.

- حيث يُقدّم مشروع "التنمر السيبراني" نصائح للضحايا والمعتدين والمراقبين، مُشدّداً على أهمية التعامل مع التنمر السيبراني بروح الدعابة واللامبالاة الصحية.
- ويُركّز مشروع "طوّر مهاراتك الوقائية" على تثقيف الأطفال بشأن عمليات الاحتيال في بيئات الألعاب الإلكترونية.

وبالنسبة للبالغين الذين تتراوح أعمارهم بين 18 و45 عاماً، يشمل البرنامج مشاريع مثل

- "نمط حياة صحي سيبرانياً"،
- و"كلمات مرور بسيطة مركبة"،
- و"اعرف دورك".

وتغطي هذه المبادرات موضوعات منها حماية الأجهزة المتنقلة، ومنع التصيد الاحتيالي، وأمن كلمات المرور، والتوعية بالاحتيال الهاتفي. كما يُلبي البرنامج احتياجات البالغين الذين تزيد أعمارهم عن 45 عاماً، مع التركيز على حمايتهم من الاحتيال الهاتفي. بالإضافة إلى ذلك، تهدف دورة متخصصة إلى تعزيز ثقافة أمن المعلومات لدى موظفي الخدمة المدنية. وقد كشفت دراسة أُجريت على مستوى الاتحاد الروسي في عام 2022 عن مؤشر عام لثقافة الأمن السيبراني بلغ 48,2 من 100، يغطي موضوعات مثل الحماية من الفيروسات، والاستخدام الآمن للإنترنت، وأمن البيانات الشخصية. وقد صُمم برنامج النظافة السيبرانية بحيث يتم تحديثه سنوياً، لضمان مواكبته للتهديدات الرقمية الناشئة واحتياجات السكان المتطورة.[13]

وفي **جمهورية كوت ديفوار**، كان برنامج التوعية بالأمن السيبراني مع التركيز بشكل خاص على الجريمة السيبرانية من بين عدد من مبادرات التوعية والتدريب في مجال الأمن السيبراني التي نفذت من خلال مؤسسات الأمن السيبراني الرئيسية في كوت ديفوار. وتُنظِّم منصة مكافحة الجريمة السيبرانية (PLCC) حملات توعية في المؤسسات التعليمية، بما في ذلك المدارس والجامعات، بالإضافة إلى المؤسسات المالية والدينية، وتنشر محتوىً تثقيفياً ومعلوماتٍ عن اعتقالات مرتكبي الجرائم السيبرانية على وسائل التواصل الاجتماعي. ويُقدِّم فريق CI-CERT (*كوت ديفوار- فريق الاستجابة للطوارئ الحاسوبية*)، وهو جهة الاتصال الوطنية للأمن السيبراني، برنامجاً تدريبياً متخصصاً يُسمى "DIGISEC" مُصمَّماً للشركات والمؤسسات لتعزيز الوعي بالأمن الرقمي في مكان العمل. وهناك مبادرة أخرى حديثة بارزة أُطلقت خلال كأس الأمم الأفريقية 2024، وهي مبادرة CyberCAN23. وقد ركّز نظام الأمن السيبراني هذا، الذي يُديره مركز CI-CERT، على رفع مستوى الوعي بشأن عمليات الاحتيال على المنصات الرقمية، وخاصة التصيُّد الاحتيالي. وقد استُخدمت الحملة منصات التواصل الاجتماعي والتلفزيون والإذاعة لنشر معلومات الأمن السيبراني. كما ينظم البلد حملة توعية وطنية بعنوان "*En ligne tous responsables*" (الجميع مسؤول على الإنترنت) في مختلف البلدات والمدن.[14]

وقد نفذت **جمهورية رواندا** العديد من المبادرات لتعزيز الوعي والتعليم والتدريب في مجال الأمن السيبراني، بما في ذلك البرنامج الوطني للتوعية والتدريب في مجال الأمن السيبراني، الذي يعزز الوعي بالأمن السيبراني لمستعملي الإنترنت ويعمل أيضاً على تطوير الكفاءات المتخصصة في مجال الأمن السيبراني لدعم المؤسسات العامة والخاصة في حماية الأنظمة الحيوية من التهديدات السيبرانية.[15]

---

[13] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/71 المقدمة من الاتحاد الروسي

[14] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/160 المقدمة من الشبكة الدولية للنساء الخبيرات في المجال الرقمي (RIFEN)

[15] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/35 المقدمة من رواندا

وفي إطار التركيز على منع الاحتيال السيبراني، عملت **الصين** على بناء "شبكة مكافحة الاحتيال" متعددة الأبعاد على مستوى المجتمع، وشجعت على تثبيت تطبيق المركز الوطني لمكافحة الاحتيال، وزيادة الوعي باعتماد تدابير النظافة السيبرانية لدى مجموعة من الفئات المستهدفة، مثل الطلاب، وكبار السن، والمزارعين، وغيرهم.[16]

وأخيراً، تعتمد مبادرة في **البرازيل** تُركّز على تعزيز ممارسات النظافة السيبرانية للسكان، على أدوات التواصل عبر الإنترنت مثل يوتيوب. وقد نفّذت البرازيل مبادرات النظافة السيبرانية من خلال وكالة الاتصالات الوطنية "أناتل". وفي إطار تخطيطها الاستراتيجي للفترة 2023-2027، أنشأت "أناتل" بوابة إلكترونية مُخصّصة لمنع الاحتيال الرقمي والنظافة السيبرانية، تُقدّم معلومات عن التهديدات الرقمية الشائعة واستراتيجيات الوقاية منها. وتُنظّم الوكالة بانتظام فعاليات توعوية مع شركائها، وتُحافظ على قائمة تشغيل مُتخصّصة للأمن السيبراني على قناتها على يوتيوب. ومن المبادرات البارزة الأخرى حملات #OctoberCyberSafe في أكتوبر 2023 وأكتوبر 2024، وفعاليات يوم الإنترنت الأكثر أمناً في فبراير 2024 وفبراير 2025.[17]

2.1 بناء القدرات الخاصة بالتعليم والتدريب في مجال الأمن السيبراني

سلّط تقرير "توقعات الأمن السيبراني العالمي لعام 2025" الذي أعده المنتدى الاقتصادي العالمي، الضوء على وجود نقص متزايد في مهارات الأمن السيبراني، حيث ازدادت فجوة مهارات الأمن السيبراني بنسبة 8 في المائة منذ التقرير السابق (التوقعات العالمية للأمن السيبراني لعام 2024). وأبلغت منظمتان من كل ثلاث منظمات عن فجوات حرجة في مهارات الأمن السيبراني، مما يعيقهما عن تلبية متطلباتهما الأمنية. ويؤكد التقرير على الحاجة الملحة إلى مبادرات لمعالجة هذه الفجوة في المهارات، بما في ذلك التدريب وإعادة التأهيل وبذل الجهود لتوظيف المواهب في مجال الأمن السيبراني والاحتفاظ بها.[18]

ويمكن اعتبار التعليم والتدريب في مجال الأمن السيبراني عملية شاملة مصممة لتزويد الأفراد بالمعارف والمهارات والقدرات اللازمة لحماية الأصول الرقمية، وتحديد التهديدات السيبرانية والتخفيف منها، وضمان أمن أنظمة المعلومات. ويشمل التعليم والتدريب في مجال الأمن السيبراني مجموعة واسعة من الموضوعات والنهج التي تهدف إلى تطوير قوة عاملة قادرة على مواجهة التحديات المتطورة في مجال الأمن السيبراني. ويمكن أن يتخذ التعليم والتدريب في مجال الأمن السيبراني أشكالاً مختلفة، بما في ذلك البرامج الأكاديمية الرسمية، والشهادات المهنية، وورش العمل العملية، ومبادرات التعلم المستمر.

وتُعد برامج التعليم والتدريب في مجال الأمن السيبراني بالغة الأهمية في المشهد الرقمي المعاصر، إذ تُساعد على منع انتهاكات البيانات والتخفيف من المخاطر السيبرانية من خلال تزويد الأفراد والمهنيين بالمعارف والمهارات اللازمة لتحديد التهديدات السيبرانية المحتملة والتعاطي معها.[19] وترى وكالة الأمن السيبراني وأمن البنى التحتية (CISA) في الولايات المتحدة أن التعليم والتدريب في مجال الأمن السيبراني " ضروريان لحماية البنى التحتية الحرجة لأمتنا"[20]، مما يُؤكد على الدور الحاسم لمتخصصي الأمن السيبراني جيدي التدريب في حماية الأمن القومي والمصالح الاقتصادية.

ويتفاوت نطاق ومستوى سياسات التعليم والتدريب في مجال الأمن السيبراني تفاوتاً كبيراً في مختلف الدول الأعضاء في الاتحاد، حيث تُطبّق بعض الدول أدوات سياساتية شاملة لزيادة عدد المتخصصين في مجال الأمن السيبراني على جميع المستويات، بينما تُركّز دول أعضاء أخرى على برامج تدريب مُحدَّدة في مجال الأمن السيبراني. وقد ركّزت بعض الدول الأعضاء على طلاب الدراسات العليا من خلال إنشاء برامج للتعليم العالي في الجامعات، بينما تُشدّد دول أعضاء أخرى على ضرورة تدريب الموظفين المنتمين بالفعل لقوة العمل. وبالإضافة إلى ذلك، ظهر عدد من البرامج الدولية التي تُديرها منظمات دولية. ولوحظت أيضاً تفاوتات على المستوى الإقليمي، حيث تُقدم دورات الأمن السيبراني على المستوى الجامعي في 91 في المائة من البلدان الأوروبية، مقارنة بنسبة 60 في المائة من البلدان في منطقة الأمريكتين، و61 في المائة من البلدان في منطقة إفريقيا.[21]

---

16 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/370 المقدمة من الصين

17 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/165 المقدمة من البرازيل؛ https://www.youtube.com/playlist?list=PLOmVJ5Ex3R10wEUM3edKTSErojXs_07xg (قائمة تشغيل الأمن السيبراني)

18 https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

19 https://www.forbes.com/councils/forbestechcouncil/2025/01/21/protecting-our-future-why-cybersecurity-training-is-essential-for-students/

20 https://niccs.cisa.gov/education-training

21 https://www.itu.int/epublications/ar/publication/global-cybersecurity-index-2024

تقدم **المملكة المتحدة** مثالاً على نهج متقدم في تعليم ومهارات الأمن السيبراني، حيث طبّقت مجموعة متنوعة من السياسات والبرامج على جميع المستويات للتخفيف من فجوة مهارات الأمن السيبراني. وتُركّز استراتيجيتها على ثلاثة مجالات رئيسية: مهارات الأمن السيبراني للبالغين، والمهارات السيبرانية للشباب، وتطوير مهن الأمن السيبراني. فبالنسبة للبالغين، تُوفر المملكة المتحدة دورات تدريبية مكثفة لمدة 12-16 أسبوعاً، بما في ذلك مبادرة "تحسين المهارات في الميدان السيبراني"، لإعادة تدريب الأفراد وتطوير مهاراتهم في مجال الأمن السيبراني. كما تُشجّع المملكة المتحدة برامج التلمذة المهنية، مثل برنامج التدريب المهني للحصول على درجة CyberFirst، لتوفير خبرة عملية أثناء العمل. أما بالنسبة للشباب، فقد أنشأت المملكة المتحدة نظاماً إيكولوجياً من العروض تحت شعار "CyberFirst". ويتضمن ذلك مسابقة وطنية للفتيات المهتمات بالحصول على وظائف في مجال الأمن السيبراني، ودورات تمهيدية خلال العطلات المدرسية، ونظام تكريم للمدارس التي لديها برامج تعليم ممتازة في مجال الأمن السيبراني. ومنصة التعلم الرائدة للشباب في المملكة المتحدة، Cyber Explorers، مجانية لجميع الأشخاص الذين تتراوح أعمارهم بين 11 و14 عاماً، وقد حققت تكافؤاً شبه كامل بين الجنسين في المشاركة. كما تعمل المملكة المتحدة على تطوير مهنة الأمن السيبراني من خلال مجلس الأمن السيبراني للمملكة المتحدة (UKCSC). وتهدف هذه الهيئة المهنية إلى إنشاء مسارات ومعايير واضحة لمجال الأمن السيبراني، مما يجعله أكثر سهولة في النفاذ إليه وأكثر هيكلة بالنسبة للأفراد في جميع مراحل حياتهم المهنية.[22]

وتقدم **البرازيل** مثالاً على سياسة للأمن السيبراني مُحكمة التصميم ذات تركيز معين ونتائج مُحددة بوضوح. فقد أطلقت البلاد برنامج "Hackers do Bem" (قراصنة القبعة البيضاء) لمعالجة نقص محدد في مُختصي الأمن السيبراني، والذين يُقدّر عددهم بنحو 000 230 وظيفة، وذلك من خلال تدريب 000 30 فرد كمتخصصين في الأمن السيبراني لملء هذه المناصب. ويُنفّذ البرنامج كلٌّ من الشبكة الوطنية للتعليم والبحوث (RNP)، وهيئة SENAI-SP، وشركة Softex، بدعمٍ من وزارة العلوم والتكنولوجيا والابتكار. ويتّبع البرنامج نهجاً مهيكلاً من خمسة مستويات لتعليم الأمن السيبراني. ويبدأ البرنامج بمرحلة تأهيل تُغطّي مفاهيم تكنولوجيا المعلومات الأساسية، ثم يتدرّج عبر مفاهيم الأمن السيبراني الأساسية والجوهرية، ويُتوّج بتدريبٍ مُتخصص. ويُركّز المستوى المُتخصص على خمسة مُستويات مهنية رئيسية: "الفريق الأحمر" (تقييم الأمن)، و"الفريق الأزرق" (معمارية الأمن)، و"DevSecOps" (أمن التطبيقات)، و(فريق الاستجابة لحوادث الأمن الحاسوبي) "CSIRT"، و(فريق الحوكمة والمخاطر والامتثال) "GRC". ويتضمن المستوى الأخير برنامجاً تدريبياً على الأمن السيبراني لمدة ستة أشهر، مع توجيهٍ من مهنيين في جميع أنحاء الولايات البرازيلية. ولضمان الاستدامة، أنشأ البرنامج مركزاً وطنياً للأمن السيبراني يربط مختلف أصحاب المصلحة، بما في ذلك المؤسسات التعليمية والهيئات الحكومية والشركات والطلاب. ويهدف مركز الأمن السيبراني هذا إلى مواءمة احتياجات الصناعة مع مخرجات التعليم، وتوسيع فرص التدريب على الأمن السيبراني في جميع أنحاء البرازيل.[23]

وتعمل بعض البلدان على تعزيز تعليم الأمن السيبراني في مستوى التعليم الثالث في محاولة لتحسين مهارات سكانها. فعلى سبيل المثال، قامت حكومة **رواندا** بإدخال وحدات دراسية في مجال أمن المعلومات ضمن برامج تكنولوجيا المعلومات (IT) وهندسة الحاسوب في المؤسسات التعليمية العليا. وتقدم جامعة كارنيجي ميلون - إفريقيا (CMU-Africa) في كيغالي برامج تغطي الأمن السيبراني، وهندسة البرمجيات، وموضوعات أخرى تتعلق بتكنولوجيا المعلومات والاتصالات (ICT). وتركز برامج CMU-Africa هذه على التدريس والبحث في مجال الأمن السيبراني والخصوصية، بدءاً من تأمين أنظمة البرمجيات والشبكات وصولاً إلى جعل الأمن والخصوصية أكثر قابلية للاستخدام.[24]

وبدلاً من استهداف المؤسسات التعليمية، ركزت بلدان أخرى على الجهات المهنية المنتمية إلى القوى العاملة بالفعل، لا سيما في القطاعات الأكثر عرضة للتهديدات السيبرانية. وقد صُممت برامج تدريبية لموظفي القطاع العام على وجه التحديد في **جمهورية الأرجنتين** تغطي موضوعات أساسية بشأن أمن البيانات والممارسات الجيدة في مجال إدارة المعلومات. وتهدف هذه الدورات إلى تزويد المشاركين بالمعارف والمهارات الأساسية لحماية الخصوصية والسرية والسلامة والتيسر فيما يتعلق بالمعلومات. ويُقدم أيضاً تدريب متخصص لموظفي الخدمة المدنية المعينين كجهات اتصال للأمن السيبراني. وتغطي الدورات التدريبية المتخصصة موضوعات مثل تحديات الأمن السيبراني الجديدة، والأدلة الرقمية، واختبار الاختراق، وتعزيز متانة أنظمة الحاسوب.[25]

[22] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/77 المقدمة من المملكة المتحدة
[23] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/184 المقدمة من البرازيل
[24] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/35 المقدمة من رواندا
[25] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/150 المقدمة من الأرجنتين

وبالمثل، نظمت **الجمهورية العربية السورية** أنشطة تدريبية تستهدف موظفي القطاع الحكومي والجامعات والعاملين في القطاع المصرفي. ويوفر مركز تميز في الهيئة الوطنية لخدمات شبكات الاتصالات دورات تدريبية في مجال أمن المعلومات، على الرغم من توقف أنشطته أثناء الحرب قبل إعادة تشغيله في عام 2021.[26]

وأنشأت **مصر** في عام 2021 مركز التدريب المصري الإفريقي في مجال تنظيم الاتصالات (EG-ATRC)، والذي يجسد قوة التعاون الإقليمي من خلال توفير التدريب الأكاديمي والمهني لرفع مستوى الكفاءات البشرية في جميع أنحاء البلدان الإفريقية في مجال تأمين المعلومات والشبكات.[27]

ومن الأمثلة الأخرى مركز الكفاءة السيبرانية لأميركا اللاتينية والكاريبي (LAC4)، وهي مبادرة يقودها **الاتحاد الأوروبي**، ومؤسسة CyberNet، وحكومة الجمهورية الدومينيكية. ويعمل المركز LAC4 على تعزيز القدرات السيبرانية الإقليمية من خلال تبادل المعارف على نطاق واسع والتدريب وتطوير الممارسات الجيدة في مجال الأمن السيبراني والتحول الرقمي. ويعمل مركز LAC4 الواقع في سانتو دومنغو، الجمهورية الدومينيكية كمحور مركزي لتبادل الخبرات الجماعية، حيث يساعد أكثر من 25 بلداً في منطقة أمريكا اللاتينية والكاريبي على تعزيز أطر الأمن السيبراني وتشجيع التعاون الإقليمي. وتشمل أنشطة التدريب والتدريبات السيبرانية واسعة النطاق التي يقدمها المركز LAC4 زيادة الوعي، وإدارة المخاطر السيبرانية، وحماية البنى التحتية الحرجة، وصياغة سياسات وقوانين الأمن السيبراني. كما ويوفر العديد من دورات التدريب التقني التي تهدف إلى تعزيز مهارات ومعارف المتخصصين في مجال الأمن السيبراني في جميع أنحاء المنطقة. ومن الجدير بالذكر أن المركز LAC4 يركز بشكل كبير على التنوع بين الجنسين في مجال الأمن السيبراني، وينظم ورش عمل تدريبية متخصصة تهدف إلى تمكين المرأة في هذا المجال. وتعتبر هذه الجهود حاسمة في بناء قوة عاملة متنوعة ومرنة في مجال الأمن السيبراني، قادرة على مواجهة التحديات المتطورة في المشهد الرقمي.[28]

وتشكل التدريبات السيبرانية التي تحاكي الهجمات السيبرانية وحوادث أمن المعلومات وأنواع الاضطرابات الأخرى عنصراً مهماً في مبادرات بناء القدرات في مجال الأمن السيبراني، وقد كانت محور تركيز جهود مكتب تنمية الاتصالات (BDT) في **الاتحاد** كوسيلة لتعزيز جاهزية البلدان للأمن السيبراني، وحماية القدرات، ورفع كفاءة الاستجابة للحوادث. وينظم الاتحاد تدريبات سيبرانية إقليمية وعالمية، بالإضافة إلى تمارين وطنية، ويُعد مواد داعمة لهذه الأنشطة.[29]

ومع تزايد أهمية الأمن السيبراني في البرنامج السياسي عالمياً، دخلت المنظمات الدولية أيضاً هذا المجال ببرامج تهدف إلى تعزيز مهارات الأمن السيبراني للأجيال القادمة. وتشمل الجهود الدولية البارزة البرامج التي ينفذها الاتحاد، وبرنامج "مساراتها السيبرانية (Her CyberTracks)" لمكتب تنمية الاتصالات، وهذا البرنامج عبارة عن مشروع مكون من ثلاثة أجزاء يشتمل على تدريبات تقنية عبر الإنترنت وفي الموقع على سياسات الأمن السيبراني والدبلوماسية، وتدريبات على المهارات الشخصية، ودوائر إرشادية شهرية، وعروض تقديمية رئيسية ملهمة، بالإضافة إلى فعاليات التواصل الإقليمية، وكلها متاحة كمنهج تكميلي شامل في إطار مشروع "مسار السياسات والدبلوماسية". ويهدف المشروع إلى تعزيز تمثيل المرأة ومشاركتها، مع السعي إلى تحسين مساهمة المرأة في العمليات سياسات الأمن السيبراني الوطنية والدولية.[30]

3.1 حماية الأطفال على الإنترنت

بحسب المعهد العالمي لسلامة الطفل (Childlight)، فإن واحداً من كل ثمانية أطفال في العالم، أي حوالي 302 مليون شاب، كانوا ضحايا لالتقاط صور ومقاطع فيديو جنسية ومشاركتها وعرضها دون موافقة في عام 2024.[31]

وتشير حماية الأطفال وسلامتهم على الإنترنت إلى التدابير والممارسات والاستراتيجيات المطبقة لحماية الأطفال والشباب من المخاطر والتهديدات المحتملة في البيئة الرقمية. وتشمل حماية الأطفال على الإنترنت مجموعة واسعة من الجهود الرامية إلى تهيئة تجربة أكثر أماناً على الإنترنت للقاصرين، بما في ذلك الحماية من أشكال

[26] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/163 المقدمة من الجمهورية العربية السورية
[27] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/329 المقدمة من مصر
[28] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/117 المقدمة من الجمهورية الدومينيكية
[29] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx
[30] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Skills-Development/Her-CyberTracks.aspx
[31] https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-globa

مختلفة من الإساءة عبر الإنترنت، مثل الاستغلال والإغواء الجنسيين،[32] والتعرض لمحتوى ضار وغير مناسب للعمر، والتنمر الإلكتروني، والمواد الإباحية، واستخدام المنصات الإلكترونية في الأنشطة غير القانونية.[33]

تُعد حماية الأطفال وسلامتهم على الإنترنت أمراً بالغ الأهمية في عصرنا الرقمي الحالي، حيث يتزايد تعرض الأطفال للإنترنت ومخاطرها المحتملة، مما يجعل التثقيف حول السلامة على الإنترنت أمراً أساسياً لتمكين الأطفال من التعامل مع العالم الرقمي بمسؤولية. ومن خلال تعليم الأطفال مخاطر الإنترنت، والتفكير النقدي، والسلوك المسؤول على الإنترنت، يمكنهم على تطوير المهارات اللازمة لحماية أنفسهم واتخاذ قرارات مستنيرة على الإنترنت.[34]

وتُظهر المساهمات المقدمة من الدول الأعضاء أنها أولت حماية الأطفال على الإنترنت اهتماماً بالغاً في السنوات الأخيرة، مستخدمةً أدواتٍ متنوعة لضمان سلامتهم على الإنترنت. وتكشف بيانات الرقم القياسي العالمي للأمن السيبراني أن 69 في المائة من الحكومات على الصعيد العالمي نفذت حملات تستهدف الآباء والمعلمين والأطفال تحديداً وذلك في إطار جهود حماية الأطفال على الإنترنت[35]. ويقوم عدد من البلدان بوضع أطر قانونية وسياساتية شاملة، بالإضافة إلى برامج وأدوات عملية، لحماية البيئة الإلكترونية للأطفال. وجُمّعت أدلةً تجريبية حول سلوك الأطفال على الإنترنت لفهم البعضِ من أكثر قضايا السلامة الإلكترونية تحدياً ومعالجتها. وقد أدركت البلدان أهمية الحلول متعددة أصحاب المصلحة التي تجمع أصحاب المصلحة المناسبين لمعالجة هذه المشكلة متعددة الجوانب. وأخيراً، نفذت البلدان برامج تجمع بين التوعية بالأمن السيبراني والسلامة على الإنترنت، مما يُظهر أهمية اتباع نهج شامل.

وتقدم **أستراليا** مثالاً على بلد اختار سنّ إطارٍ قانونيٍّ متينٍ لمعالجة حماية الأطفال على الإنترنت. وفي عام 2021، وضعت الحكومة إطاراً قانونياً متيناً من خلال قانون السلامة على الإنترنت، الذي يُعالج التنمّر الإلكتروني، والإساءة الإلكترونية للبالغين، والإساءة عبر الصور. وفي عام 2022، أنشأت أستراليا أيضاً مجلس الشباب للسلامة الإلكترونية، الذي يضم 24 عضواً تتراوح أعمارهم بين 13 و24 عاماً، يُقدّم مساهماتٍ مباشرةٍ عن السياسات والبرامج، ويعمل مع شركات التكنولوجيا الكبرى لتعزيز مساءلة المستعملين.[36]

وتقدم **الصين** مثالاً آخر لبلد لديه سياسة شاملة لحماية الأطفال على الإنترنت، وقد نفّذ برامج تعليمية شاملة حول سلامة الإنترنت. وتعمل المدارس كقناة أساسية لتقديم التعليم في مجال الأمن السيبراني، حيث وصلت إلى 90,3 في المائة من القاصرين، بينما تُعدّ العائلات ثاني أهم قناة بنسبة 61,7 في المائة. وبشكل عام، تلقى 85,4 في المائة من القاصرين شكلاً ما من أشكال التعليم في مجال سلامة الإنترنت. وقد أنشئ برنامج "النطاق العريض لحماية القاصرين" من خلال شركات الاتصالات الوطنية، وساعد في توفير الحماية لنحو 160 مليون أسرة لديها أطفال في سن الدراسة، ولديه القدرة على التعامل مع أكثر من 1,02 مليار مكالمة. كما أطلقت الحكومة حملات خاصة لمعالجة مخاوف السلامة على الإنترنت. وقد سنّت الصين العديد من السياسات الرئيسية، بما في ذلك لوائح حماية شبكات المعلومات الشخصية للأطفال ولوائح حماية القاصرين على الإنترنت. وتتجلى فعالية هذه البرامج في الإحصاءات: إذ أصبح أكثر من 70 في المائة من القاصرين قادرين على رصد الاحتيال عبر الإنترنت، ويُظهر أكثر من نصفهم وعياً بالاستخدام السليم للإنترنت.[37]

ودأبت بلدان أخرى أيضاً على دمج التوعية بالأمن السيبراني مع التعليم حول السلامة على الإنترنت. فعلى سبيل المثال، نفّذ **الاتحاد الروسي** "حملة محو الأمية الرقمية" كجزء من برنامجه الوطني الأوسع "الاقتصاد الرقمي" الذي أُطلق عام 2018. ويُقدّم البرنامج محتوىً من خلال فيديوهات رسوم متحركة تفاعلية تُغطّي مواضيع أساسية في مجال الأمن السيبراني، بما في ذلك كشف التصيّد الاحتيالي، وحماية المعلومات الشخصية، والتصدّي للتنمّر الإلكتروني، وممارسات التواصل الاجتماعي الآمنة، والتحقق من المعلومات. ويمتدّ المنهج ليشمل مجالات مُحدّدة، مثل التوعية بحقوق النشر، ومنع الاحتيال الإلكتروني، والحماية من فيروسات الحاسوب، وآداب السلوك

---

[32] يمكن تعريف الإغواء بأنه الاقتراح المتعمد، من خلال تكنولوجيا المعلومات والاتصالات، من قبل شخص بالغ لمقابلة طفل لم يبلغ السن القانوني بعد لممارسة نشاط جنسي، بغرض ارتكاب أعمال الاعتداء الجنسي أو إنتاج مواد الاعتداء الجنسي على الأطفال، وفقاً للمادة 23 من اتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال والاعتداء الجنسيين - https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201

[33] https://www.nspcc.org.uk/keeping-children-safe/online-safety/

[34] https://www.cois.org/about-cis/child-protection/resources؛ https://learning.nspcc.org.uk/online-safety

[35] https://www.itu.int/epublications/ar/publication/global-cybersecurity-index-2024

[36] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/167 المقدمة من أستراليا

[37] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/212 المقدمة من شركة China Mobile Communications Co. Ltd.

الرقمي، وسلامة التعاملات المالية الإلكترونية. ولضمان فعالية التنفيذ، تُزوّد الحملة المُعلّمين بمواد منهجية لدمج دروس الأمن السيبراني هذه في حصص علوم الحاسوب واجتماعات أولياء الأمور والمعلّمين.[38]

ووضع عدد من الإدارات الحكومية أدوات تكنولوجية محددة لحماية الأطفال على الإنترنت. وفي إطار استراتيجية وطنية شاملة لحماية وتمكين الأطفال والشباب على الإنترنت، أطلقت **كوت ديفوار** الموقع الإلكتروني "jemeprotegeenligne.ci" (أحمي نفسي على الإنترنت)[39]، الذي يوفر أدوات تفاعلية ومحركات بحث ومواقع تواصل اجتماعي مصممة خصيصاً للأطفال. كما يتضمن الموقع آلية إبلاغ تتيح للمستعملين الإبلاغ عن الإساءات بشكل مجهول وسري. وتتضمن هذه المبادرة تعاوناً بين مختلف أصحاب المصلحة، وقد حظيت بدعم من مؤسسة مراقبة الإنترنت.[40]

وبالإضافة إلى ذلك، أدركت البلدان والمنظمات أيضاً الحاجة إلى إشراك العديد من أصحاب المصلحة في عملية حماية الأطفال على الإنترنت. ففي **نيجيريا**، تعمل مبادرة حماية الأطفال عبر الإنترنت كإطار عمل أساسي، حيث تدمج السياسات في شروط وأحكام موردي خدمات الإنترنت. وباعتبارها إحدى الجهات الفاعلة الرئيسية في السياسات في البلاد، أنشأت لجنة الاتصالات النيجيرية (NCC) آليات للإبلاغ عن محتوى الإساءة للأطفال ونفذت تدابير حظر لهذه المواد.[41] وأطلقت **جمهورية زامبيا** استراتيجية وطنية لحماية الأطفال على الإنترنت في عام 2020، مع خطة تنفيذ مدتها خمس سنوات (2020-2024) تركز على الهياكل التنظيمية وبناء القدرات والتدابير القانونية والتعاون الدولي والإجراءات التقنية. وحددت زامبيا العديد من الدروس المستفادة بما في ذلك التعاون الأوسع بين أصحاب المصلحة والتمويل المستدام والمستمر وإطار قوي للرصد والتقييم.[42] وأخيراً، تعمل مبادرة حماية الأطفال على الإنترنت (COP) التابعة **للاتحاد** كمنصة قيادة عالمية تضم مجتمعاً لأصحاب المصلحة المتعددين يتمتع بخبرة مثبتة وسجل ناجح في تقديم المساعدة التقنية يمتد لأكثر من 10 سنوات في أنشطة حماية الأطفال على الإنترنت في جميع أنحاء العالم. وتضم هذه المبادرة، التي شارك فيها أكثر من 80 شريكاً معرفياً، أنشطة تشمل تطوير مواد للأطفال[43]، ومبادئ توجيهية موجهة للآباء والمعلمين[44]، والصناعة[45]، وواضعي السياسات[46]، وإجراء تدريب عبر الإنترنت من خلال أكاديمية الاتحاد الدولي للاتصالات، وتقديم تدريب شخصي للمعلمين والشباب.[47] وتُمثل هذه المبادئ التوجيهية المذكورة أعلاه مجموعة شاملة من التوصيات لجميع أصحاب المصلحة المعنيين حول كيفية المساهمة في تطوير بيئة إنترنت آمنة ومُمكّنة للأطفال والشباب. وقد طُوّرت هذه المبادئ التوجيهية ونُشرت من خلال الترجمة والتوطين وحملات التوعية.

وركزت بلدان مختلفة أيضاً على أنشطة بناء القدرات وكذلك على جمع البيانات التجريبية لفهم كيفية تفاعل الأطفال على الإنترنت. وفي **كينيا**، نفّذت هيئة الاتصالات حملتي "Be the COP" و"*Huwezi Tucheza, Tuko Cyber Smart*"، اللتين استهدفتا أولياء الأمور والأوصياء والمعلمين والشباب. كما طوّرت كينيا، بالتعاون مع المعهد الإفريقي للاتصالات المتقدمة، موارد تعليمية ومبادرات لبناء القدرات، بما في ذلك برنامج تدريبي حول حماية الأطفال وتدابير السلامة على الإنترنت. وقد قدم هذا البرنامج التدريب على حماية الأطفال على الإنترنت لنحو 951 مشاركاً من مختلف القطاعات. وتُجري كينيا أيضاً استقصاءً وطنياً حول حماية الأطفال وسلامتهم على الإنترنت لجمع بيانات تجريبية حول سلوكهم على الإنترنت. وكان من المتوقع الانتهاء من هذا الاستقصاء في عام 2024.[48]

[38] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/170 المقدمة من الاتحاد الروسي
[39] https://www.jemeprotegeenligne.ci/
[40] وثيقتا لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/34 و2/137 المقدمتان من كوت ديفوار
[41] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/20 المقدمة من نيجيريا
[42] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/114 المقدمة من زامبيا
[43] https://www.itu-cop-guidelines.com/children
[44] https://www.itu-cop-guidelines.com/parentsandeducators
[45] https://www.itu-cop-guidelines.com/industry
[46] https://www.itu-cop-guidelines.com/policymakers
[47] https://www.itu-cop-guidelines.com/
[48] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/119 المقدمة من كينيا

الفصل الثاني - ممارسات ضمان الأمن السيبراني

برزت ممارسات ضمان الأمن السيبراني كعنصر حاسم في حماية الشبكات والأنظمة والبيانات من الأنشطة الضارة.[49] وتشير ممارسات ضمان الأمن السيبراني بوجه عام إلى الإجراءات المستخدمة لضمان وجود ضوابط ذات صلة لحماية سرية وسلامة وتيسر الأجهزة والأنظمة والشبكات والبيانات الإلكترونية. وبالرغم من ممارسات ضمان الأمن السيبراني لا تمنع الهجمات السيبرانية مباشرة، فإن هدفها، إذا نُفذت على الوجه الصحيح، هو تقليل خطر هذه الهجمات إلى أدنى حد. ويمكن التحقق من ممارسات ضمان الأمن السيبراني قياساً بضوابط ومبادئ توجيهية ومعايير أمنية محددة ويمكن أن تفرضها اللوائح أو تعتمدها دوائر الصناعة طواعية. ولكن، لا يوجد نهج واحد يناسب الجميع، حيث تستخدم السلطات الوطنية وهيئات تنظيم القطاعات في كثير من الأحيان ممارسات مختلفة تتراوح بين التقييم الذاتي والمبادئ التوجيهية الطوعية وصولاً إلى مخططات الوسم وعمليات التحقق الصارمة من الالتزام.

وعلى الرغم من عدم وجود نهج واحد يوصى به، من الواضح أنه في السنوات الأخيرة، حدث تحول مستمر نحو اعتماد ممارسات ضمان الأمن السيبراني في جميع أنحاء العالم، بتطورات مختلفة في عدة بلدان ومناطق. وكمثال على هذا التحول نحو اعتماد ممارسات ضمان الأمن السيبراني، أطلقت **منظمة التعاون والتنمية في المجال الاقتصادي (OECD)** في ديسمبر 2022 توصية المجلس بشأن "الأمن الرقمي للمنتجات والخدمات" والتي توصي باعتماد سياسات لتعزيز الأمن الرقمي للمنتجات والخدمات بما يتناسب مع المخاطر، بدءاً بنهج خفيف يقوم على تدابير سياساتية طوعية، ثم استكشاف الحاجة إلى تدابير إلزامية.[50] وينقل هذا الفصل التحديات التي وُوجهت ويقيّم آثارها ويعرض الدروس المستفادة حتى الآن في تحديد ممارسات ضمان الأمن السيبراني وتنفيذها

1.2 نُهُج لتقييم الأهمية الحاسمة والمخاطر والتكاليف

عند النظر في تنفيذ ممارسات ضمان الأمن السيبراني، من الأهمية بمكان أولاً تحديد ما الذي يحاول أي كيان حمايته والمخاطر التي تواجهها الأصول المحددة. وينبغي للبلدان والشركات التي ترغب في الحماية من الهجمات السيبرانية، أن تحدد على سبيل الأولوية الأنظمة والأصول التي تحتاج إلى الحماية وأن تقيِّم مواطن ضعفها. وفي هذا الصدد، يعد إطار أو مخطط إجراء تقييمات المخاطر أداة مفيدة. وأحد الأطر الأكثر شهرة لإجراء تقييمات المخاطر هو إطار الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا (NIST) في **الولايات المتحدة**،[51] والذي حُدِّث مؤخراً[52] وهو يقدم نهجاً واسع الاستخدام للمساعدة في تحديد مخاطر المنظمة وتقليلها إلى أدنى حد. ويضع هذا الإطار مبادئ توجيهية غير تنظيمية تتيح للمنظمات على الصعيد العالمي تبيُّن مشهد المخاطر الخاصة بها وتطبيق ضوابط الأمن السيبراني المناسبة. ويعتمد الإطار المراجَع، الذي نُشر في أوائل عام 2024، على التعامل الواسع والطويل الأجل مع مجتمع أصحاب المصلحة الذين يستخدمون هذه المبادئ التوجيهية، فضلاً عن المواءمة المستمرة مع المعايير الدولية الأخرى.[53]

وقد سمح وضع المعهد الوطني للمعايير والتكنولوجيا (NIST)، بوصفه وكالة غير تنظيمية، بانخراط أعمق مع أصحاب المصلحة في دوائر الصناعة من جميع أنحاء العالم لفهم تحديات العالم الحقيقي بشكل أفضل وتلقي التعقيبات التي أدرجت في المبادئ التوجيهية الجديدة[54]. والغرض من هذه المبادئ التوجيهية أن تكون قابلة للتكيف ومرنة وقابلة للتطبيق على جميع المنظمات والقطاعات. وقد دمجت شركة **BitSight** إطار الأمن السيبراني لدى المعهد الوطني للمعايير والتكنولوجيا في منصتها التي يستخدمها مختلف الوكالات الحكومية المسؤولة عن الأمن السيبراني (مثل أفرقة الاستجابة للطوارئ الحاسوبية (CERT) والوكالات الوطنية للأمن

---

49 يرتبط الأمن التشغيلي ارتباطاً وثيقاً بممارسات ضمان الأمن السيبراني، حيث يمكن للأمن التشغيلي أن يوفر أساساً جيداً لممارسات الضمان. وعرضت شركة Broadcom نموذج الظروف الجيدة مسلطة الضوء على أنها تتألف من أربعة عناصر رئيسية هي: الأشخاص والعمليات، والمعرفة، ومنتجات الأمن (الأمن الخارجي) والأمن في الأصول (الأمن الداخلي). انظر "تقليل المخاطر وحماية السمعة"، وثيقة لجنة الدراسات 17 لقطاع تقييس الاتصالات SG17-C214 المقدمة من شركة Broadcom

50 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481

51 https://www.nist.gov/cyberframework

52 https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20

53 https://www.nist.gov/cyberframework

54 عرض تقديمي Q3/2_2023_07 مقدم من الولايات المتحدة في ورشة عمل لجنة الدراسات 2 لقطاع تنمية الاتصالات

السيبراني ومنظمي الاتصالات)[55]. ومن خلال هذه المنصة، تستطيع البلدان إجراء تقييمات للمخاطر التي تهدد ما يعتبر حرجاً من بنيتها التحتية وأصولها وقياس عوامل المخاطرة الخاصة بها.

ويمكن لتقييم المخاطر أن يساعد أيضاً على تحديد مستوى الضمان المناسب، بمراعاة حساسية البيانات والأصول الجارية حمايتها، والعواقب المترتبة على الخرق وبيئة التهديد (أي ما إذا كان كيان ما معرضاً لهجمات سيبرانية). وفي بعض الحالات، ستملي المتطلبات التنظيمية مستويات الضمان. وكلما ارتفع مستوى الضمان، كانت الضوابط الأمنية أكثر صرامةً. فعلى سبيل المثال، قد يتطلب مستوى منخفض من الضمان كلمة مرور للنظام أو جدار حماية، بينما يتطلب مستوى أعلى من الضمان إضافة ضوابط أكثر تقدماً مثل التجفير المتقدم والاستيقان المتعدد العوامل.

وفي حين أن ممارسات ضمان الأمن السيبراني تضيف إلى ميزانيات تكنولوجيا المعلومات، فإن التقاعس عن وضع ضوابط أمنية يمكن أن يكون أكثر تكلفةً. فتكاليف التعرض لهجوم سيبراني لا تُقاس من الناحية المالية فحسب، إذ يمكن أن تكون التكلفة الإضافية المتعلقة بالسمعة أشد ضرراً بكثير. ولفقدان ثقة العملاء والمواطنين تأثير طويل الأجل يمتد إلى ما هو أبعد من المال، ويجب أن تكون المنظمات قادرة على فهم ذلك استراتيجياً. وبالمثل، بالنسبة للقطاع العام، قد تؤثر الهجمات الناجحة على تقديم الخدمات العامة والأنشطة الحرجة، كما أن تعطيل هذه الخدمات والأنشطة لا يمكن قياسه من الناحية المالية فقط، لأنه يؤثر على حياة المواطنين.

وقد يكون تخطيط الاستثمار في الأمن السيبراني ووضع ميزانيته لضمان الامتثال للوائح الوطنية مهمة صعبة بالنسبة لمختلف المنظمات. ولدعم المؤسسات في تخطيط تكاليف ضوابط الأمن السيبراني المطلوبة قانوناً، حاولت الهيئة الوطنية للأمن السيبراني (NCA) في **المملكة العربية السعودية** تطوير أداة لتقدير التكلفة من أجل تنفيذ "ضوابط الأمن السيبراني الأساسية" في المملكة العربية السعودية.[56] وبعد التجارب المبكرة، خلصت الهيئة الوطنية للأمن السيبراني إلى أن أداة تقدير التكلفة أثبتت فعاليتها، وتقدم تقديراً جيداً، خاصة بالنسبة للمؤسسات التي لا تزال في المراحل الأولى من تنفيذ الضوابط المتعلقة بالأمن السيبراني، وبالتالي غالباً ما تفتقر إلى سجلات سابقة للميزانية المقدرة أو الوقت أو الموارد اللازمة لتنفيذ ضوابط الأمن السيبراني هذه.

2.2 نُهُج أصحاب المصلحة المتعددين

من المهم مقارنة المبادرات بالمبادرات الأخرى من أجل فهم الممارسات الجيدة والتعلم من نجاح الآخرين وأخطائهم أثناء وضع المبادرات. ومن المهم أيضاً التعامل مع العديد من أصحاب المصلحة، بمن فيهم دوائر الصناعة، للحصول على رؤى هامة بشأن تطوير المبادرة.

وعلى الرغم من أن ممارسات ضمان الأمن السيبراني أصبحت ضرورية بشكل متزايد في أقل البلدان نمواً (LDC)، فقد لا يزال من الصعب تنفيذها. ويمكن أن تكون حالة شركة الدفاع السيبراني عن إفريقيا (CDA) في **توغو** مثالاً لتوضيح بعض التحديات التي تواجهها السوق المحلية في تقديم ضمان الأمن السيبراني عبر مشغلي الخدمات الأساسية (ESO).[57] وقد استُشهد بالافتقار إلى التمويل، وانعدام الثقة في الحكومة كمقدم للخدمة، والافتقار إلى القدرات البشرية والمرافق المحلية، بوصفها بعض التحديات المواجَهة. ولدعم مشغلي الخدمات الأساسية في الالتزام بضوابط الأمن السيبراني المنشورة حديثاً، أنشأت حكومة توغو شراكة بين القطاعين العام والخاص مع مقدم كبير مرموق للأمن السيبراني لتقديم خدمات الأمن السيبراني في القطاعين العام والخاص. ومن خلال هذا نموذج الشراكة هذا، أنشأت توغو شركة الدفاع السيبراني عن إفريقيا (CDA) بوصفها مقدماً محلياً للأمن السيبراني مكتفياً ذاتياً وعالي الجودة لدعم مشغلي الخدمات الأساسية على أساس غير إلزامي. وسمح نموذج الاكتفاء الذاتي المستخدم لتوغو بالحد من التحديات الكثيرة المذكورة أعلاه والبدء في تعزيز المواهب المحلية في مجال الأمن السيبراني، فضلاً عن تشجيع تنمية السوق المحلية. وأشير أيضاً إلى شركة الدفاع السيبراني عن إفريقيا (CDA) ككيان خاص في سوق تنافسية لضمان القدرة على التكيف وعلو جودة الخدمات والتسعير التنافسي.

ومن المهم أيضاً تعزيز التعاون بين واضعي السياسات الذين قد يحددون البيئة التنظيمية ومنظمات المجتمع المدني. ويمكن لمنظمات المجتمع المدني أن تعزز الطلب على الأمن، بالإضافة إلى توجيه التطور السياساتي والتنظيمي على أساس الممارسات الإقليمية والدولية المحددة القائمة. فعلى سبيل المثال،

[55] عرض تقديمي Q3/2_2023_02 مقدم من شركة BitSight في ورشة عمل لجنة الدراسات 2 لقطاع تنمية الاتصالات
[56] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/201 المقدمة من المملكة العربية السعودية
[57] عرض تقديمي Q3/2_2023_09 مقدم من شركة الدفاع السيبراني عن إفريقيا في ورشة عمل لجنة الدراسات 2 لقطاع تنمية الاتصالات

شركة DiploFoundation هي منظمة دولية تقدم برامج تدريبية وخبرات في بناء القدرات للحكومات والهيئات التنظيمية والأعمال التجارية والمجتمع المدني بشأن مسائل الساعة المتعلقة بالأمن السيبراني، وهي تشارك أيضاً في "حوار جنيف بشأن السلوك المسؤول في الفضاء السيبراني".[58] وفي عام 2020، أسفر حوار جنيف عن مجموعة من الممارسات الجيدة،[59] تشمل التعاريف المقترحة للتصميم الآمن وإدارة مواطن الضعف، ونمذجة التهديدات، وأمن الطرف الثالث وسلسلة التوريد، والتنمية الآمنة، وإدارة مواطن الضعف والكشف عنها، فضلاً عن الثقافة التنظيمية.

و**المنتدى العالمي للخبرات السيبرانية (GFCE)** هو منصة دولية تدعم تنسيق المشاريع وتعزز تبادل المعارف والخبرات ومطابقة الطلبات مع عروض دعم بناء القدرات وتطور المشاريع البحثية[60]. وأنشأ المنتدى أربعة محاور إقليمية في جزر المحيط الهادئ وإفريقيا والأمريكتين ومنطقة البحر الكاريبي وجنوب شرق آسيا. ونظراً إلى رقعته العالمية، ودعمه المتنوع في البلدان النامية، فإن المنتدى في وضع جيد لتقديم وجهات نظر أكثر تنوعاً على الصعيد الإقليمي بشأن احتياجات بناء القدرات السيبرانية ومتطلباتها. ويتضمن المنتدى بوابة إلكترونية تستخدم كمستودع للمشاريع المنفَّذة والجارية في مجال بناء القدرات السيبرانية، والموارد والأدوات. وتساعد البوابة الإلكترونية للمنتدى على تقليل ازدواجية الجهود وتساعد أيضاً على تحديد الثغرات والأنماط في تقديم بناء القدرات.[61]

3.2 النُّهج التنظيمية المتطورة

في كثير من الحالات، تُقدم ممارسات ضمان الأمن السيبراني على أساس طوعي قبل أن تصبح إلزامية. ويصبح التحول إلزامياً عموماً عندما ترى الحكومات أن دوائر الصناعة لا تفعل ما يكفي لتأمين المنتجات وأن المستهلكين لا يملكون بالضرورة المعرفة اللازمة لتقييم ما إذا كانت المنتجات آمنة أم لا. ويمكن أن يؤدي ذلك بالحكومات والسلطات الوطنية إلى التصرف والنص على ممارسات الضمان التي تتوقع أن تلبيها دوائر الصناعة. وسواء كان ذلك إلزامياً بموجب القانون أم لا، فمن الممارسات الجيدة استعراض ممارسات ضمان الأمن السيبراني وتكييفها بمرور الوقت في ضوء مشهد التهديدات الدينامية ومخاطر الأمن السيبراني الناشئة.

ففي **البرازيل**، تعرض هيئة تنظيم الاتصالات، الوكالة الوطنية للاتصالات Anatel، مثالاً لنهج متطور يتضمن إنشاء نظام لهيئات إصدار الشهادات ومختبرات الاختبار داخل البلد لإصدار الشهادات لمعدات منشآت العملاء (CPE) أو البوابات المنزلية. وتمثل النهج الأولي للوكالة الوطنية للاتصالات في توفير مبادئ توجيهية غير إلزامية للأمن السيبراني لقطاع الاتصالات. ولكن تبين من خلال إجراء تقييمات المخاطر أن التوصيات ليست كافية لتأمين معدات منشآت العملاء، بالنظر إلى مواطن الضعف والتهديدات المرتبطة بهذا النوع من المعدات، وأن الضرورة تقتضي وضع متطلبات إلزامية دنيا لسلامة هذه المنتجات. وقد نشرت المتطلبات الإلزامية لمقدمي خدمات الاتصالات في البرازيل، في أوائل عام 2023، وهي تركز على مواطن الضعف مثل كلمات المرور غير الآمنة وأجزاء الخدمة الممكّنة بلا داع.[62] وأصبحت المتطلبات سارية في أوائل عام 2024 كجزء من الاختبارات المختبرية الإلزامية للموافقة على المنتَجات.[63] وأوضحت الوكالة الوطنية للاتصالات أن التطور من نهج غير إلزامي إلى متطلبات الشهادة الإلزامية للأمن السيبراني لمجموعة محددة من المعدات ما كان ليتسنى إلا بعد مناقشة شاملة مع القطاع.

وبالمثل، ألقت الهيئة الوطنية للأمن السيبراني (NCA) في **المملكة العربية السعودية** الضوء على مبادرتها لبناء نظام إيكولوجي مستقل للتحقق وإقرار الصلاحية (IV&V) [64] لاختبار واعتماد منتجات من منظور ضمان الأمن السيبراني على المستوى الوطني. وتهدف المبادرة أيضاً إلى تحديد وتصنيف العتاد والبرمجيات التي تتسم بدرجة عالية من الحساسية للمخاطر والتهديدات السيبرانية. وعلاوة على ذلك، تسعى المبادرة إلى المساهمة في تطوير القدرات البشرية في مجال التحقق وإقرار الصلاحية. وتنظر خارطة طريق المبادرة في البدء ببرنامج طوعي قبل

---

58 عرض تقديمي Q3/2_2023_11 مقدم من DiploFoundation في ورشة عمل لجنة الدراسات 2 لقطاع تنمية الاتصالات

59 https://genevadialogue.ch/goodpractices/

60 عرض تقديمي Q3/2_2023_12 مقدم من المنتدى العالمي للخبرة السيبرانية في ورشة عمل لجنة الدراسات 2 لقطاع تنمية الاتصالات

61 https://cybilportal.org/

62 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/58 المقدمة من البرازيل

63 عرض تقديمي Q3/2_2023_12 مقدم من البرازيل؛
و https://informacoes.anatel.gov.br/legislacao/index.php/component/content/article?id=1505؛
و https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2023/1850-ato-2436 في ورشة عمل لجنة الدراسات 2 لقطاع تنمية الاتصالات

64 https://nca.gov.sa/en/news?item=535

جعل ضمان الأمن السيبراني التزاماً إلزامياً. وأشارت الهيئة الوطنية للأمن السيبراني أيضاً إلى أهمية أن يصبح مثل هذا النظام الإيكولوجي "مستداماً ذاتياً" في نهاية المطاف، وهذا ما استرشد به نهج الهيئة لتشجيع أصحاب المصلحة في السوق على إجراء تقييمات التحقق وإقرار الصلاحية هذه.

وفي مجال أمن إنترنت الأشياء (IoT)، تقدم المملكة المتحدة وأستراليا أيضاً دراسات حالة للتطور من نهج ضمان الأمن السيبراني الطوعي إلى الإلزامي. وفي السنوات الأخيرة، قرر كلا البلدين، من خلال التشريعات، فرض متطلب أمني أساسي لمنتجات إنترنت الأشياء الاستهلاكية استناداً إلى معيار المعهد الأوروبي لمعايير الاتصالات (ETSI) EN 303 645،[65] وهو أول معيار للأمن السيبراني قابل للتطبيق عالمياً لأجهزة إنترنت الأشياء الاستهلاكية.

ففي **المملكة المتحدة**، سيكون المصنعون والمستوردون والموزعون ملزمين بالامتثال لثلاثة من المبادئ التوجيهية الأمنية الثلاثة عشر الصادرة عن المعهد الأوروبي لمعايير الاتصالات (ETSI)، ويخول القانون الحكومة صلاحيات لاعتماد متطلبات إضافية عند الضرورة، تبعاً لتقييمات التهديد المنتظمة. وقد جاء قرار فرض خط أساس للمتطلبات الأمنية بعد فترة من الاعتماد الطوعي. وفي عام 2018، وضع البلد مدونة ممارسات طوعية[66] لأمن إنترنت الأشياء للمستهلك، ولكن التزام دوائر الصناعة لم يكن على النحو المتوقع. وبينت الأدلة التي جُمعت من خلال عمليات التشاور أن المستهلكين يثمّنون الأمن وأنهم على استعداد لدفع علاوة سعرية لقاء المنتجات المأمونة. ولكن تهديدات الأمن السيبراني لا تخضع لنفس مستوى التنظيم القوي الذي تخضع له سلامة المنتجات، مما يؤدي إلى نقص الشفافية من جانب المصنعين وبطء اعتماد السياسات الأمنية. وتوصلت الأدلة أيضاً إلى أن سوق المنتجات الاستهلاكية القابلة للتوصيل لا يشجع اعتماد الميزات الأمنية الأساسية، نظراً لأن المستهلكين يفترضون في الغالب أن المنتجات آمنة أصلاً. ويهدف نظام أمن المنتجات والبنية التحتية للاتصالات (PTSI) إلى سد هذه الفجوة بفرض عناصر مدونة الممارسات لضمان إدراك المصنعين لمواطن الضعف واتخاذ خطوات للتخفيف منها. ودخل نظام أمن المنتجات والبنية التحتية للاتصالات حيز النفاذ في أبريل 2024 وهو ينطبق على أي منتج استهلاكي يمكنه التوصيل بالإنترنت.[67]

وبالمثل في **أستراليا**، وجدت الحكومة إقبالاً ضعيفاً على مدونة الممارسات الطوعية "تأمين إنترنت الأشياء للمستهلكين" التي نشرت في عام 2020. وفي عام 2024، اقترحت الحكومة قانوناً يفرض مدونة الممارسات، وحصل مشروع مدونة الممارسات على إجماع بعد المشاورة العامة. ويتماشى هذا القانون بشكل وثيق مع نهج المملكة المتحدة، ويهدف إلى منح الوزير سلطة فرض معايير أمنية محددة لأجهزة إنترنت الأشياء من خلال تشريعات (قواعد) ثانوية. ومن خلال دمج المعايير في القواعد بدلاً من التشريعات الأولية، تأمل حكومة أستراليا أن تتمكن من تحديث هذه المعايير سريعاً لضمان حماية المستهلكين في أستراليا بناء على الممارسات الجيدة الدولية والصناعية.[68]

ومن التحديات التي تحدَدت في **المملكة المتحدة** التأثير الممكن على المشاريع الصغيرة والصغيرة جداً التي قد تواجه صعوبات في الالتزام بالنظام PSTI الجديد. وتعكف سلطة إنفاذ نظام أمن المنتجات والبنية التحتية للاتصالات في المملكة المتحدة على وضع إرشادات للتخفيف من أي تأثير غير متناسب. وبالإضافة إلى العمل مع دوائر الصناعة، أفادت المملكة المتحدة بأن المتطلبات الثلاثة الأولى المزمع فرضها في الخطة قد تحدَدت وأُعلنت بشفافية لعدة سنوات. وخلال هذه الفترة، أجرت المملكة المتحدة عدداً من التمارين بشأن عملية تنفيذ النظام، بما في ذلك متطلبات كلمة المرور، والمعمارية الأساسية للمنتج، والتعرض للثغرات الأمنية، ومتطلبات الشفافية الأمنية. وقد أظهر تقييم التأثير أن الفوائد الإجمالية لخفض حجم الهجمات السيبرانية على المستهلكين والشركات يُتوقع أن تتجاوز التكاليف المرتبطة بتنفيذ النظام PSTI. وبما أن نظام أمن المنتجات والبنية التحتية للاتصالات (2022) هو أول تشريع إلزامي لمنتجات الأمن السيبراني في العالم، فإن تكلفة إنفاذ النظام غير مؤكدة، إلا أن التقديرات الأولية تشير إلى أن التمويل المخصص سيكون كافياً.

وفي بعض الحالات، يحدد نوع المستعمل أو العميل ما إذا كانت ممارسة ضمان الأمن السيبراني إلزامية أم طوعية. فعلى سبيل المثال، أطلقت **جمهورية كوريا** برنامج ضمان الأمن السحابي (CSAP)، وهو شهادة أمنية لخدمات الحوسبة السحابية.[69] وبصفة عامة، تكون شهادة برنامج ضمان الأمن السحابي (CSAP) طوعية. ولكن يتعين على العملاء في القطاع العام (الوكالات العامة) استخدام خدمة سحابية حاصلة على شهادة برنامج ضمان

[65] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
[66] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
[67] عرض تقديمي Q3/2_2023_03 مقدم من المملكة المتحدة في ورشة عمل لجنة الدراسات 2 لقطاع تنمية الاتصالات
[68] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/320 المقدمة من أستراليا
[69] https://isms.kisa.or.kr/main/csap/intro/index.jsp ووثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/34 المقدمة من جمهورية كوريا

الأمن السحابي (CSAP) وفقاً للوائح ذات الصلة، وبالتالي يتعين على مقدمي الخدمات السحابية الحصول على شهادة CSAP عند تقديم الخدمات السحابية للوكالات العامة.

ويعتبر إجراء عمليات مراجعة داخلية منتظمة يمكنها أن تساعد على تحديد الثغرات في الضوابط ومخاطر التعرض، فضلاً عن الاشتراك في المعلومات الاستخبارية عن التهديدات، من الممارسات السديدة. وحتى في حال اعتماد منتج ما، فإنه قد يعاني، على مدى دورة حياته، من عيوب أمنية. وتتطلب أي خطة لإصدار الشهادات تقديم المعلومات في وقت محدد، فهذه العملية لا تحتسب التغيرات الدينامية في التهديدات مستقبلاً. وأظهرت دراسة حديثة أجرتها شركة BitSight وجود علاقة قوية بين ضعف "إيقاع الترقيع التصحيحي" لنقاط الضعف واحتمال التعرض لحادث أمني سيبراني،[70] وهو ما يشير إلى الأهمية الحرجة لتحديث الأنظمة بمجرد توفر البرمجيات التصحيحية الأمنية، مع مراعاة التوزيع المتفاوت المبلغ عنه للبرمجيات التصحيحية في جميع أنحاء العالم.

واختبار الاختراق أو "اختبار الاقتحام" هو عملية لضمان الأمن تساعد على تقييم أمن نظام تكنولوجيا المعلومات وتحديد مواطن الضعف التي يمكن استخدامها لاستغلال الأنظمة. وتدير هيئة Ofcom، وهي هيئة تنظيم الاتصالات في **المملكة المتحدة**، خطة TBEST طواعية مع مقدمي خدمات الاتصالات. ويهدف مخطط اختبار الاختراق هذا إلى تحفيز أي هجوم سيبراني من أجل تحديد مواطن الضعف الأمنية التي يمكن بعد ذلك معالجتها، من خلال عملية معالجة، لتحسين وضع أمن شبكة المشغلين.[71]، [72] وبصورة أوسع، يعتبر هذا المخطط مثالاً على نهج النظام الإشرافي الذي تتبعه هيئة Ofcom، والذي يشدد على أهمية بناء علاقات تعاونية مع دوائر الصناعة التي تنظمها الهيئة. وحتى الآن، فإن جميع مقدمي خدمات الاتصالات في المملكة المتحدة اعتمدوا خطة TBEST طواعية، أو أنهم يقومون بذلك، وقد أدخلوا تغييرات نتيجة لذلك. وخطة TBEST ليست "معياراً" ولا هو عملية إصدار شهادات. بل الهدف منه هو تمكين مقدمي خدمات الاتصالات من التنبه إلى التهديدات السيبرانية وتنفيذ التغييرات المناسبة في الوقت المناسب لتحسين قدراتهم في مجال الدفاع السيبراني. وإذ يعي المشغل مواطن الضعف هذه ويعالجها، يصبح في وضع أقوى بكثير لحماية شبكاته.

4.2 تثقيف المستهلكين والمصنّعين

بُذلت جهود لتثقيف الجمهور بشأن أهمية الأمن السيبراني وفوائد اختيار منتجات أكثر أمناً.

وأحد النُهج في هذا الصدد يتمثل في وضع مخطط لتوسيم الأمن السيبراني، ويمكن أن تكون المنتجات المعتمدة مصحوبة بوسم على النحو المعمول به في **جمهورية سنغافورة** مثلاً. وتعمل مخططات الوسم أساساً كأداة إعلامية للمستهلكين. وفي سنغافورة، تهدف وكالة الأمن السيبراني (CSA) المسؤولة عن مخطط توسيم الأمن السيبراني، إلى مساعدة المستهلكين على التمييز بين أجهزة إنترنت الأشياء الأكثر أمناً والأقل أمناً.[73] والمخطط طوعي (باستثناء مسيِّرات Wi-Fi التي يكون إلزامياً لها) وله أربعة مستويات، حيث يمثل المستوى 1 خط الأساس الأمني. ويستند المستويان 1 و2 إلى التقييم الذاتي من جانب المصنعين، أما المستويان 3 و4 فيعتمدان على تقييم طرف ثالث بواسطة مختبر معتمد. والمخطط متعدد المستويات لتحفيز المصنعين على إدراج تدابير أمنية إضافية تتجاوز المتطلبات الأساسية.

ونظرت وكالة الأمن السيبراني (CSA) أيضاً في المفاضلات التي ينطوي عليها فرض معايير الأمن السيبراني، بما في ذلك خطر خروج المصنعين من السوق نتيجة لزيادة تكاليف الالتزام. وبدلاً من ذلك، فإن الهدف هو تغيير عقلية المصنعين لكي ينظروا إلى الأمن السيبراني كعامل تمكين وتمييز في السوق وليس كتكلفة إضافية. وفيما يتعلق بتأثير مخطط وسم الأمن السيبراني في سنغافورة، فالعملية لا تزال في مراحلها المبكرة، والجهود جارية لتشجيع المصنعين على المشاركة في المخطط وتحسين أمنهم السيبراني. وسيجرى استطلاع عام في المستقبل لتقييم وعي المستهلك وسلوكه. وتقل تكلفة الالتزام إلى أدنى حد على المصنعين في المستويين 1 و2، ولم تحدث زيادة كبيرة في تكلفة المنتجات على المستهلكين. وبوجود المخطط الطوعي، يُتوقع لقوى السوق أن تدفع عجلة التحسينات في الأمن السيبراني بين المصنعين.

---

[70] https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity

[71] يعمل في شراكة وثيقة مع وزارة العلوم والابتكار والتكنولوجيا (DSIT) والمركز الوطني للأمن السيبراني (NCSC) لتشغيله.

[72] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/74 المقدمة من المملكة المتحدة

[73] عرض تقديمي Q3/2_2023_05 مقدم من سنغافورة في ورشة عمل لجنة الدراسات 2 لقطاع تنمية الاتصالات

ففي **الولايات المتحدة**، يعد برنامج علامة الثقة السيبرانية الأمريكي المنشأ حديثاً مثالاً على برنامج طوعي لوسم الأمن السيبراني لمنتجات إنترنت الأشياء.[74] ولدى تطوير البرنامج، سلطت اللجنة الفيدرالية للاتصالات (FCC) الضوء على أن من الأهمية بمكان التماس مدخلات الجمهور والتعليقات من جميع أصحاب المصلحة المعنيين، بمن فيهم دوائر الصناعة والحكومة والمجتمع المدني، لتصميم وإدارة برنامج يلبي الاحتياجات المحددة. وبينما تتولى اللجنة الفيدرالية للاتصالات قيادة البرنامج، سيُنفذ برنامج علامة الثقة السيبرانية جنباً إلى جنب مع مجموعة متنوعة من الشركاء بين الوكالات الذين يحتاجون إلى تعاون وثيق مع جميع فروع الحكومة المعنية.

وبعيداً عن الوسوم، من المهم بالقدر نفسه الاستثمار في الضوابط التقنية وبناء الوعي وتثقيف السكان بشأن مخاطر الأمن السيبراني التي تواجهها المنظمات والبلدان. وتشكل هجمات برمجيات الفدية حالياً الاتجاه الأكثر إقلاقاً. وبالنسبة لهذه الأنواع من الهجمات، فإن الناقل الرئيسي للهجوم، بمعنى الطريقة التي يدخل بها المجرم إلى أي شبكة أو نظام، هو عبر رسائل البريد الإلكتروني التصيدية.[75] وفي هذا السياق، كثيراً ما يتمكّن المجرمون السيبرانيون من تجاوز الضوابط الأمنية عند قيام الأشخاص بمجرد النقر على بريد إلكتروني تصيدي. لذلك، من الأهمية بمكان لضمان الأمن السيبراني توعية المواطنين والموظفين بهذه القضايا. ويتناول الفصل 1 من هذا التقرير تعزيز وعي المستعمل بالأمن السيبراني.

5.2 النُهج المتبعة في الاتفاقات الدولية بشأن التآزر/التنسيق والمعاملة بالمثل

إن وجود اتفاقات المعاملة بالمثل بين نماذج ضمان الأمن السيبراني، مثل مخططات إصدار الشهادات والوسم، يمكن أن يكون عاملاً محدداً في توسيع نطاق هذه الممارسات. وكما أوضح أصحاب المصلحة، يمكن لاتفاقات المعاملة بالمثل أن تساعد على تسهيل التزام الجهات الفاعلة الصناعية العاملة في أسواق متعددة. ولكن بالنظر إلى أن اتفاقات المعاملة بالمثل هي آلية رسمية، وقد يكون لها العديد من الشروط الوطنية، وتستغرق وقتاً للموافقة عليها وتوقيعها، يجب أن تلتمس ممارسات لضمان الأمن السيبراني أوجه تآزر مع النُهج الدولية القائمة التي تتماشى مع الاحتياجات والأولويات الوطنية. ومن شأن ذلك أن يخفف العبء التنظيمي على مقدمي المنتجات والخدمات بغية تجنب المتطلبات المتناقضة.

وشددت وكالة الأمن السيبراني (CSA) على أهمية التعاون الدولي في وضع وتنفيذ مخططها لتوسيم الأمن السيبراني. وقد وقعت **سنغافورة** ترتيبات الاعتراف المتبادل مع فنلندا وجمهورية ألمانيا الاتحادية وهي تعمل على توسيع شراكاتها في هذا المجال. وأشارت سنغافورة مستعرضةً تجربتها إلى أن الحكومات يتعين أن تكون استباقية في إرساء الاعتراف، على الرغم من أن للمصنعين أيضاً مصلحة في دعم عملية الاعتراف حيث تساهم ترتيبات الاعتراف المتبادل في تقليل عبء الاختبارات المتكررة وإصدار الشهادات، بالإضافة إلى المساعدة في الوصول إلى الأسواق في إطار ولايات قضائية مختلفة. وتنطوي العملية على جمع الأطراف المهتمة معاً لتنسيق المتطلبات ووضع معايير مشتركة واقعية وغير مغالية في أعبائها.

وعلى المستوى الأوروبي، تتمتع **وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA)** بصلاحية وضع ثلاث خطط لإصدار الشهادات من شأنها أن تحظى بالاعتراف عبر السوق الداخلية، فتحصل بالتالي على "الاعتراف المتبادل" التلقائي عبر الاتحاد الأوروبي. وهذه الخطط هي: *خطة المعايير المشتركة التي وضعها الاتحاد الأوروبي لمنتجات تكنولوجيا المعلومات والاتصالات*، التي اعتُمدت اللائحة التنفيذية الخاصة بها في أوائل عام 2024؛ و*خطة الخدمات السحابية*، التي لا تزال قيد المناقشة؛ وأخيراً، *خطة تكنولوجيا الجيل الخامس (5G)*، الجاري تطويرها.[76]

وبالإضافة إلى المعاملة بالمثل، وبالنظر إلى الأسواق الدولية التي تعمل فيها دوائر صناعة الاتصالات، فإن تنسيق متطلبات الأمن الأساسية هو أيضاً من الاعتبارات الهامة. وتقدم معايير المعهد الأوروبي لمعايير الاتصالات (ETSI) بشأن المنتجات الاستهلاكية لإنترنت الأشياء مثالاً على محاولة تنسيق المتطلبات الأمنية الأساسية. والسؤال الرئيسي هو إلى أي مدى ستتسق الأطر التنظيمية المختلفة، وإلى أي مدى ستترابط من خلال المعايير الدولية نفسها. وفي هذا الصدد، لوحظ أن تعزيز الحوار وحتى إيجاد المكان المناسب له يشكل تحدياً. وفي مجال التنسيق، تتطلب أنشطة وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) في مجال تقييس الأمن السيبراني وتكنولوجيا الجيل الخامس التعاون بين اللجنة الأوروبية المعنية بالتقييس (CEN)، واللجنة الأوروبية للتقييس

---

[74] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/196 المقدمة من الولايات المتحدة

[75] تكتيك شائع يستخدمه المجرمون السيبرانيون لخداع الناس كي يكشفوا عن معلومات حساسة أو ينزلوا برمجيات ضارة تصيب النظام المستهدَف/الشبكة المستهدَفة.

[76] عرض تقديمي Q3/2_2023_10 مقدم من وكالة الاتحاد الأوروبي للأمن السيبراني في ورشة عمل لجنة الدراسات 2 لقطاع تنمية الاتصالات

الكهرتقني (CENELEC)، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، والمنظمة الدولية للتوحيد القياسي (ISO)، واللجنة الكهرتقنية الدولية (IEC)، ورابطة النظام العالمي للاتصالات المتنقلة (GSMA)، ومشروع شراكة الجيل الثالث (3GPP) والمنصة GlobalPlatform. ويتمثل أحد النواتج الرئيسية لوكالة الاتحاد الأوروبي للأمن السيبراني في تجميع ضوابط أمن تكنولوجيا الجيل الخامس من مختلف منظمات وضع المعايير (SDO) في مستودع واحد.[77]

[77] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

الفصل الثالث - التنسيق الوطني لأفرقة الاستجابة لحوادث الأمن السيبراني من أجل صمود البنى التحتية الحرجة والاستجابة لحوادث الأمن السيبراني

في ظل المشهد الرقمي الراهن سريع التطور، تواجه المنظمات تهديداً متزايداً من حوادث الأمن السيبراني التي قد تُعرّض البيانات الحساسة للخطر، وتُعطّل العمليات، وتُقوّض ثقة أصحاب المصلحة. ويعزز التنسيق الوطني لجهود أفرقة الاستجابة لحوادث الأمن السيبراني (CIRT) قدرة البنية التحتية الحرجة (CI) على الصمود. ومن خلال تعزيز التعاون وتبادل المعلومات والبروتوكولات الموحدة، تهدف هذه المبادرات إلى تعزيز القدرة الجماعية على اكتشاف الحوادث السيبرانية والتخفيف من حدتها والتعافي منها بكفاءة. ولتحقيق هذا الهدف، ينبغي للدول الأعضاء تكثيف جهودها لإنشاء وتطوير أفرقة الاستجابة لحوادث الأمن السيبراني، باعتبارها عادةً الخطوة الأولى المهمة نحو إرساء ثقافة الأمن السيبراني. وجدير بالإشارة إلى أن "أفرقة الاستجابة لحوادث الأمن السيبراني" يُشار إليها أيضاً باسم "CSIRT" وباسم "CERT" (أفرقة الاستجابة للطوارئ الحاسوبية)، وهذه المصطلحات مترادفة لأغراض هذا التقرير.[78]

وإحدى مهام أفرقة الاستجابة للحوادث السيبرانية الوطنية هي الاستجابة للتهديدات التي تستهدف البنية التحتية الحرجة (CI). وتشير البنية التحتية الحرجة إلى مجموعة من الأنظمة والشبكات والأصول التي تُعتبر أساسية للسلامة العامة. ولا يوجد تعريف واحد لما يُشكل "بنية تحتية حرجة"، إذ تُحدد على المستوى الوطني بناءً على الاحتياجات والأولويات الوطنية للبلدان، بيد أنه يشمل عادةً قطاعات مثل النقل وأنظمة الطاقة وأنظمة الاتصالات وأنظمة المياه والأنظمة المالية والرعاية الصحية. ولا يزال استهداف الأنشطة السيبرانية الضارة للبنية التحتية الحرجة الوطنية يُمثل تحدياً كبيراً للحكومات، وقد يُشكل مخاطر على المواطنين. ويشير تقرير صادر عن شركة KnowBe4 عام 2024 إلى أن الأنشطة السيبرانية الضارة ضد البنية التحتية الحرجة قد ارتفعت بنسبة 30 في المائة منذ عام 2022، مُمثلةً أكثر من 420 مليون هجوم بين يناير 2023 و2024. وهذا يُعادل 13 هجوماً في كل ثانية.[79]

وتُشكل هجمات البنية التحتية الحرجة أكبر تهديد يؤثر على حياة المواطنين اليومية. وغالباً ما تشمل الأهداف خدمات الرعاية الصحية وخدمات الطوارئ، مما يؤثر على القدرة على تلقي الرعاية الطبية، مثل العمليات الجراحية والوصفات الطبية. ومن الأمثلة المستهدفة الأخرى البنية التحتية للطاقة، مثل شبكات الكهرباء. ونظراً لاحتمال تأثيرها على الأرواح، يُعد التنسيق والاستجابة لمثل هذه الحوادث أمراً بالغ الأهمية ووظيفة أساسية لأفرقة الاستجابة للحوادث السيبرانية.

وكجزء من تطوير أفرقة الاستجابة للحوادث السيبرانية واكتمالها، غالباً ما تضع البلدان خططاً قوية للاستجابة لحوادث الأمن السيبراني للكشف عن الخروقات الأمنية واحتوائها والتخفيف منها والتعافي منها بشكل فعال. وتُعد خطة الاستجابة الاستباقية والمحددة جيداً لحوادث الأمن السيبراني أمراً ضرورياً للمنظمات للتخفيف من تأثير الحوادث الأمنية بشكل فعال. وقد اعتمدت البلدان نماذج مختلفة لخطط الاستجابة لحوادث الأمن السيبراني من أجل إدارة المخاطر والحد من الأنشطة السيبرانية الضارة على أفضل وجه. وتستخدم هذه النماذج عموماً نهجاً شاملاً، يدمج الممارسات الجيدة، ويعزز ثقافة التحسين المستمر لتعزيز القدرة على الصمود في مواجهة التهديدات السيبرانية وحماية الأصول الرقمية. ومع تطور مشهد التهديدات، يجب أن تظل استراتيجيات الاستجابة للحوادث متقدمة خطوة على خصوم الإنترنت وأن تحمي سلامة المنظمة وثقتها.

ومن الاتجاهات الحديثة في إدارة حوادث الاستجابة، إنشاء مراكز تنسيق سيبراني وطنية لتعزيز التنسيق على مستوى الحكومة ككل. فخلال الحوادث السيبرانية الخطيرة، حيث غالباً ما تشارك عدة جهات حكومية؛ يمكن

---

[78] لمزيد من المعلومات عن المصطلحات، أنظر مطبوع وكالة الاتحاد الأوروبي للأمن السيبراني بشأن "*كيفية إنشاء أفرقة الاستجابة لحوادث الأمن السيبراني والأداة البرمجية SOC*" - https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

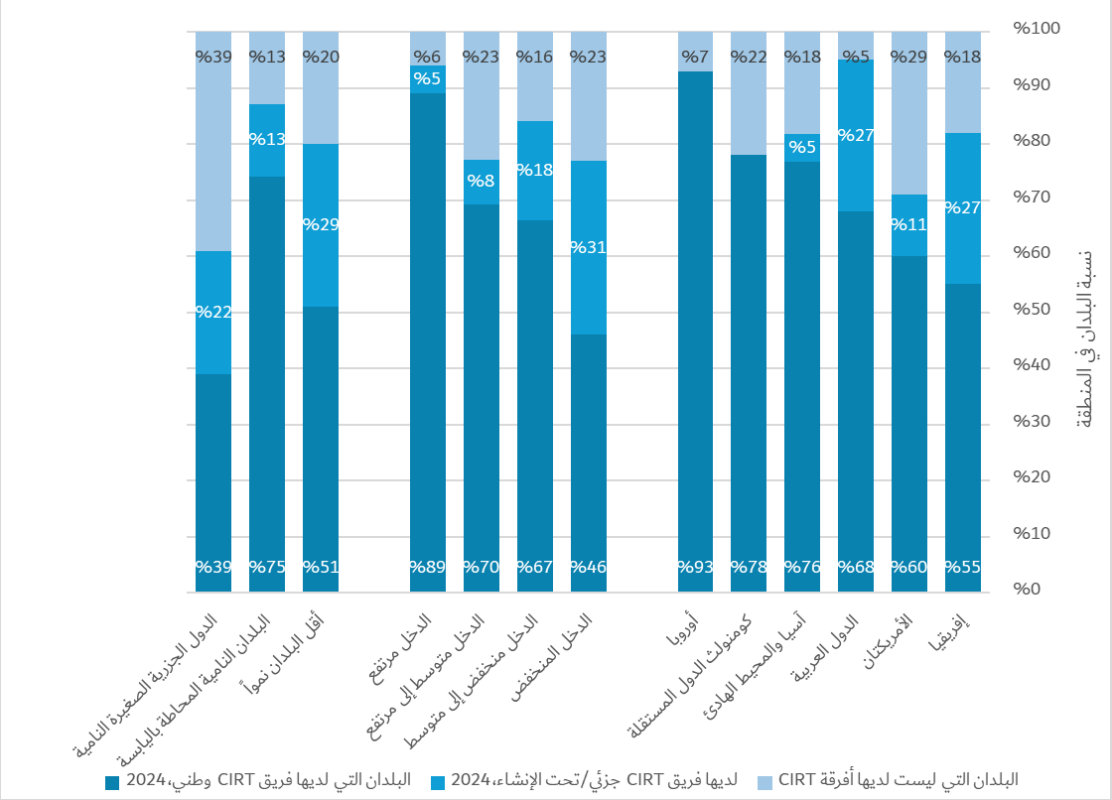
[79] https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf?hsLang=en-us

أن يكون تنسيق الاستجابة السريعة هو العامل الحاسم بين الآثار الطفيفة والكبيرة. ومن شأن وجود مركز أو وحدة تنسيق مركزية أن يتيح الاستجابة السريعة والإدارة والسيطرة الشاملة. وجدير بالذكر أن البنية التحتية الحرجة ليست بالضرورة بنية تحتية مملوكة ومدارة من قِبل القطاع العام، وبالتالي، يُعدّ ضمان التنسيق مع القطاع الخاص أيضاً عنصراً بالغ الأهمية عند مواجهة الحوادث السيبرانية والاستجابة لها.

1.3 إنشاء أفرقة الاستجابة للحوادث الحاسوبية

وفقاً للرقم القياسي العالمي للأمن السيبراني (GCI) لعام 2024،[80] "*يمتلك 139 بلداً فريقاً وطنياً للاستجابة للحوادث السيبرانية، في حين أن 55 دولة ليس لديها فريق أو فريق وطني قيد الإنشاء للاستجابة للحوادث السيبرانية*".

الشكل 1: النسبة المئوية للبلدان التي لديها فريق استجابة للحوادث السيبرانية، بحسب المنطقة/مستوى الدخل/المستوى الإنمائي



المصدر: الاتحاد الدولي للاتصالات

تختلف أدوار أفرقة الاستجابة للحوادث السيبرانية، ولكن من أهم وظائفها اكتشاف وتحليل التهديدات المحتملة في الشبكات والأنظمة، والاستجابة لها لتخفيف آثارها. ويُعدّ إنشاء فريق استجابة للحوادث السيبرانية خطوةً مهمةً نحو تعزيز ثقافة الوعي بالأمن السيبراني وصموده. ويشمل إنشاء فريق الاستجابة للحوادث السيبرانية بناء القدرات والآليات اللازمة لحماية البنية التحتية الحرجة.

وقد أنشأت حكومة **كينيا** مركز تنسيق الفريق الوطني للاستجابة للحوادث الحاسوبية في كينيا (KE-CERT/CC) لتنسيق جهود الأمن السيبراني الوطنية، والعمل كجهة اتصال وطنية في هذا الشأن. ويتألف المركز KE-CERT/CC من فريق يضم أصحاب مصلحة متعددين، يتمتعون بمهارات متنوعة للاستجابة للحوادث الأمنية الحاسوبية وإدارتها بفعالية. وإدراكاً منها لأهمية الأمن السيبراني في تعزيز اقتصاد رقمي مزدهر، أطلقت هيئة

[80] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

الاتصالات (CA) الكينية سلسلة دورات تدريبية وفعاليات هاكاثون للأمن السيبراني في كينيا لبناء القدرات المحلية في مجال الأمن السيبراني.[81]

وتعمل **جمهورية قيرغيزستان**، بمساعدة الاتحاد الدولي للاتصالات، على إنشاء فريق وطني للاستجابة لحوادث الأمن السيبراني. وتشمل مهام هذا الفريق تحديد التهديدات السيبرانية وإدارتها والاستجابة لها، بالإضافة إلى قدرات المراقبة والإنذار والاستجابة للحوادث، وبناء القدرات الوطنية، ونقل الدراية التقنية لتقيق مزيد من التطوير في مجال حماية البنية التحتية الحرجة للمعلومات.[82]

ويتعاون **الاتحاد** مع الدول الأعضاء والمنظمات العالمية لتعزيز الأمن السيبراني من خلال إنشاء وتطوير أفرقة الاستجابة للحوادث السيبرانية الوطنية والإقليمية. ومن خلال مكتب تنمية الاتصالات (BDT)، يجري الاتحاد تقييمات لمدى اكتمال أفرقة الاستجابة للحوادث السيبرانية، حيث ساعد حتى الآن 84 بلداً على تقييم جاهزيتها للأمن السيبراني وإنشاء أفرقة وطنية للاستجابة للحوادث السيبرانية أو تحسينها. وقد نفذ الاتحاد 21 مشروعاً مرتبطاً بأفرقة الاستجابة للحوادث السيبرانية، ويعمل حالياً على ثلاثة مشاريع أخرى. وقد أُجريت تقييمات اكتمال لأفرقة الاستجابة للحوادث السيبرانية في أذربيجان وسيراليون وجمهورية تنزانيا المتحدة، وتُجري حالياً تقييمات في جمهورية زمبابوي ومملكة بوتان ومملكة ليسوتو.[83] وتُفيد هذه التقييمات أفرقة الاستجابة للحوادث السيبرانية الوطنية في صياغة خططها التشغيلية للتحسين. كما يتعاون الاتحاد مع مجتمع FIRST لتعزيز إطار خدمات أفرقة الاستجابة للحوادث السيبرانية وتنقيح مواد التدريب لبناء القدرات في مجال إدارة عمليات أفرقة الاستجابة للحوادث السيبرانية الوطنية.[84]

2.3 دور أفرقة الاستجابة للحوادث الحاسوبية ومسؤولياتها، والبنية التحتية الحرجة

لأفرقة الاستجابة للحوادث السيبرانية دور حيوي في حماية البنية التحتية الحرجة في مختلف القطاعات من خلال توفير المراقبة في الوقت الفعلي، وإدارة الحوادث، وتحليل التهديدات، وتقييم مواطن الضعف. وتتولى هذه الأفرقة عادةً مسؤولية ضمان قدرة أنظمة تكنولوجيا المعلومات والاتصالات (ICT) على الصمود، وتمكين الكشف السريع عن تهديدات الأمن السيبراني ومواجهتها، وتنسيق الجهود لتدنية تأثير الحوادث على الأمن الوطني والسلامة العامة والاقتصاد. وتتولى هذه الأفرقة أدواراً وعلاقات مختلفة، وفقاً لاحتياجات البلد ومستواه الإنمائي وقطاعات البنية التحتية الحرجة فيه.

ففي **جمهورية ليتوانيا**، يعمل الفريق الوطني للاستجابة للطوارئ الحاسوبية (CIRT) تحت إشراف المركز الوطني للأمن السيبراني (NCSC) الأوسع نطاقاً، ويركز بشكل خاص على الاستجابة للحوادث السيبرانية وتنسيق الصمود في جميع قطاعات البنية التحتية الحرجة. وقد سعت الحكومة جاهدةً لضمان امتلاك الفريق للمسؤوليات والقدرات التقنية اللازمة لحماية البنية التحتية الحرجة بفعالية، ويُعدّ هذا العمل نموذجاً يُحتذى به للبلدان الأخرى التي تسعى إلى بناء قدرات أفرقتها. وللفريق دور محوري في توفير خدمات إدارة الحوادث لأصحاب المصلحة في القطاعين العام والخاص، بما يضمن تنفيذ الاستجابات المناسبة أثناء الهجمات السيبرانية وبعدها. ومن الجوانب الرئيسية لدور الفريق في إدارة الحوادث قدرته على التنسيق مع مسؤول الشبكة أو النظام المتضررين، مما يُسهّل التعافي السريع للعمليات.

أثناء الحوادث الكبرى، ينتشر متخصصو فريق الاستجابة للطوارئ الحاسوبية في ليتوانيا في مواقعهم لمساعدة مشغلي البنية التحتية الحرجة على استعادة العمليات الاعتيادية. فعلى سبيل المثال، أثناء هجوم من هجمات الحرمان من الخدمة الموزع (DDoS) على قطاع الاتصالات في ليتوانيا، قام فريق الاستجابة لحالات الطوارئ الحاسوبية الوطني بدور حاسم في تنسيق الاتصالات بين شركات التشغيل المتضررة وتقديم توصيات تقنية ساعدت في استعادة الخدمات بسرعة.

ولا يقتصر دور حماية البنية التحتية الحرجة على الاستجابة للحوادث السيبرانية الضارة فحسب، بل يشمل أيضاً الوقاية منها، من خلال ميزة أكثر تطوراً لأفرقة الاستجابة للطوارئ الحاسوبية. كما أوكلت ليتوانيا إلى فريق الاستجابة للطوارئ الحاسوبية التابع لها مسؤولية إدارة الثغرات الأمنية من خلال جمع المعلومات من المصادر العامة والمنتديات المغلقة وآليات الإبلاغ عن الثغرات. ويقوم الفريق بمسح الأصول الرقمية الليتوانية بنشاط

---

[81] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/112 المقدمة من كينيا

[82] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/170 المقدمة من مكتب تنمية الاتصالات وعرض الجلسة الإعلامية للجنة الدراسات 2 لقطاع تنمية الاتصالات SG2_2023_05 من مكتب تنمية الاتصالات

[83] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/201 المقدمة من مكتب تنمية الاتصالات

[84] لمزيد من التفاصيل عن برنامج الاتحاد الدولي للاتصالات المتعلق بأفرقة الاستجابة للحوادث السيبرانية: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

لتحديد الثغرات التي يمكن أن يستغلها المتسللون. ومن خلال نشر المعلومات المتعلقة بالثغرات والتهديدات، يُسهم فريق الاستجابة لحالات الطوارئ الحاسوبية الوطني في تحصين أنظمة البنية التحتية الحرجة ضد الهجمات السيبرانية المحتملة، بما يضمن حماية استباقية في مختلف القطاعات الرئيسية.[85]

وأنشأت **البرازيل** العديد من المنظمات الشاملة لضمان بقاء البنية التحتية الحرجة مستجيبة ومحمية وأنها تطبق الإجراءات اللازمة للأمن السيبراني. وفي البرازيل، يتولى فريقان مسؤوليات الاستجابة للطوارئ الحاسوبية هما: الفريق الوطني البرازيلي للاستجابة للطوارئ الحاسوبية (CERT.br) ومركز الوقاية والعلاج والاستجابة للحوادث السيبرانية الحكومية (CTIR Gov). وهناك أيضاً عدد من أفرقة الاستجابة للطوارئ الحاسوبية القطاعية، بالإضافة إلى الشبكة الفيدرالية لإدارة الحوادث السيبرانية (ReGIC) المنشأة في عام 2021، التي ينسقها مركز الوقاية والعلاج والاستجابة للحوادث السيبرانية الحكومية.[86]

ومن الأمثلة على الأفرقة CIRT القطاعية مركز الاستجابة للحوادث الأمنية (CAIS) التابع للشبكة الوطنية للتعليم والبحوث (RNP). فمنذ إنشائه في عام 1997، كان المركز CAIS هو الفريق CIRT الأساسي للشبكة الأكاديمية البرازيلية. والمركز CAIS الذي يعمل بموجب المبادئ التوجيهية بشأن طلب تعليقات (RFC) رقم 2350، تم تكليفه بالكشف عن الحوادث الأمنية والاستجابة لها ومنعها داخل الشبكة الأكاديمية في البرازيل. وبالرغم من أن المركز CAIS ليس لديه سلطة مباشرة على المؤسسات في القطاع الأكاديمي، فإن له دوراً تنسيقياً رئيسياً في التعامل مع الحوادث. وتبرز أنشطة المركز CAIS الحاجة المتزايدة للتعاون داخل قطاعات محددة لإدارة مخاطر الأمن السيبراني بشكل فعال. وتقدم حالة المركز CAIS مثالاً على فريق CIRT قطاعي محدد يضمن حماية البنية التحتية الحرجة.[87]

وكجزء من جهد آخر حديث في البرازيل لدعم الأمن السيبراني الوطني، تعزز الشبكة ReGIC، وهي إطار الاستجابة للحوادث السيبرانية الفيدرالي في البرازيل، التنسيق بين كيانات الحكومة الفيدرالية لحماية البنية التحتية الحرجة

وتحدد الشبكة ReGIC ولايات وتوقعات الوكالات الفيدرالية. وفي إطار الشبكة ReGIC، فإن الوكالات الفيدرالية ملزمة بالمشاركة في الشبكة، والتي تتضمن تدابير لتبادل معلومات التهديدات، وإنذارات بالهجمات السيبرانية، والتنسيق أثناء الحوادث النشطة. ومن الأدوار المحددة الأخرى للشبكة ReGIC ولايتها بالتنسيق بين القطاعات، حيث يُطلب من الهيئات التنظيمية، مثل الوكالة الوطنية للاتصالات (Anatel)، إنشاء أفرقة قطاعية للاستجابة لحوادث الأمن السيبراني (CSIRT) وتقديم تقارير عن قطاعاتها.

وكان إنشاء أفرقة استجابة للطوارئ الحاسوبية (CERT) مخصصة لقطاعات محددة، بالإضافة إلى إنشاء فريق وطني للاستجابة للطوارئ الحاسوبية (CERT) هو النهج الذي اتبعته أيضاً **تنزانيا**[88]، حيث أنشأت الفريق TZ-Fincert للمؤسسات المالية والمصرفية، والفريق CERT للمؤسسات الأكاديمية، وeGSoC للوزارات والإدارات والوكالات والسلطات الحكومية. وأتاحت هذه التطورات زيادة فعالية الاستجابة للتهديدات، مما أسفر عن تعزيز الحماية، وتحسين الاستجابة الشاملة للحوادث، وتحسين التنسيق بشأن المسائل المتعلقة بقطاعات محددة

وللأفرقة CIRT دور لا غنى عنه في حماية بنيتها التحتية الحرجة من التهديدات السيبرانية. ومن خلال تنسيق إدارة الحوادث، وتبادل معلومات التهديدات، وإجراء تقييمات للثغرات، وتقديم مبادئ توجيهية مُخصصة، تزيد الأفرقة CIRT امن الصمود السيبراني للأنظمة الحرجة، بما يضمن التعافي السريع والحد من تأثير الهجمات السيبرانية. وتُسلط الأمثلة المذكورة في هذا الفصل الضوء على أهمية الاستجابات الخاصة بكل قطاع، والتعاون بين كيانات القطاعين العام والخاص، والحاجة إلى جهود مستمرة لتعزيز الصمود لحماية البنية التحتية الوطنية من التهديدات السيبرانية المعقدة. ولضمان تطبيق الأفرقة CIRT الوطنية للممارسات الجيدة في التصدي لحوادث الأمن السيبراني، وتعزيز التعاون التقني بين هذه الأفرقة، ينظم **الاتحاد** تدريبات سيبرانية[89] على المستوى الإقليمي وداخل المناطق. ومن خلال تمارين الأمن السيبراني، تبني الدول الأعضاء في الاتحاد قدراتها على تعزيز الجاهزية والحماية وتحسين الاستجابة للحوادث.

---

85 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/322 المقدمة من NRD Cyber Security
86 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/182 المقدمة من البرازيل
87 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/183 المقدمة من البرازيل
88 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/346 المقدمة من تنزانيا
89 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx

3.3 ما وراء الأساسيات: التنسيق من أجل النجاح عبر الحدود

مع إنشاء البلدان الأفرقة CIRT الخاصة بها وتعميق ثقافة الأمن السيبراني لديها، توجد خطوات ونماذج تُمكّن من تنسيق حماية البنية التحتية الحرجة بما يتجاوز الأساسيات. بمجرد أن يُنشئ بلد ما فريقاً قوياً للاستجابة لحالات الطوارئ الحاسوبية وبرامج وسياسات محلية للتعامل مع الحوادث، من الضروري النظر لما هو أبعد من الحدود الوطنية والانخراط في تنسيق دولي لمنع الحوادث السيبرانية والاستجابة لها والتخفيف من حدتها. وفي عالمنا المترابط اليوم، غالباً ما تتجاوز التهديدات السيبرانية الحدود، مما يتطلب استراتيجيات تعاونية لتعزيز صمود الأمن السيبراني العالمي. وقد طورت كل من الولايات المتحدة والاتحاد الأوروبي نماذج ناجحة للتعاون الدولي تُظهر أهمية هذه الجهود، بما في ذلك بناء العلاقات على الصعيدين المحلي والدولي.

ففي **الولايات المتحدة**، نفذت وكالة الأمن السيبراني وأمن البنية التحتية (CISA) برنامج الإخطار المسبق ببرمجيات طلب الفدية، وهو مبادرة استشرافية مصممة لتحديد تهديدات برمجيات طلب الفدية والاستجابة لها قبل أن تُسبب ضرراً. ويُجسد هذا البرنامج الأمن السيبراني الاستباقي من خلال الإنذارات المبكرة، التي تهدف إلى مساعدة المنظمات على تجنب فقدان البيانات الحرجة، والانقطاعات التشغيلية، والآثار المالية الناجمة عن هجمات برمجيات طلب الفدية. ويعتمد البرنامج على ركيزتين أساسيتين: الشراكات القوية والجمع المنهجي للمعلومات القابلة للتنفيذ.[90]

ولهيئة التعاون المشترك للدفاع السيبراني (JCDC) التابعة لوكالة CISA دور محوري من خلال تصفية المعلومات الواردة من مجتمع أبحاث الأمن السيبراني، ومقدمي خدمات البنى التحتية، ومنظمات معلومات التهديدات. كما تضمن العلاقات القوية مع كيانات القطاع الخاص وباحثيه تقديم معلومات عالية الجودة في الوقت المناسب. وبمجرد تلقي بلاغ موثوق، تسخر الهيئة JCDC موظفيها الوطنيين والميدانيين لإخطار المنظمات المتضررة وتقديم إرشادات التخفيف.

ويُعدّ امتداد البرنامج الدولي، من خلال التنسيق الوثيق مع الأفرقة CIRT الأجنبية، جزءاً هاماً من هذا البرنامج. فعندما تتعلق البلاغات عن التهديد بمنظمة خارج الولايات المتحدة، تعمل الهيئة JCDC مع نظيراتها الدولية لضمان إنذار الجهة المتضررة فوراً. وتُعدّ هذه العلاقات بين الأفرقة CIRT أمراً بالغ الأهمية، لا سيما عند الحاجة إلى اتخاذ إجراءات سريعة لمنع انتشار برمجيات طلب الفدية. وفي الحالات التي يكون قد تم فيها بالفعل نشر برمجيات طلب الفدية، تدعم الهيئة JCDC المنظمات المتضررة من خلال توفير رؤى حول تكتيكات وتقنيات وإجراءات الجهات القائمة بالتهديد، والمساعدة في جهود التحقيق والمعالجة. وغالباً ما يشمل هذا الدعم تحديد البيانات المسربة وتقديم إرشادات للتخفيف من الآثار طويلة الأجل للهجوم.

وقد أولى **الاتحاد الأوروبي**، على نحو مماثل، أولويةً للتنسيق الدولي لتعزيز صموده السيبراني. ومن أبرز الأمثلة على ذلك مشروع أفرقة الاستجابة السيبرانية السريعة والمساعدة المتبادلة في مجال الأمن السيبراني (CRRT) التابع لمنظمة PESCO.[91] ويُمكّن هذا البرنامج من النشر السريع لخبراء الأمن السيبراني في جميع أنحاء الدول الأعضاء في الاتحاد الأوروبي للاستجابة للحوادث واسعة النطاق، لا سيما تلك التي تستهدف البنية التحتية الحرجة. ومن خلال تجميع الخبرات والموارد، يُعزز الاتحاد الأوروبي قدرته الجماعية على مواجهة الأزمات السيبرانية على المستويين الوطني والإقليمي. كما تُعدّ هذه المبادرة دليلاً على التزام الاتحاد الأوروبي بالأمن السيبراني التعاوني، إذ تضمن قدرة الدول الأعضاء على تقديم الدعم المتبادل في حالات الطوارئ.

وإلى جانب هذه المبادرات، تُشدد كلٌّ من الولايات المتحدة والاتحاد الأوروبي على أهمية تبادل المعلومات المتعلقة بالتهديدات، وتعزيز الثقة، ووضع بروتوكولات موحدة للتنسيق عبر الحدود.

ومع استمرار تطور التهديدات السيبرانية من حيث التعقيد والنطاق، يُصبح التنسيق عبر الحدود عنصراً حاسماً للنجاح. وتُبيّن النماذج المذكورة أعلاه كيف يُمكن للتعاون الدولي أن يُعزز من قدرات الاستجابة للحوادث، ويُعزز الحماية السيبرانية العالمية. ومن خلال إعطاء الأولوية للتعاون والاستفادة من خبرات الشركاء العالميين، يُمكن للبلدان مُواجهة تحديات المشهد الرقمي المُتزايد الترابط بشكل أفضل.

---

[90] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/164 المقدمة من الولايات المتحدة

[91] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/322 المقدمة من NRD Cyber Security؛
https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

4.3 إنشاء مراكز التنسيق

أنشأت كل من أستراليا والاتحاد الروسي مراكز تنسيق وطنية، واختبرت فوائد نماذج كل منها. وبالنسبة للحكومتين، تُعدّ مراكز التنسيق الوطنية جزءاً من استجابة أوسع شاملة للحكومة ككل للحوادث السيبرانية. ولا تُعدّ مراكز التنسيق أفرقة للاستجابة للطوارئ الحاسوبية، بل تعمل جنباً إلى جنب مع هذه الأفرقة.

وقد أنشأت حكومة **أستراليا** وحدة تنسيق للاستجابة للأمن السيبراني (CSRCU) تابعة لوزارة الشؤون الداخلية في أعقاب انتهاكات بيانات كل من Optus وMedibank عام 2022. وكان الهدف هو إنشاء تنسيق مركزي للحوادث السيبرانية ذات الأهمية الوطنية.[92] أما **الاتحاد الروسي**، فقد أنشأ مركزه الوطني للاستجابة والتنسيق للحوادث الحاسوبية (NCIRCC) بموجب قانون وطني لتعزيز البنية التحتية للمعلومات الحرجة. ويؤدي هذان المركزان مهاماً متشابهة: تنسيق الاستجابة للحوادث وتوصيل المعلومات الحرجة. ويركز مركز NCIRCC على تنسيق تدابير الاستجابة للحوادث السيبرانية، وعلى التواصل مع البنية التحتية الحرجة بشأن الوسائل والأساليب المتعلقة بجمع البيانات عن مثل هذه الحوادث وتخزينها وتحليلها.[93] ويتمتع كل من مركز CSRCU في أستراليا ومركز NCIRCC بالصلاحية لتشكيل أفرقة عمل، وإشراك المنظمات المعنية والخبراء المعنيين، ونشر المعلومات والمواد المرجعية.

[92] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/218 المقدمة من أستراليا
[93] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/79 المقدمة من الاتحاد الروسي

الفصل الرابع - النُهج والممارسات الجيدة وجمع معلومات عن تجارب تنفيذ الاستراتيجيات والسياسات الوطنية المتعلقة بالأمن السيبراني

مع تزايد الاعتماد العالمي على التكنولوجيات الرقمية، لا يمكن أن يكون من باب المبالغة الإقرار بأهمية وضع استراتيجيات وسياسات وطنية فعّالة للأمن السيبراني. وتتطور التهديدات السيبرانية بسرعة، وتستهدف البلدان المتقدمة والنامية على حد سواء. ولحماية البنية التحتية الحرجة والاقتصاد الرقمي وخصوصية المواطنين، يجب أن تعتمد البلدان استراتيجيات شاملة ومتكيّفة للأمن السيبراني. ويستكشف هذا الفصل مختلف النُهُج والممارسات الجيدة التي تتبعها مختلف البلدان لبناء أطر مرنة للأمن السيبراني. ومن خلال تحليل تجارب مختلف البلدان، يهدف هذا الفصل إلى تقديم خارطة طريق لتصميم وتنفيذ سياسات واستراتيجيات الأمن السيبراني الوطنية.

تشمل سياسات واستراتيجيات الأمن السيبراني الوطنية طيفاً واسعاً من الممارسات، كل منها مصمم خصيصاً للسياقات السياسية والاجتماعية والاقتصادية والقانونية والتكنولوجية المتميزة لمختلف البلدان. ويتميز تنفيذ هذه السياسات والاستراتيجيات بمجموعة فريدة من التحديات والفرص، والتي تتأثر بشكل كبير بالظروف الخاصة بكل بلد. ويخوض هذا الفصل في التجارب العملية لمختلف البلدان، مسلطاً الضوء على التحديات والنجاحات التي واجهتها في عملها من أجل تعزيز حمايتها الرقمية وقدرتها على الصمود في مواجهة التهديدات المتطورة.

ويمتد النقاش عبر مجالات حيوية مثل التوافق الاستراتيجي، وإشراك أصحاب المصلحة، وبناء القدرات، والتكيف المستمر مع مشهد التهديدات السيبرانية الديناميكي. ولا يهدف هذا الاستكشاف الشامل إلى توضيح التعقيدات التي تنطوي عليها حماية المصالح الوطنية بفعالية في المجال السيبراني الذي يشهد تنافساً متزايداً فحسب، بل يهدف أيضاً إلى تقديم رؤى استراتيجية يمكن أن توجه واضعي السياسات والمتخصصين في الأمن السيبراني في تعزيز استراتيجياتهم الخاصة.

1.4 المواءمة الاستراتيجية والقيادية وإطار السياسات

يعتمد نجاح تنفيذ استراتيجيات الأمن السيبراني الوطنية بشكل حاسم على توافق هذه الاستراتيجيات مع التحول الرقمي الأوسع، والأمن الوطني، والسياسات الاقتصادية. ويضمن هذا التوافق أن تكون مبادرات الأمن السيبراني داعمةً ومتكاملةً أيضاً للأهداف العامة للبلد وأطر الحوكمة. فعلى سبيل المثال، قامت **جمهورية إستونيا**، المعروفة على نطاق واسع بمجتمعها الرقمي المتقدم، بمواءمة استراتيجيتها للأمن السيبراني بفعالية مع أهدافها في الحوكمة الإلكترونية والاقتصاد الرقمي، مما أدى إلى إنشاء بنية تحتية رقمية قادرة على الصمود تدعم مبادرات القطاعين العام والخاص.[94] ويُسهل هذا التوافق الاستراتيجي في إستونيا من خلال التحديثات المنتظمة لاستراتيجيتها للأمن السيبراني، والتي تتم مزامنتها مع التغيرات في البيئة التكنولوجية والجيوسياسية الأوسع.

إضافةً إلى هذه الرؤى، تتطلب سياسات واستراتيجيات الأمن السيبراني الفعّالة توافقها مع السياسات والأهداف الاقتصادية الوطنية الأوسع. ويضمن هذا التوافق ألا تعالج تدابير الأمن السيبراني التهديدات المباشرة فحسب، بل تدعم أيضاً المصالح الوطنية طويلة الأجل، مما يُهيئ بيئة رقمية آمنة وقادرة على الصمود تُشجع على النمو والابتكار. ويُعدّ هذا التوافق الاستراتيجي ضروري لفعالية تدابير الأمن السيبراني، ويدعم الأهداف الوطنية الأوسع، ويعزز قدرة البلد على منع الحوادث السيبرانية ومعالجتها والاستجابة لها، مع دعم نمو قطاع الأمن السيبراني المحلي.

[94] https://www.weforum.org/stories/2020/07/estonia-advanced-digital-society-here-s-how-that-helped-it-during-covid-19/

تُقدم **جمهورية تيمور-ليشتي الديمقراطية**[95] مثالاً واضحاً على أهمية التركيز على الأمن السيبراني في سياق سياسات واستراتيجيات وخطط وخارطة طريق التحول الرقمي. وأدركت تيمور-ليشتي أنه مع التحول الرقمي، يجب إدارة مخاطر الأمن السيبراني لمنع الهجمات السيبرانية وانتهاكات البيانات. ومن هذا المنطلق، تحتاج أقل البلدان نمواً (LDC) إلى إعطاء الأولوية للأمن السيبراني كركيزة أساسية، مما يعكس فهماً للدور الحاسم للأمن السيبراني في التحول الرقمي ومن ثم التحول الرقمي نفسه في التنمية الوطنية.

ويُعد ضمان وجود قيادة قوية ومتوافقة داخل المنظمات المسؤولة عن التنسيق السيبراني الوطني، كجزء لا يتجزأ من مجتمع الأمن السيبراني الحكومي الأوسع، عنصراً مهماً آخر للنهوض بالأمن السيبراني. ويمكن للمنسق المعيّن تسهيل وقيادة استجابة في إطار الحكومة ككل. وفي هذا الصدد، يتضمن نموذج **أستراليا** منسقاً وطنياً للأمن السيبراني، تتمثل وظيفته الرئيسية في قيادة إدارة الأحداث السيبرانية الوطنية. وقد تم إنشاء منصب المنسق هذا في فبراير 2023، ويرفع الشخص المعيّن تقاريره إلى وزير الأمن السيبراني.[96] وفي مايو 2022، أصدر رئيس **الاتحاد الروسي** مرسوماً يحدد معايير صارمة لتعيين المسؤولين عن أمن المعلومات، مع التركيز على شروط الكفاءة، بما في ذلك التعليم والخبرة في هذا المجال، بالإضافة إلى المتطلبات التنظيمية. كما يشجع المرسوم إعادة التدريب المهني للأفراد الذين يفتقرون إلى خلفية متخصصة في أمن المعلومات.[97]

2.4 الأطر القانونية والإدارة

تُجسّد **جمهورية إفريقيا الوسطى**[98] و**جمهورية الكونغو الديمقراطية**[99] كيف يُمكن للإجراءات التشريعية وأطر الحوكمة المُصمّمة خصيصاً أن تُعزّز قدرات الأمن السيبراني بشكل كبير. ففي جمهورية إفريقيا الوسطى، شرعت الحكومة في إصلاحات قانونية وأنشأت هيئات مُخصّصة للأمن السيبراني لإنفاذ سياساتها، معلنة عن نهج استباقي لتعزيز الدفاعات الرقمية. وبالمثل، اعتمدت جمهورية الكونغو الديمقراطية ميثاقاً شاملاً قائماً على الممارسات الجيدة الدولية، يشمل التشريعات السياساتية، والتعاون متعدد المستويات، وحملات التوعية العامة المُكثّفة. وتُعدّ هذه التدابير بالغة الأهمية للبلدان، وخاصةً في المناطق النامية، لتأمين فضاءاتها السيبرانية من التهديدات المُتزايدة.

وتُضيف **جمهورية ألبانيا**[100] بُعداً جديداً إلى هذه الرؤية من خلال إصلاحاتها الشاملة الأخيرة في مجال الأمن السيبراني. ويعكس إنشاء فريق CSIRT وطني وإعادة هيكلة هيئته المعنية بالأمن السيبراني التزام ألبانيا بإجراء توافق لإطار عملها للأمن السيبراني مع المعايير الدولية والممارسات الجيدة. وتهدف هذه الخطوات الاستراتيجية إلى تعزيز البنية التحتية الوطنية للأمن السيبراني في ألبانيا من خلال ضمان تحقيق استجابة منسقة للحوادث السيبرانية وتعزيز حوكمة جهود الأمن السيبراني. كما تهدف الإصلاحات القانونية في ألبانيا إلى تحديث وتعزيز الإطار التشريعي الحالي، بما يضمن مواجهته لتحديات وتهديدات الأمن السيبراني الحالية. ويُعدّ هذا التوافق بين العناصر القانونية والمؤسسية والتشغيلية في استراتيجية الأمن السيبراني في ألبانيا نموذجاً يُحتذى به للدول الأخرى التي تسعى إلى تعزيز دفاعاتها في مجال الأمن السيبراني من خلال إصلاحات شاملة للحوكمة.

وتسعى **كوت ديفوار** أيضاً إلى إجراء مجموعة من التحديثات التشريعية في إطار هدفها السياساتي المتمثل في إرساء الثقة الرقمية بحلول عام 2025.[101] ومن أبرز الجهود المبذولة تعزيز الهياكل القانونية لدعم إقامة مجتمع معلومات موثوق، بما يتماشى مع المعايير الإقليمية، مثل معايير الجماعة الاقتصادية لدول غرب أفريقيا واتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية. وتلعب هيئة تنظيم الاتصالات/تكنولوجيا المعلومات والاتصالات في كوت ديفوار (ARTCI) دوراً محورياً، مع تركيز خاص على الثقة الرقمية وأمن الشبكات، وحماية البيانات الشخصية، وإدارة المعاملات الإلكترونية. ويؤكد إنشاء لجان استشارية، مثل اللجنة الاستشارية للثقة الرقمية واللجنة الاستشارية لحماية البيانات الشخصية، على مدى الالتزام العميق بتعزيز بيئة سيبرانية آمنة. وتهدف هذه الجهود المنظمة إلى بناء فضاء رقمي موثوق، وتعزيز أمن البنية التحتية الرقمية لكوت ديفوار، وتعزيز ثقة الجمهور في الاقتصاد الرقمي.

---

95 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/120 المقدمة من تيمور-ليشتي
96 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/218 المقدمة من أستراليا
97 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/79 المقدمة من الاتحاد الروسي
98 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/141 المقدمة من جمهورية إفريقيا الوسطى
99 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/115 المقدمة من جمهورية الكونغو الديمقراطية
100 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/309 المقدمة من ألبانيا
101 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/29 المقدمة من كوت ديفوار

وتوضح هذه الأمثلة أهمية توافق استراتيجيات الأمن السيبراني مع أطر الحوكمة الوطنية، وهو ما لا يعزز فعالية هذه الاستراتيجيات فحسب، بل يضمن أيضاً استدامتها وقدرتها على التكيف في مواجهة التهديدات السيبرانية المتطورة.

3.4 التعاون والدعم الدوليان

للمنظمات الدولية دور بالغ الأهمية في دعم الجهود الوطنية للأمن السيبراني، كما يتضح من عدد من مبادرات **البنك الدولي**.[102] ويُساعد البنك الدولي البلدان المتعاملة معه، وخاصةً تلك المُصنَّفة ضمن أقل البلدان نمواً، من خلال تقديم الدعم المالي والتقني على حد سواء من أجل بناء أسس رقمية متينة وتسريع وتيرة الاستخدام الرقمي في مختلف القطاعات. ويُعدُّ هذا الدعم حيوياً لهذه البلدان لتحقيق التوافق لسياساتها واستراتيجياتها للأمن السيبراني مع التطورات العالمية، بما يضمن صمودها في مواجهة التهديدات السيبرانية الحالية والناشئة

وتُسلّط جهود البنك الدولي الضوء على الأثر الكبير للشراكات العالمية وتبادل الخبرات في تعزيز أطر الأمن السيبراني الوطنية. ومن خلال تسهيل دمج أحدث التكنولوجيات والممارسات الجيدة، يُساعد البنك الدولي البلدان ليس فقط في التصدي للتهديدات السيبرانية، بل أيضاً في الاستفادة من التحوّل الرقمي لتحقيق النمو الاقتصادي والاجتماعي.

وفي **جمهورية هايتي**،[103] تُقدم الشراكات الدولية، لا سيما مع البنك الدولي ومصرف التنمية للبلدان الأمريكية، دعماً مالياً وتقنياً بالغ الأهمية. ويُعد هذا الدعم أساسياً لتطوير بنى تحتية رقمية متينة وتعزيز تدابير الأمن السيبراني في جميع أنحاء البلاد.

ومن المبادرات الرئيسية في هذا الصدد، فريق العمل المشترك الذي شكله المجلس الوطني للاتصالات في هايتي (CONATEL) ومعهد هايتي للإحصاء والمعلوماتية (IHSI). ويُكلَّف فريق العمل المشترك هذا بوضع استراتيجية وطنية منسقة للأمن السيبراني، تُركِّز على حماية البنى التحتية الحرجة ومكافحة الجرائم السيبرانية. ويضمن الدور التنظيمي لكوناتيل الامتثال لبروتوكولات الأمن، بينما يُدير معهد IHSI تهديدات ومخاطر الأمن السيبراني، بما يُعزز الأمن العام للأنظمة الرقمية في هايتي.

وتدعم هذه الجهود مشاريع دولية مثل مشروع تسريع التحول الرقمي في هايتي، الذي يهدف إلى تحسين توصيلية النطاق العريض وتعزيز الصمود الرقمي. ولا يقتصر هذا النهج الشامل على حماية هايتي من التهديدات السيبرانية الناشئة فحسب، بل يدعم أيضاً نموها الاجتماعي والاقتصادي في العصر الرقمي. وتعزيزاً لهذه الجهود، أجرت هايتي تقييماً شاملاً لمدى اكتمال الأمن السيبراني بالتعاون مع المركز العالمي لقدرات الأمن السيبراني والبنك الدولي. وشمل هذا التقييم أصحاب مصلحة مختلفين، مع استخدم نموذج اكتمال قدرات الأمن السيبراني للدول لتحديد المجالات الحيوية التي تحتاج إلى استثمارات استراتيجية. وقد وجهت النتائج إلى إجراء تحسينات مستهدفة لتعزيز البنية التحتية للأمن السيبراني في هايتي.

4.4 الأطر التعاونية ومشاركة أصحاب المصلحة

نفذت **البرازيل**[104] سلسلة من التدابير الاستراتيجية الرامية إلى تعزيز بنيتها التحتية الوطنية للأمن السيبراني من خلال مشاركة فعالة وشاملة لأصحاب المصلحة. ويؤكد النهج المتبع في البلاد على أهمية التعاون بين الهيئات الحكومية وكيانات القطاع الخاص والمؤسسات الأكاديمية. وتُسهل هذه المشاركة لأصحاب المصلحة المتعددين من خلال مبادرات وشراكات مختلفة تستفيد من نقاط القوة الفريدة والرؤى المتفردة لكل قطاع لتعزيز المشهد العام للأمن السيبراني. ومن التطورات الأخيرة إنشاء اللجنة الوطنية للأمن السيبراني بغية مراقبة تنفيذ وتطوير السياسات الوطنية للأمن السيبراني. وتضم اللجنة 25 عضواً، حيث يمثل 15 عضواً كيانات وهيئات الإدارة العامة الفيدرالية، بما في ذلك Anatel، ويمثل 10 أعضاء منظمات أخرى مثل لجنة توجيه الإنترنت البرازيلية (CGI.br)، في حين خصصت 3 مقاعد لتمثيل المجتمع المدني، و3 مقاعد للهيئات الأكاديمية، و3 مقاعد لكيانات القطاع الخاص ذات الصلة بالأمن السيبراني.

اتخذت **أستراليا** خطوات تتجاوز إنشاء فريق الاستجابة للطوارئ الحاسوبية لضمان حماية البنية التحتية الحرجة وقدرتها على الصمود، وهي خطوة أكثر تقدماً في تطوير الأمن السيبراني. فبدلاً من مجرد الاستجابة والحماية،

[102] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/74 المقدمة من البنك الدولي
[103] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/121 المقدمة من هايتي
[104] وثيقتا لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/57 وSG2RGQ/181 المقدمتان من البرازيل

صُمم برنامج تعزيز البنية التحتية الحرجة (CI-UP) لمساعدة مؤسسات البنية التحتية الحرجة الأسترالية على تحسين قدرتها على الصمود في مواجهة الهجمات السيبرانية المعقدة. ويعمل البرنامج، الذي تديره حكومة أستراليا، جنباً إلى جنب مع مؤسسات البنية التحتية الحرجة في القطاع الخاص لتعزيز قدرتها على مواجهة مسارات الهجمات التي تستهدف أصول البنية التحتية الحرجة وبيئات التكنولوجيا التشغيلية. ويعمل البرنامج CI-UP كبرنامج طوعي على مستوى البلاد، موجه نحو التعاطي مع التهديدات.[105]

وينصب التركيز الأساسي للبرنامج CI-UP على مساعدة مؤسسات البنية التحتية الحرجة على تحسين مستوى الأمن السيبراني لديها في عدة مجالات رئيسية:

- تعزيز الرؤية والوعي: يساعد برنامج CI-UP الكيانات على تحقيق رؤية أفضل للحوادث السيبرانية وزيادة الوعي بالثغرات المحتملة في أنظمتها.
- احتواء الحوادث والاستجابة لها: يعزز البرنامج قدرة مؤسسات البنية التحتية الحرجة على احتواء الحوادث السيبرانية والاستجابة لها بفعالية.
- تعزيز ثقافة الأمن السيبراني: يشجع برنامج CI-UP أيضاً على تطوير ثقافة واعية بالأمن السيبراني في جميع قطاعات البنية التحتية الحرجة في أستراليا.

ويعكس هذا البرنامج أهمية التعاون بين الحكومات والقطاع الخاص ضمن إطار تعدد أصحاب المصلحة من أجل تعزيز الأمن. ويقدم برنامج CI-UP هذه الخدمات من خلال مجموعة متنوعة من أنشطة التفاعل، بما في ذلك العروض التقديمية وورش العمل وتبادل المعلومات وتقديم مبادئ توجيهية مفصلة للتخفيف من آثار المخاطر. كما يعمل البرنامج في الموقع مع موظفي أهم كيانات البنية التحتية الحرجة في أستراليا، مقدماً استشارات متخصصة ومتعمقة مصممة خصيصاً لتلبية الاحتياجات المحددة لكل مؤسسة.

يُعدّ إشراك مجموعة واسعة من أصحاب المصلحة أمراً بالغ الأهمية للتنفيذ الفعال لسياسات واستراتيجيات الأمن السيبراني الوطنية. ويشمل هذا التعاون الوكالات الحكومية، ومؤسسات القطاع الخاص، والهيئات الأكاديمية، والمجتمع المدني، حيث يُقدّم كلٌّ منها وجهات نظره واحتياجاته وأولوياته وخبراته المتفردة. ويُساعد هذا التعاون في وضع السياسات الوطنية ومراجعتها وتحسينها وصقلها، ويضمن أن تكون الاستراتيجيات المُنفّذة عمليةً وتعكس احتياجات وواقع جميع القطاعات.

5.4 تنمية البنية التحتية للأمن السيبراني

شرعت **جمهورية الكونغو الديمقراطية** [106] في تنفيذ خطة طموحة لإصلاح وتحديث بنيتها التحتية الرقمية. وتنبع هذه المبادرة من إدراكها أن الأنظمة الرقمية القوية والآمنة هي ركيزة الأمن السيبراني الفعال، وأنها ضرورية للتنمية الوطنية. وقد أولت الحكومة الأولوية لتحديث البنية التحتية للشبكات الحرجة، ليس فقط لمواجهة طيف التهديدات السيبرانية المتزايد، بل أيضاً لدعم المتطلبات الرقمية لاقتصادها المتنامي. وتتضمن استراتيجية جمهورية الكونغو الديمقراطية نشر تكنولوجيات الأمن السيبراني المتقدمة، مثل جدران الحماية المتطورة، وأنظمة كشف الاقتحام، وأساليب تشفير البيانات الشاملة. وتُعد هذه التكنولوجيات بالغة الأهمية للحماية من النفاذ غير المصرح به وحماية المعلومات الحساسة. بالإضافة إلى ذلك، تعمل جمهورية الكونغو الديمقراطية على توسيع نطاق النفاذ إلى النطاق العريض فيها، وهو أمر حيوي لضمان وصول تدابير الأمن السيبراني إلى جميع أنحاء البلاد، بما في ذلك المناطق النائية وشحيحة الخدمات.

وتُطوّر **جمهورية بوروندي** [107] بنيتها التحتية للأمن السيبراني كجزء أساسي من استراتيجيتها الوطنية المستقبلية للأمن السيبراني. وتلتزم الحكومة بتحقيق التحول الرقمي ورقمنة الخدمات، مُدركةً الأهمية الحيوية لتكنولوجيا المعلومات والاتصالات في التنمية. واستجابةً لتصاعد التهديدات السيبرانية، أنشأت بوروندي، من خلال وزارة تكنولوجيا المعلومات والاتصالات، لجنةً لوضع استراتيجية وطنية شاملة للأمن السيبراني، تشمل تعزيز الأطر القانونية لتنظيم الأمن السيبراني، ونشر ثقافة الأمن السيبراني، وبناء المعرفة التقنية، والمشاركة في الجهود الإقليمية والدولية، ورفع مستوى الوعي بتهديدات الأمن السيبراني في مختلف القطاعات. ويُنفّذ هذا التطوير للبنية التحتية من خلال آليات لحماية البيانات وأمنها، بما يضمن النزاهة والثقة بين المستعملين وموردي الخدمات.

---

105 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/214 المقدمة من أستراليا
106 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/104 المقدمة من جمهورية الكونغو الديمقراطية
107 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/134 المقدمة من بوروندي

6.4 بناء القدرات

يتضمن بناء القدرات اللازمة لتنفيذ استراتيجيات الأمن السيبراني الوطنية تعزيز مهارات متخصصي الأمن السيبراني، وإنشاء بنى تحتية تكنولوجية، ووضع أطر قانونية وتنظيمية. ويُعد الاستثمار المستمر في التدريب وبناء القدرات أمراً بالغ الأهمية للحفاظ على الأمن السيبراني الوطني. وكما هو موضح في الفصل الأول، فإن التطوير المستمر لمهارات متخصصي الأمن السيبراني وتثقيف الجمهور يُمكّن الدول من إدارة الحوادث السيبرانية والاستجابة لها بشكل أفضل، مع دعم الأهداف الأوسع للتنمية الاقتصادية والاجتماعية من خلال تعزيز حرفية تكنولوجيا المعلومات والاتصالات.

7.4 التكيف المتواصل مع مشهد التهديدات السيبرانية

تتطلب الطبيعة الدينامية لمشهد التهديدات السيبرانية أن تكون سياسات واستراتيجيات الأمن السيبراني الوطنية، كما ينبغي أن تكون أي تشريعات أو لوائح أخرى خاصة بالأمن السيبراني، قابلة للتكيف بطبيعتها. وتُعدّ المراقبة المستمرة للمشهد المتطور، بما في ذلك التحديات التي تفرضها التكنولوجيات الجديدة والناشئة، بالإضافة إلى تقييم فعالية السياسات والاستراتيجيات والتحديث المنتظم لممارسات الأمن السيبراني، عناصر أساسية لهذه القدرة على التكيف في مجال الأمن السيبراني. ونوقشت ضرورة تكييف الأمن السيبراني في الفصل 2، عند تناول ممارسات ضمان الأمن السيبراني.

الفصل الخامس - التحديات والنُهج المتعلقة بالأمن السيبراني لتكنولوجيا الجيل الخامس (5G)

يمثل نشر تكنولوجيا الجيل الخامس تطوراً كبيراً في مجال الاتصالات، إذ أنها توفر سرعات أكبر وتوصيلية أفضل مع إمكانية تحسين الصناعات وتوسيع نطاق تطبيقات إنترنت الأشياء (IoT) وإدخال نُهج جديدة للاتصالات الرقمية. ومع ذلك، فإن المعمارية المتطورة التي تُمكّن هذه التطورات تجلب معها تحديات معقدة للأمن السيبراني تتطلب فهماً شاملاً وتدابير وقائية قوية.

ومع نشر شبكات الجيل الخامس على مستوى العالم، يعتبر إنشاء نظام إيكولوجي آمن ضرورياً لضمان سلامة المعلومات وتوافرها وسريتها، فضلاً عن حماية البنية التحتية التي أصبحت العمود الفقري للاقتصاد الرقمي.

ويعرض هذا الفصل مناقشات بشأن تعقيدات الأمن السيبراني لتكنولوجيا الجيل الخامس (5G) ويستهدف تبادل المعلومات بشأن الممارسات الحالية، واستكشاف حلول مبتكرة للتهديدات الناشئة، مع تبادل الأفكار والممارسات الجيدة للأمن السيبراني للشبكات الإلكترونية العامة من الجيل الخامس التي يمكن للدول الأعضاء في الاتحاد النظر فيها وتنفيذها في سياقاتها الوطنية.

1.5 لمحة عامة عن الأمن السيبراني لتكنولوجيا الجيل الخامس (5G)

تتسم تكنولوجيا الجيل الخامس بأنظمة برمجيات متقدمة تتيح التشكيل السهل والتوصيلية الضخمة للمشتركين والأجهزة. وتدعم تكنولوجيا الجيل الخامس التطبيقات المنخفضة الكمون، مثل الواقع المعزز والجراحة عن بُعد وخدمات الإنترنت المتكاملة، التي تعتمد على وجود شبكة قوية وموثوقة. وأحد حالات الاستخدام الأساسية لتكنولوجيا الجيل الخامس هي إنترنت الأشياء (IoT) التي تستفيد من قدرة الجيل الخامس على ربط عدد كبير من النقاط الطرفية. ومن المنتظر أن تُحدث تكنولوجيا الجيل الخامس ثورةً في التوصيلية، وهذا ما يمثل أيضاً مخاطر وتحديات جديدة وديناميةً للأمن السيبراني.

وبخلاف الأجيال السابقة من التكنولوجيات اللاسلكية، تقدم تكنولوجيا الجيل الخامس تحولاً كبيراً نحو المعمارية السحابية والشبكات المعرَّفة بالبرمجيات (SDN) والتمثيل الافتراضي لوظائف الشبكة (NFV). ويُنشئ هذا التحول مشهداً أكثر تعقيداً وديناميةً للأمن السيبراني.

ومع زيادة انتشار تكنولوجيا الجيل الخامس، من المتوقع أيضاً أن تصبح البنية التحتية للاتصالات هدفاً أكثر جاذبية للأنشطة السيبرانية الضارة، مما يستلزم تدابير أمنية متقدمة يمكنها التكيف مع التهديدات المتطورة. ويجب أن يركز الأمن السيبراني لتكنولوجيا الجيل الخامس على زيادة قدرة النظام الإيكولوجي بأكمله على الصمود، بما في ذلك البنية التحتية والتطبيقات. ويشمل ذلك حماية الأجهزة والبيانات والشبكات الموصولة ضد التهديدات السيبرانية.

وإقراراً بأن المنظمات المختلفة تستخدم تعاريف مختلفة للأمن السيبراني،[108] ينبغي أن يوضع في الاعتبار أن مصطلح "الأمن السيبراني لشبكات الجيل الخامس" في هذا التقرير يشير إلى الأمن السيبراني في سياق الجيل الخامس بمعلماته ومعاييره وسماته التكنولوجية الجديدة التي يتعين إدارتها بشكل صحيح لحماية النظام الإيكولوجي الرقمي بأكمله وضمان القدرة السيبرانية على الصمود.

[108] https://www.enisa.europa.eu/publications/definition-of-cybersecurity

الإطار 1: تعريف الأمن السيبراني

في الاتحاد، يعرَّف الأمن السيبراني في التوصية ITU-T X.1205 على أنه "*مجموع الأدوات والسياسات ومفاهيم الأمن وتحفظات الأمن والمبادئ التوجيهية ونُهج إدارة المخاطر والإجراءات والتدريب والممارسات الفضلى وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين. وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المرسَلة و/أو المحفوظة في البيئة السيبرانية. ويسعى الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسة والمستعملين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية. وتضم الأهداف العامة للأمن ما يلي:*

- *التيسر*
- *السلامة، التي قد تضم الاستيقان وعدم الرفض*
- *السرية.*"

2.5 نشر الشبكات القديمة

غالباً ما يقوم مقدمو خدمات الاتصالات مبدئياً بنشر شبكات الجيل الخامس على أساس أنها غير قائمة بذاتها (NSA)، بحيث يستفيدون من البنية التحتية الحالية لشبكة الجيل الرابع قبل نشر أي شبكة قائمة بذاتها (SA) من طرف إلى طرف.[109] وستَرِث شبكات الجيل الخامس غير القائمة بذاتها نقاط الضعف القديمة لشبكات الجيل الرابع أو حتى شبكات الجيلَ الثاني/الجيل الثالث، والتي يجب إدارتها وفقاً لذلك. وبالنسبة لبعض المشغلين، فإن ذلك بمثابة "ديون تقنية" حيث تعني إدارة الأنظمة القديمة الحاجة إلى وضع مجموعة من الضوابط الأمنية المقيَّسة لقياس الحالة الأمنية لمكونات البنية التحتية في مختلف مراحل نضجها الجيلي.[110]

ومن المهم التأكيد على أن شبكات الجيل الخامس القائمة بذاتها تقدم فرصاً لتحسين الأمن السيبراني مقارنةً بالأجيال السابقة من التكنولوجيات المتنقلة: فهي مصممة لتكون أكثر أمناً من شبكات الجيل الرابع. وقد لوحظت تحسينات في مجالات مثل أمن المشتركين وخصوصيتهم، وشبكة النفاذ الراديوي (RAN)، والشبكة الأساسية، وأمن التجوال.[111]، [112]

3.5 أنشطة المعايير في مجال أمن تكنولوجيا الجيل الخامس

1.3.5 منظمات وضع المعايير النشطة في مجال الأمن السيبراني لتكنولوجيا الجيل الخامس

نظراً لتعقيدات تكنولوجيا الجيل الخامس والقضايا المرتبطة بها، لا تتمتع منظمة واحدة لوضع المعايير (SDO) بولاية حصرية للاضطلاع بالعمل المتعلق بالأمن السيبراني لشبكات الجيل الخامس. وتجنباً لازدواجية العمل، أُنشئت آليات لتبادل المعلومات بين منظمات وضع المعايير وتنسيق المقترحات وبنود العمل.

وللمساعدة على ربط هذه الأنشطة المختلفة وإرشاد اتجاه أعمال تقييس الشؤون الأمنية المتعلقة بتكنولوجيا الجيل الخامس في قطاع تقييس الاتصالات **بالاتحاد** (ITU-T)، أعدت لجنة الدراسات 17 (SG17) تقريراً تقنياً لربط المعايير القائمة وتلك الجاري وضعها في منظمات وضع المعايير وتطبيقها في شبكات الجيل الخامس.[113]

---

[109] ستتصل الأجهزة بترددات الجيل الخامس لنقل البيانات عند الحاجة إلى نطاق ترددي أكبر وكمون أقصر (مثل الاتصال بين السيارات الذكية)، أو لتقليل استهلاك الطاقة على الأجهزة التي تدعم إنترنت الأشياء، ولكنها ستظل تعتمد على شبكات الجيل الرابع وحتى الجيل الثاني والثالث للمكالمات الصوتية والرسائل النصية القصيرة. المصدر: https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf

[110] https://www.itu.int/md/D22-SG02.RGQ-ADM-0019 و https://www.itu.int/md/D22-SG02.RGQ-ADM-0043

[111] https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf

[112] https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era

[113] https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-2-PDF-E.pdf

ويحدد التقرير المعايير الصادرة عن قطاع تقييس الاتصالات، ومشروع شراكة الجيل الثالث (3GPP)، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، ورابطة المعايير التابعة لمعهد مهندسي الكهرباء والإلكترونيات (IEEE SA)، إلى جانب الموارد غير القياسية ذات الصلة بالأمن السيبراني لتكنولوجيا الجيل الخامس.

ونشرت لجنة الدراسات 11 توصية بشأن أمن تكنولوجيا الجيل الخامس، استناداً إلى المساهمات التي أعدها المشغلون والبائعون ومصنعو الهواتف الذكية ومقدمو المحتوى وغيرهم. وتركز هذه التوصيات على الأمن في خمسة مجالات: الشبكات المعرّفة بالبرمجيات - التمثيل الافتراضي لوظائف الشبكة (SDN-NFV)، وتقسيم الشبكات إلى شرائح، وحافة الأجهزة المتنقلة، وإدارة شبكات الجيل الخامس، وخدمات الجيل الخامس. وقد أقامت لجنة الدراسات 17 علاقات شراكة مع منظمات وضع المعايير الأخرى - مثل مشروع شراكة الجيل الثالث 3GPP وفريق مهام هندسة الإنترنت (IETF)، ومجموعات الصناعة التي تعمل على المواصفات ذات الصلة بتقييس الأمن السيبراني للجيل الخامس.

وتتمثل إحدى مجموعات الصناعة هذه في **رابطة النظام العالمي للاتصالات المتنقلة** (GSMA). وعلى الرغم من أن الرابطة بحد ذاتها ليست هيئة معنية بوضع المعايير، فإنها تصدر مواصفات من خلال عقد اجتماعات لأعضائها والعمل مع منظمات وضع المعايير لتحسين هذه المواصفات و/أو اعتمادها كمعيار. ونشرت الرابطة قائمة بالضوابط الأمنية الأساسية التي يمكن لمشغلي الاتصالات المتنقلة مراعاتها، على أساس طوعي، عند نشر شبكات الجيل الخامس.[114]

ونظراً للمصادر العديدة للمعلومات ذات الصلة بأمن تكنولوجيا الجيل الخامس، نشرت **وكالة الاتحاد الأوروبي للأمن السيبراني** (ENISA)، مستودعاً موحداً للضوابط الأمنية التقنية لشبكات الجيل الخامس، وهو "مصفوفة الضوابط الأمنية للجيل الخامس".[115] ويُنشر هذا المستودع حالياً في شكل جدول بيانات، ولكن تعمل الوكالة أيضاً على إعداد أداة على الويب لتحسين قابلية الاستخدام.

ومع استمرار تزايد تعقيد الشبكات، وتقارب الاتصالات مع شبكات بروتوكول الإنترنت، أصبح من الصعب إسناد مجالات محددة لأعمال التقييس إلى فرادى منظمات وضع المعايير. ويزيد ذلك من مخاطر تداخل وازدواج العمل، وهو ما يعزز أهمية التواصل وتبادل المعلومات بين منظمات وضع المعايير.

2.3.5 دمج المعايير في المتطلبات التنظيمية

تساعد المعايير على ضمان قابلية التشغيل البيني للتكنولوجيات وتقلل من الوقت اللازم لنفاذ أي ابتكار إلى السوق العالمية الخاصة به. ويمكن أن تحدد معايير الأمن السيبراني أساساً أمنياً مشتركاً متفقاً عليه يعبر عن الممارسات الجيدة العالمية. وتوضع المعايير كنتيجة لعملية قائمة على توافق الآراء. وقد تكون المعايير إلزامية، ولكنها تكون في معظم الحالات اختيارية، بحيث تتيح للبائعين والمشغلين مزيداً من المرونة في قرارات النشر التي يتخذونها. وفي بعض الحالات، يمكن أن تصبح المعايير إلزامية إذا أدرجت اللوائح التقنية الوطنية معياراً محدداً في متطلباتها الأمنية.

وينبغي أن تعكس الاستراتيجيات الوطنية للأمن السيبراني لتكنولوجيا الجيل الخامس توازناً بين الممارسات الجيدة العالمية والواقع التشغيلي المحلي. وكقاعدة عامة، ينبغي أن تستند المتطلبات التنظيمية الوطنية إلى المعايير الدولية المتفق عليها، مع تكييفها وفقاً للسياقات والاحتياجات المحلية لضمان نجاح نشر شبكات الجيل الخامس وأمنها السيبراني.

4.5 استكمال المعايير والمواصفات بتدابير الأمن السيبراني الاستباقية

1.4.5 الاعتبارات الأمنية على مستوى البائع

المعايير والمواصفات ليست سوى مكون واحد من مكونات الأمن السيبراني لتكنولوجيا الجيل الخامس. وتحدد الطريقة التي ينفذ بها البائعون والمشغلون هذه المعايير ويشكلونها الوضع الأمني لشبكات الجيل الخامس. وقد تبنت شركة Ericsson نهجاً شاملاً إزاء أمن تكنولوجيا الجيل الخامس يتم تناوله على مستوى أربع طبقات: المعايير، وتطوير منتجات البائعين، ونشر الشبكات، وتشغيل الشبكات.[116] وترى الشركة أن هذا النهج الشامل

[114] https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/

[115] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

[116] https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security

من شأنه أن يضمن تنفيذ تدابير تخفيف المخاطر بطريقة تفي بالترابطات بين الطبقات، بالإضافة إلى الاحتياجات الخاصة بكل طبقة.

وكمثال ملموس على التدابير الأمنية للجيل الخامس، تسعى خطة ضمان أمن معدات الشبكات (NESAS)،[117] التي وضعتها **رابطة النظام العالمي للاتصالات المتنقلة (GSMA)** و**مشروع شراكة الجيل الثالث (3GPP)**، إلى تحسين مستويات أمن معدات شبكات الاتصالات المتنقلة من خلال توفير خطة ضمان يمكن تطبيقها عالمياً. وتعتمد خطة الضمان على مراجعة الخبراء الداخلية والمستقلة، وهو مزيج من التقييم بين عمليات البائعين وتقييم المنتج، وهو ما يوفر الاعتماد. والهدف من هذه الخطة هو تقليل عبء اختبار الأمن لمورّدي معدات الشبكات الذين غالباً ما يعملون على نطاق عالمي. وقد حصل البائعون الرئيسيون بالفعل على اعتماد بموجب خطة ضمان أمن معدات الشبكات (NESAS). والخطة مرشحة أيضاً لخطة اعتماد الأمن السيبراني للاتحاد الأوروبي المتعلقة بتكنولوجيا الجيل الخامس[118]، وهو اعتماد على مستوى الاتحاد الأوروبي يحقق التوافق عبر الدول الأعضاء في الاتحاد الأوروبي. ولن يحل هذا الاعتماد محل الخطة NESAS الحالية، ولكنهما سيتواجدان جنباً إلى جنب معها. ويعد إنشاء مبادرات الخطط/الاعتماد بحيث تظل مرنة ويمكن تحديثها بسرعة أمراً ضرورياً نظراً لتطور مشهد التهديدات.

وفي **المملكة المتحدة**، يوصي المركز الوطني للأمن السيبراني (NCSC) باستخدام إطار تقييم البائعين،[119] وهو عبارة عن توجيهات تساعد المشغلين على تقييم المخاطر السيبرانية المرتبطة باستخدام معدات البائع.

2.4.5 الاعتبارات الأمنية على مستوى المشغل

يمكن أن توفر خطة ضمان أمن معدات الشبكات (NESAS) مستوى ضمان على أن يكون عنصر من معدات الشبكة آمناً قبل النشر. ومع نشر المشغلين لشبكاتهم وتشغيلها، تدعو الحاجة إلى دمج اعتبارات أمنية أخرى من قبيل اكتشاف الهجمات والاستجابة الأوتوماتية. وهذه هي المرحلة التي ينبغي أن يفكر فيها المشغلون في الاستفادة من الذكاء الاصطناعي (AI) واستخبارات التهديدات والتحليلات للمساعدة على دعم الأمن السيبراني. ويوفر الأمن السيبراني لتكنولوجيا الجيل الخامس فوائد، مثل الأمن في الوقت الفعلي واستراتيجيات، من قبيل الثقة الصفرية، تحسن رؤية النظام. ومع ذلك، يواجه الأمن السيبراني لتكنولوجيا الجيل الخامس أيضاً تحديات خاصة به مثل الحفاظ على التوصيلية عبر شبكات مختلفة بمستويات أمن متفاوتة؛ والعمل مع المكونات القديمة وأنواع الشبكات المتنوعة؛ وتعقيدات دمج الذكاء الاصطناعي في التدابير الأمنية. ويضمن تطبيق ضوابط نفاذ صارمة وفقاً لمبدأ "أقل الامتيازات" التقليل إلى أدنى حد من الحقوق المختلفة في الشبكة، مثل حقوق النفاذ بين وظائف الشبكة، وحقوق مديري الشبكة، وتشكيل التمثيل الافتراضي. وتتاح للمشغلين ثروة من الأدبيات المتعلقة باستراتيجيات الأمن السيبراني الخاصة بتكنولوجيا الجيل الخامس يمكنهم النظر فيها.[120]

ويعد اختبار شبكات الاتصالات الحية أيضاً ضرورياً لتحديد المخاطر السيبرانية الحقيقية التي تواجهها شبكات الاتصالات. ويمكن للمشغلين إجراء بعض أشكال الاختبارات الأمنية على شبكاتهم وأنظمتهم، إما باستخدام الموارد الداخلية، وإما بالاستعانة بمقاولين خارجيين مستقلين. وفي **المملكة المتحدة**، تعد خطة TBEST خطة اختبار للاختراق قائمة على النتائج وتحاكي التقنيات والأساليب التي قد يستخدمها المهاجمون السيبرانيون الذين لديهم موارد كثيرة. وتُقيّم خطة TBEST مدى قدرة مقدم خدمات الاتصالات على اكتشاف مثل هذه الهجمات واحتوائها والتصدي لها. ويتمثل الهدف العام في تحديد نقاط الضعف الأمنية أو نقاط الضعف الأخرى في وظائف مقدم الخدمات أو عملياته أو سياساته أو أنظمته أو شبكاته والتي يمكن استخدامها معاً لاختراق أنظمة الشركة الحيوية قبل اكتشافها ومعالجة نقاط الضعف هذه. ومن خلال الخضوع لخطة TBEST الطوعية، يمكن لمقدمي خدمات الاتصالات تحديد مجالات محددة يمكن فيها تحسين أمنهم، ثم تعمل الهيئة التنظيمية Ofcom مع مقدم الخدمة للمساعدة في تنفيذ التغييرات المناسبة في الوقت المناسب.[121]

ومن الضروري وجود مبرر تجاري قوي بشأن الأمن السيبراني لتكنولوجيا الجيل الخامس. ففي حين أن المشغلين يحتاجون إلى رؤية عائد على استثماراتهم في خدمات الجيل الخامس، ينبغي الاعتراف بأن الامتثال للتدابير الأمنية الأساسية أمر لا غنى عنه ويجب تخصيص الميزانية اللازمة لذلك.

---

117 https://www.gsma.com/solutions-and-impact/industry-services/certification-services/network-equipment-security-assurance-scheme-nesas/

118 https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

119 https://www.ncsc.gov.uk/report/vendor-security-assessment

120 انظر على سبيل المثال https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf، و https://www.5gamericas.org/security-for-5g/

121 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/74 المقدمة من المملكة المتحدة

الإطار 2: شبكة النفاذ الراديوي المفتوح

تمثل شبكة النفاذ الراديوي المفتوح (Open RAN) تفكيك شبكة النفاذ الراديوي (RAN)، وتقييس السطوح البينية توصّل هذه العناصر المفككة مما يتيح بناء الشبكات باستخدام معدات من بائعين مختلفين.

فمن ناحية، يمكن أن تجلب شبكات النفاذ الراديوي المفتوح المزيد من التعقيد إلى سلسلة توريد شبكات الاتصالات. وتتطلب هذه المعمارية، التي تشجع تنوع البائعين في شبكة النفاذ الراديوي المفتوح، المزيد من جهود التكامل على امتداد سلسلة توريد الشبكة ويمكن أن تزيد ناقلات الهجمات. ومن ناحية أخرى، تضيف شبكة النفاذ الراديوي المفتوح الشفافية لسلاسل التوريد، وتمنح المشغلين مزيداً من الرؤية وتسمح لهم بمراقبة واكتشاف المخاطر الأمنية. فهي، باختصار، تحسن فهمهم لمعمارية الشبكة ومعداتها، وتمكّن من المسح بحثاً عن مواطن الضعف وإدارتها بشكل أشمل. ويعمل تحالف O-RAN، المصدر الرئيسي لمواصفات شبكات النفاذ الراديوي المفتوح، على المواصفات الأمنية لمعمارية شبكة النفاذ الراديوي المفتوح ويهدف إلى تقييس هذه المواصفات في المعهد الأوروبي لمعايير الاتصالات (ETSI).

ويعتبر المشغل NTT Docomo في اليابان واحداً من المشغلين الذين تبنوا معمارية شبكة النفاذ الراديوي المفتوح بسبب مرونتها فيما يتعلق باختيار المعدات. وأثار القرار تساؤلات من منظور أمني لأنه من المعتقد عموماً أن الانفتاح يعني زيادة احتمالات الهجمات. ومع ذلك، قارن المشغل بين شبكة النفاذ الراديوي التقليدية وشبكة النفاذ الراديوي المفتوح وخلص إلى وجود اختلاف أمني ضئيل بينهما.[1]

[1] لمزيد من المعلومات عن أمن شبكة النفاذ الراديوي المفتوح، انظر على سبيل المثال https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/enhancing-the-security-of-communication-infrastructure_79b78b4d/bb608fe5-en.pdf

5.5 مثال على السياسات واللوائح الوطنية لتأمين شبكات الجيل الخامس

بالإضافة إلى المعايير والممارسات التي يتبعها البائعون والمشغلون، يمكن اقتراح سياسات ولوائح لتأمين شبكات الجيل الخامس على المستوى القُطري. ويمكن أن تتخذ هذه السياسات واللوائح أشكالاً مختلفة منها تقييم البائعين، والاختبار، والاعتماد ووضع مبادئ توجيهية أو متطلبات. وفي حين تختلف النُهج حسب السياقات الوطنية، فإن هذه المبادرات كلها تهدف إلى تخفيف المخاطر الأمنية التي تفرضها تكنولوجيا الجيل الخامس، بما في ذلك المخاطر السيبرانية. وينبغي أيضاً النظر إلى أنظمة التنفيذ والامتثال كجزء من الإطار العام.

وتعرض الأمثلة أدناه لمحات عن الإجراءات التي اتخذتها مختلف البلدان والمناطق لتحقيق الأمن السيبراني لشبكات الجيل الخامس السيبراني، وحالتها الراهنة:

- يركز النهج الشامل الذي تتبعه **البرازيل** إزاء الأمن السيبراني لتكنولوجيا الجيل الخامس على إدارة المخاطر مع المشغلين. وبموجب شروط مزاد طيف الجيل الخامس ولوائح الأمن السيبراني لقطاع الاتصالات،[122] يُطلب من جميع مشغلي شبكات الجيل الخامس الامتثال للإطار التنظيمي الذي يتضمن المبادئ الأساسية والمبادئ التوجيهية والضوابط المسبقة لضمان الأمن السيبراني عبر القطاع. وتجمع الضوابط بين حوكمة الأمن السيبراني والإشعار الإلزامي بالحوادث وتبادل المعلومات ودورات تقييم مواطن الضعف والإبلاغ عن البنية التحتية الحيوية، وغيرها من الأحكام. وأقامت الوكالة الوطنية للاتصالات في البرازيل (Anatel) أيضاً شراكة مع الهيئات الأكاديمية لإجراء دراسات في هذا الصدد.[123]

[122] https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740؛ و https://informacoes.anatel.gov.br/legislacao/resolucoes/2024 (كلاهما بالبرتغالية).

[123] بعض النتائج متاحة في: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/estudos-e-pesquisas (بالبرتغالية).

- طورت حكومة **المملكة المتحدة** إطاراً أمنياً لمقدمي شبكات أو خدمات الاتصالات الإلكترونية العامة من خلال قانون الاتصالات لعام 2003 بصيغته المعدّلة بموجب قانون (أمن) الاتصالات لعام 2021 (TSA). وينطبق هذا الإطار على شبكات الجيل الخامس وجميع الشبكات الأخرى: في حين أن المملكة المتحدة تنتقل إلى مستقبل تكون فيه جميع الشبكات من الجيل الخامس وتعمل بالألياف البصرية بالكامل، فإن العديد من موزّدي الشبكات يدمجون التكنولوجيات القديمة في بنيتهم التحتية. ويحدد القانون TSA واجبات أمنية جديدة لجميع مقدمي خدمات الاتصالات العامة[124] ويمنح وزير الدولة سلطات جديدة لوضع اللوائح وإصدار مدونات الممارسة، والتي تم تطويرها منذ ذلك الحين وإرشادها من خلال التشاور العام.[125] ويتضمن القانون TSA أيضاً أحكاماً تعزز السلطات التنظيمية لهيئة Ofcom لمراقبة وإنفاذ كيفية امتثال المزودين لواجباتهم الجديدة.

- يُسلَّم بأن لوائح وسياسات الأمن السيبراني للجيل الخامس في **جمهورية كوريا** من بين الأكثر صرامة على مستوى العالم، وهو ما يعكس المكانة الرائدة للدولة في تبني تكنولوجيا الجيل الخامس. ونفذت الحكومة الوطنية، من خلال وزارة العلوم وتكنولوجيا المعلومات والاتصالات (MSIT) ووكالة الإنترنت والأمن الكورية (KISA)، إطاراً شاملاً لحماية شبكات الجيل الخامس. ويتضمن الإطار متطلبات صارمة للأمن السيبراني لتمكين مشغلي الاتصالات من تأمين البنية التحتية للشبكة وحماية بيانات المستعمل وتخفيف مخاطر الأمن السيبراني. وتؤكد اللوائح على الحاجة إلى سلاسل توريد آمنة ومعايير تجفير متقدمة ونشر مبادئ الأمن منذ مرحلة التصميم في معمارية الشبكة. وبالإضافة إلى ذلك، تتعاون جمهورية كوريا مع الشركاء الدوليين ومنظمات وضع المعايير لضمان أن تتواءم التدابير الأمنية لشبكات الجيل الخامس مع الممارسات الجيدة العالمية.

- يشمل الإطار القانوني والتقني في **الهند** المتعلق بتعزيز الأمن السيبراني لشبكات الجيل الخامس ما يلي:
  - التوجيهات الأمنية الوطنية بشأن قطاع الاتصالات، والتي توفر ضماناً لمعالجة الشواغل ومواطن الضعف في سلاسل توريد الاتصالات الموثوقة ومصادرها؛
  - والاختبار الإلزامي لمعدات الاتصالات واعتمادها، بما يضمن الامتثال للمتطلبات الأمنية الأساسية لكل وظيفة من وظائف شبكات الجيل الخامس؛
  - وشروط ترخيص مقدمي خدمات الاتصالات، التي تضمن المراجعات الأمنية الدورية للبنية التحتية للاتصالات.

  ولدعم ما سبق، أُنشئت مجموعة متنوعة من الآليات المؤسسية: مركز وطني لأمن الاتصالات (NCCS)، مكلف بوضع متطلبات/معايير أمن الاتصالات (متطلبات ضمان أمن الاتصالات في الهند (ITSAR)) مع مختبرات الاختبار والاعتماد الأمنية المرتبطة به؛ وفريق استجابة لحوادث الأمن الحاسوبي (CSIRT) لقطاع الاتصالات الوطني؛ وعدد من تدابير إدارة الاحتيال وحماية المستهلك التي تستهدف المواطن، وما إلى ذلك. وفيما يتعلق ببروتوكولات ومعايير الأمن من قبيل المشروع 3GPP، نظرت الهند في المواصفات المقترحة من هيئات معايير الصناعة لمراقبة الامتثال والشروط الإضافية لترخيص الاتصالات التي تتضمن عمليات مراجعة أمنية منتظمة لشبكات مقدمي الخدمة.

- في **الإمارات العربية المتحدة**، يتم التطرق إلى تأمين شبكات الجيل الخامس من خلال استراتيجية متعددة الأوجه تتضمن تمارين وتدريبات سيبرانية وطنية صارمة، وإنشاء مركز وطني لعمليات الأمن (SOC) لمراقبة التهديدات والاستجابة لها في الوقت الفعلي، ومبادرة Cyber Pulse التي تعمل على إذكاء الوعي وتدريب الموظفين على استراتيجيات الدفاع الرئيسية. ويؤكّد على التعاون وتبادل المعلومات مع الشركاء الدوليين والبائعين والهيئات الأكاديمية وأصحاب المصلحة الآخرين لتعزيز تدابير الأمن السيبراني. وبالإضافة إلى ذلك، وُضع إطار مرن للأمن السيبراني يتماشى مع المعايير الدولية مثل المعايير الصادرة عن المنظمة الدولية للتوحيد القياسي (ISO) والمعهد الوطني للمعايير والتكنولوجيا (NIST) لضمان الامتثال عبر قطاع الاتصالات. ولبناء ثقة المستهلك والشركات في أمن تكنولوجيا الجيل الخامس، وضع البلد سياسات وإجراءات وقوانين تعزز مبادئ الأمن منذ مرحلة التصميم وممارسات الأمن المسؤولة بين البائعين. وأخيراً، تبنى البلد نهجاً محوره الناس في مجال الأمن السيبراني، يشمل تركيزه على التدريب وإذكاء الوعي والدعم لتمكين الأفراد والمنظمات في مكافحة التهديدات السيبرانية، وبالتالي ترسيخ دفاع قوي ضد التهديدات المحتمل أن تتعرض لها شبكة الجيل الخامس.

---

124 باستثناء الكيانات بالغة الصغر.

125 https://www.legislation.gov.uk/uksi/2022/933/contents/made؛
و https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

- تتناول **زمبابوي** الأمن السيبراني لتكنولوجيا الجيل الخامس، مع التركيز على الأهمية الناشئة لحوسبة الحافة واستكشاف اعتماد تكنولوجيا شبكات النفاذ الراديوي المفتوح لإتاحة المرونة للبائعين. وفي حين لا يوجد قانون محدد لأمن شبكات الجيل الخامس، فإن تشريعات حماية البيانات الحالية ووثيقة حوكمة الذكاء الاصطناعي قيد التنفيذ تدعم نهج البلد. وستعمل زمبابوي على مواءمة ممارساتها الأمنية مع المعايير الدولية مثل المعيار 27001 للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية ومعايير المعهد الوطني للمعايير والتكنولوجيا (NIST)، مما يضمن امتثال السطوح البينية الراديوية الجديدة للجيل الخامس لبروتوكولات الأمن المعمول بها. وتعمل هيئة تنظيم البريد والاتصالات في زمبابوي على إنفاذ المبادئ التوجيهية الأمنية وإذكاء وعي الصناعة للحفاظ على سلامة البنية التحتية الوطنية للاتصالات.
- اعتمدت **كينيا** خارطة طريقها واستراتيجيتها للجيل الخامس فيما يتعلق بالاتصالات المتنقلة في أبريل 2022. وتقر الاستراتيجية بأن الأمن يمثل جانباً مهماً من معمارية شبكة الجيل الخامس. وتكتسي الطبيعة المتطورة للخدمات الموصولة والزيادة الكبيرة المتوقعة في عدد وأنواع الأجهزة الموصولة أهمية أكبر فيما يتعلق بخصوصية البيانات وحماية البيانات والأمن السيبراني في كينيا؛ ويشمل ذلك اكتشاف التهديدات واستيقان المستعملين والممارسات التشغيلية الجيدة. وتوفر تكنولوجيا الجيل الخامس أمناً أفضل منذ مرحلة التصميم بحيث تشمل متطلبات أمنية معززة تستند إلى تطور الشبكات وتتكيف وفقاً للدروس المستفادة من التكنولوجيات السابقة. واعتمدت هيئة الاتصالات في كينيا معياراً دولياً معتمداً وضعه الاتحاد بالاشتراك مع مشروع 3GPP لضمان التشغيل البيني للأنظمة المتنقلة وأمنها. وتعتزم الهيئة الاستفادة من خبرة مختلف أصحاب المصلحة والممارسات الجيدة الدولية في مجال الأمن السيبراني لتطوير الشفرات التقنية وإعداد قائمة مقيسة لتقييم الحد الأمني الأدنى لضمان أن تلبي شبكات الجيل الخامس أحدث المعايير التقنية وأن تكون متوافقة مع المعايير العالمية فيما يتعلق بأمن الجيل الخامس.
- بعد استعراض واسع لمخاطر الأمن السيبراني التي تتعرض لها شبكات الجيل الخامس، وضع **الاتحاد الأوروبي** مجوعة أدوات لتدابير تخفيف المخاطر[126] بهدف تحديد مجموعة مشتركة من التدابير لتخفيف المخاطر الرئيسية للأمن السيبراني لتكنولوجيا الجيل الخامس، والمساعدة على تحديد أولويات تدابير تخفيف المخاطر في الخطط على مستوى الاتحاد الأوروبي وعلى المستوى الوطني. وتسلط استراتيجية الأمن السيبراني للعقد الرقمي الضوء على أهمية حماية الجيل القادم من شبكات النطاق العريض المتنقلة، وتتضمن تذييلاً محدداً بشأن الخطوات التالية للأمن السيبراني لشبكات الجيل الخامس.[127] ويتضمن إطار الاعتماد للاتحاد الأوروبي التطوير المستمر لنظام إصدار شهادات الأمن السيبراني لتكنولوجيا الجيل الخامس.[128]

6.5 تحديات التنفيذ والامتثال

في حين يعد وضع السياسات ضرورياً، فإن التركيز ينبغي أن ينصب على التنفيذ الفعال. وتعتبر آليات الإبلاغ، والامتثال للمعايير ذات الصلة، والتدابير العملية لإنفاذ السياسات واللوائح ضرورية لضمان أمن سيبراني قوي لشبكات الجيل الخامس. وستتطلب الأطر الجديدة التي تقدم تغييرات لأمن شبكات الاتصالات رحلة امتثال مستمرة لمقدمي خدمات الاتصالات وبالتالي التعاون بشكل وثيق مع الصناعة. وفي **المملكة المتحدة**، تستخدم هيئة Ofcom نموذجاً إشرافياً بموجب سياسة أمن الاتصالات الخاصة بها وتتعاون مع الأفرقة التنظيمية والتقنية لدى مقدمي خدمات الاتصالات. وتعتبر الهيئة التنظيمية أن التنفيذ لا يتعلق بالتدابير التقنية فحسب، بل يتطلب أيضاً تحولاً ثقافياً في طريقة تفكير مقدمي خدمات الاتصالات في الأمن، ما يقتضي منهم تحديد الأجزاء من شبكاتهم وخدماتهم التي أسندوها لمصادر خارجية وتحمل المسؤولية عنها. ويعد العمل على المستوى العالي والحصول على التزام كبار المسؤولين عبر الحكومة والهيئات التنظيمية والصناعة ورعايتهم شرطاً أساسياً للنجاح.[129]

وفي **ماليزيا**، وافقت الحكومة على مشروع قانون جديد بشأن الأمن السيبراني ينص على أن وكالة واحدة ستدير جميع البنى التحتية الحيوية. وستقع شبكات الاتصالات، بما في ذلك شبكات الجيل الخامس، في إطار مشروع قانون الأمن السيبراني الجديد هذا. والهيئة التنظيمية[130] بصدد وضع مجموعة من المتطلبات للمشغلين للإبلاغ

126 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

127 https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

128 https://certification.enisa.europa.eu/index_en

129 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات SG2RGQ/191 المقدمة من المملكة المتحدة

130 https://www.nacsa.gov.my/act854.php

عن الامتثال الأمني. وفي إطار المخرج المؤقت للمسألة 3/2 بشأن الأمن السيبراني للجيل الخامس،[131] سلط أحد مشغلي الاتصالات في البلد الضوء على أن تنفيذ السياسة الجديدة قد يكون صعباً، إذ إنه يتضمن التواصل بشأن المخاطر وتحديد الحد الأدنى من المتطلبات الأمنية، وهو ما يتطلب مشاورات مكثفة من حيث الوقت والتكلفة والعمل، مما يؤثر غالباً على اعتبارات المساهمين. وبالنسبة للمشغلين الذين لديهم مساهمون، فإن الهياكل والسياسات واللوائح المتعلقة بالأمن لا تكون متوافقة في بعض الأحيان، مما قد يشكل تحدياً لأفرقة الأمن. وبناء على ذلك، هناك حاجة إلى إشراك جميع الأفرقة، بما في ذلك المسؤولون التنفيذيون عند النظر في أطر الأمن الجديدة.

7.5 ضرورة منح الأولوية للاستثمار في تعليم وتدريب القوى العاملة

وفقاً لشركة Allied Market Research،[132] من المتوقع أن تصل قيمة السوق العالمية لأمن تكنولوجيا الجيل الخامس إلى 37,8 مليار دولار أمريكي بحلول عام 2031، مع طلب متزايد على المهنيين في مجال الأمن السيبراني، وخاصة أولئك الذين لديهم مهارات متخصصة لحماية شبكات الجيل الخامس. وينبغي أن تعطي البلدان والمنظمات والمؤسسات الأولوية لتدريب القوى العاملة وتوظيفها لضمان تقدم الأمن السيبراني لشبكات الجيل الخامس. ومن الصعب حالياً العثور على المهارات المتخصصة اللازمة في القوى العاملة؛ وعلاوةً على ذلك، من الصعب تحقيق التوازن بين الجنسين في التوظيف. وإذا كانت القوى العاملة غير جاهزة، فسيؤدي ذلك إلى تباطؤ وتعقيد الانتقال إلى الجيل الخامس. وفي حين ينبغي للبلدان أن تعطي الأولوية للتدريب والتعليم من خلال البرامج الوطنية، يمكن للقطاع الخاص أيضاً أن يستكشف برامج التدريب وتنمية المهارات، لأن مشاركة الصناعة على نطاق أوسع ضرورية لضمان تلبية الاحتياجات.

ومن الأمثلة على البلدان التي تجد حلولاً لتحديات القوى العاملة **تركيا**، بزيادة الإستثمار في تعليم وتدريب القوى العاملة القادرة على إدارة تعقيدات أمن الجيل الخامس. وفي إطار هذا الالتزام، أنشأت مؤسسات رئيسية موقع الاختبار المفتوح لوادي الجيل الخامس، منها هيئة تكنولوجيا المعلومات والاتصالات، وجامعة الشرق الأوسط التقنية، وجامعة Bilkent İhsan Doğramacı، وجامعة Hacettepe، ومشغلو الاتصالات Türk Telekomünikasyon A.Ş. و Turkcell İletişim Hizmetleri A.Ş. و Vodafone Telekomünikasyon A.Ş. ويعمل هذا الموقع كمنصة حيوية للبحث والتطوير واختبار تكنولوجيات الجيل الخامس وما بعده، مما يوفر فرصاً للتعاون الأكاديمي والصناعي. ويضمن المجلس التنفيذي لوادي الجيل الخامس، الذي يضم ممثلين من المؤسسات المذكورة أعلاه، التنفيذ الفعال لهذه المبادرة. ومن خلال توفير منصة يستطيع من خلالها الأكاديميون والباحثون وطلاب الدكتوراه والشركات الناشئة المشاركة في العمل المتعلق بتكنولوجيا الجيل الخامس وما بعده، فإن موقع الاختبار المفتوح لوادي الجيل الخامس لا يعمل على تعزيز الابتكار فحسب، بل يساهم أيضاً في تطوير قوى عاملة عالية المهارة. وهذه المبادرة جزء لا يتجزأ من استراتيجية تركيا لإعطاء الأولوية لأمن شبكات الجيل الخامس وتعزيزها من خلال الاستثمار المستمر في التعليم والتدريب والبحث.[133]

8.5 ما بعد الجيل الخامس: تحديد الاتجاه للأمن السيبراني للجيل السادس

على الرغم من أن تكنولوجيا الجيل الخامس لا تزال في مرحلة التخطيط والنشر في العديد من البلدان والمناطق، فإن الاهتمام بالبحث والتطوير، فضلاً عن عمليات التقييس، يتجاوز بالفعل شبكات الجيل الخامس. وبالتالي، وافق قطاع الاتصالات الراديوية **بالاتحاد** (ITU-R) في نهاية عام 2023 على الإطار والأهداف العامة للتطوير المستقبلي للاتصالات المتنقلة الدولية لعام 2030 وما بعده، المعروفة تجارياً باسم الجيل السادس.[134]

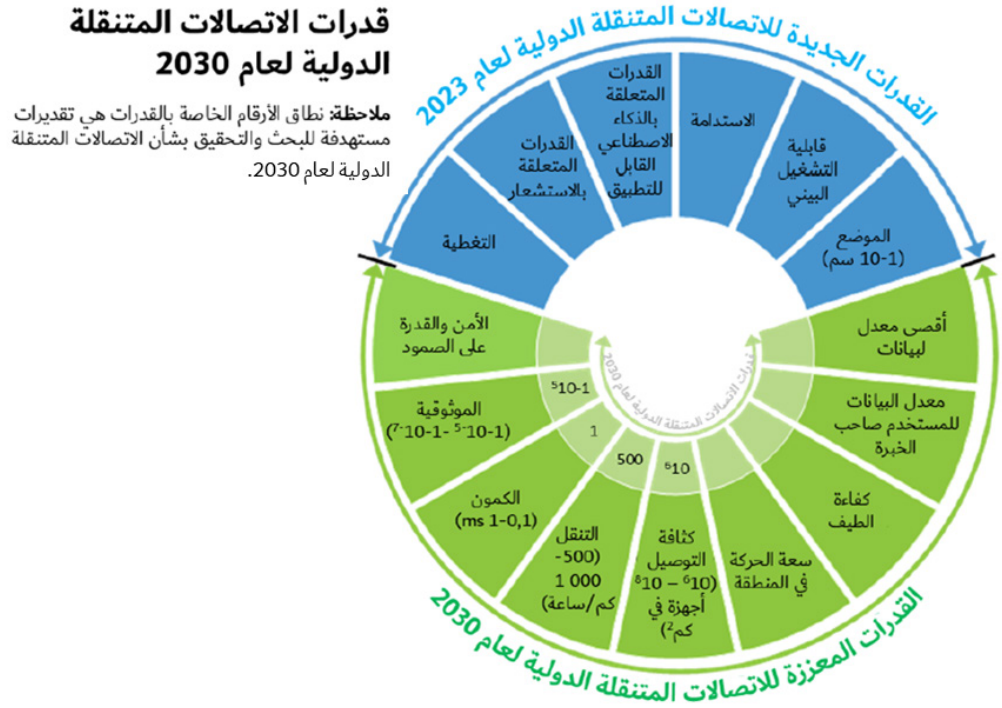
131 https://www.itu.int/hub/publication/d-stg-sg02.03.2-2024/#/ar
132 https://www.alliedmarketresearch.com/5g-security-market-A12820
133 https://5gtrforum.org.tr/en
134 التوصية ITU-R M.2160 متاحة في: https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en

الإطار 3: الاتصالات المتنقلة الدولية-2030

يسلط هذا الإطار الضوء على أن من المتوقع أن تكون أنظمة الاتصالات المتنقلة الدولية-2030 عاملاً تمكينياً مهماً لتعزيز الأمن والقدرة على الصمود. ومن المتوقع أن تكون هذه الأنظمة آمنة منذ مرحلة التصميم وأن تتمتع بالقدرة على الاستمرار في العمل أثناء وقوع حدث معطل، سواء كان طبيعياً أو من صنع الإنسان، وإصلاحه بسرعة. وتؤكد الوثيقة أيضاً أن أمن أنظمة الاتصالات المتنقلة الدولية-2030 وقدرتها على الصمود أمران أساسيان لتحقيق الأهداف المجتمعية والاقتصادية الأوسع.

وفي سياق الاتصالات المتنقلة الدولية-2030، تعرَّف القدرة الأمنية من خلال الإطار على أنها "*الحفاظ على سرية وسلامة وتوافر المعلومات، مثل بيانات المستخدم والإشارات، وحماية الشبكات والأجهزة والأنظمة ضد الهجمات السيبرانية مثل القرصنة، والحرمان من الخدمة الموزَّع، وهجمات الوسيط، وما إلى ذلك*". وتعرَّف القدرة على الصمود على أنها "*قدرة الشبكات والأنظمة على الاستمرار في العمل بشكل صحيح أثناء وبعد اضطراب طبيعي أو من صنع الإنسان، مثل فقدان المصدر الأساسي للطاقة، وما إلى ذلك*".

الشكل 2: قدرات الاتصالات المتنقلة الدولية-2030



المصدر: الاتحاد الدولي للاتصالات

لقد أصبح من الواضح أن العمل جار على تصور الجيل السادس وأن عمليات تقييسه يجري تصورها بمستوى قلق كبير فيما يتعلق بالأمن والقدرة على الصمود، على النقيض من مراحل التصميم المبكرة لتكنولوجيا الجيل الخامس، بما في ذلك من منظور التقييس. ومن خلال المقارنة مع رؤية الاتصالات المتنقلة الدولية-2020 (المعروفة تجارياً باسم الجيل الخامس) التي تمت الموافقة عليها في عام 2015،[135] يتضح جلياً التحول في التفكير مع إقرار الحاجة إلى تناول الأمن السيبراني والقدرة السيبرانية على الصمود بشكل صحيح كركيزة تمكينية للتحول الرقمي والاقتصاد الرقمي.

[135] التوصية ITU-R M.2083 متاحة في: https://www.itu.int/rec/R-REC-M.2083-0-201509-I

الفصل السادس - التحديات والنُهُج المتعلقة بمكافحة الاحتيال عبر خدمة الرسائل القصيرة

تُستخدم خدمة الرسائل القصيرة (SMS) من قِبل جهات ضارة كأداة لتنفيذ الهجمات. وعالمياً، شهد استخدام خدمة الرسائل القصيرة في عمليات الرسائل الاقتحامية[136] وعمليات الاحتيال عبر الرسائل النصية زيادة ملحوظة. وتعتمد هذه الأخيرة على أساليب لخداع المستعملين عند تقديم بياناتهم الشخصية، بما في ذلك البيانات المالية، وتنزيل برمجيات ضارة على أجهزتهم. ولا يؤدي الاحتيال عبر الرسائل القصيرة إلى انخفاض ثقة المستعمل في خدمات المراسلة في الاتصالات ومستوى رضاه فحسب، بل يؤدي أيضاً إلى هدر موارد الشبكة.

وتشير بيانات لجنة التجارة الفيدرالية الأمريكية إلى خسائر مُبلغ عنها بقيمة 330 مليون دولار أمريكي نتيجة لعمليات الاحتيال عبر الرسائل النصية في عام 2022، أي أكثر من ضعف الخسائر المُبلغ عنها في عام 2021.[137] وخلال الفترة نفسها، تلقت وحدة مراقبة الاحتيال في أستراليا التابعة للمركز الوطني لمكافحة الاحتيال ما يقرب من 000 80 بلاغ عن عمليات احتيال عبر الرسائل النصية، بلغت قيمتها أكثر من 28 مليون دولار أسترالي.[138]

وعلى الرغم من اختلاف استخدام خدمات الرسائل النصية القصيرة باختلاف البلدان، وأن الابتكار في قطاع الاتصالات/تكنولوجيا المعلومات والاتصالات قد أتاح أساليب جديدة للتواصل، بما في ذلك من خلال تطبيقات خدمة المراسلة عبر الهواتف المتنقلة المنتشرة عالمياً، فإن خدمة الرسائل القصيرة لا تزال قيّمة للمستخدمين نظراً لبساطتها وتوافرها على جميع الهواتف المتنقلة.

وفي هذا السياق، يتناول هذا الفصل "الاحتيال عبر خدمة الرسائل القصيرة" وهو أحد أكثر أنواع حوادث خدمة الرسائل القصيرة انتشاراً، وتوصيات المعايير لمكافحة الاحتيال عبر خدمة الرسائل القصيرة، وبعض التجارب والنُهُج الوطنية لمواجهة مثل هذه التحديات.[139]

1.6 الاحتيال عبر خدمة الرسائل القصيرة

يعني مصطلح "التصيد الاحتيالي" استخدام رسائل البريد الإلكتروني أو الرسائل النصية أو المكالمات الصوتية أو رسائل مواقع التواصل الاجتماعي التي تبدو شرعية، ولكنها تهدف إلى خداع المتلقي، وعادةً ما يتم ذلك من خلال انتحال هوية شخص أو جهة موثوقة، مثل بنك أو جهة حكومية أو جهة عمل أو أحد أفراد الأسرة. وغالباً ما يُوجه المستعمل إلى موقع إلكتروني يُدخل فيه بياناته الشخصية، مما يؤدي إلى سرقة الهوية، أو قد يتم استدراج المستعمل لتقديم معلومات شخصية مثل بيانات مصرفية أو معلومات بطاقة ائتمان، أو لإجراء دفعة مالية إلى حساب وهمي.

وفي مجال الأمن السيبراني، يُعدّ الاحتيال عبر خدمة الرسائل القصيرة أحد أكثر أنواع الاحتيال شيوعاً، وهو مصطلح يجمع بين كلمتي "التصيد الاحتيالي" و"خدمة الرسائل القصيرة"، ويشير إلى رسائل التصيد الاحتيالي المرسلة إلى الهواتف المتنقلة عبر خدمة الرسائل القصيرة. ووفقاً للإضافة 29 للتوصية ITU-T X.1242،[140] فإن الاحتيال عبر خدمة الرسائل القصيرة هو "*هجوم يُخدع فيه المستعمل لتنزيل حصان طروادة أو فيروس أو أي برمجيات ضارة أخرى على هاتفه الخلوي أو أي جهاز متنقل آخر*"، ويُعرّف التصيد الاحتيالي بأنه "*هجوم للحصول على معلومات حساسة، مثل أسماء المستعملين وكلمات المرور وتفاصيل بطاقات الائتمان، لأغراض خبيثة، من خلال بالتنكر ككيان موثوق في رسالة إلكترونية*".

---

136 عُرف الرسائل الاقتحامية على أنها "*المعلومات الإلكترونية التي يتم تسليمها من المرسلين إلى المستلمين من خلال مطاريف مثل أجهزة الحاسوب والهواتف المتنقلة والهواتف وما إلى ذلك، والتي عادة ما تكون غير مطلوبة وغير مرغوب فيها وضارة للمستلمين*" بموجب التوصية ITU-T X.1242 - https://www.itu.int/rec/T-REC-X.1242-200902-I

137 https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022

138 https://www.scamwatch.gov.au/research-and-resources/scam-statistics

139 يرتبط هذا الموضوع ارتباطاً وثيقاً بخدمات الاتصالات واسعة الانتشار وأنشطة مكافحة الاحتيال على الإنترنت. ويتضمن التقرير النهائي للمسألة 6/1 (توعية المستهلك وحمايته وحقوقه) بنداً مخصصاً عن الاحتيال على الإنترنت.

140 https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13409

وأصبحت هجمات الاحتيال عبر خدمة الرسائل القصيرة تهديداً متزايداً خلال السنوات الأخيرة، وقد زاد استخدام أدوات الذكاء الاصطناعي (AI) من انتشاره، مما يُبرز نطاق هذا النوع الجديد من الهجمات السيبرانية وطبيعته المتطورة بشكل متزايد. ففي عام 2022، تعرّض أكثر من نصف الأجهزة المتنقلة الشخصية وربع أجهزة الشركات المحمولة لهجوم تصيد احتيالي واحد على الأقل كل ثلاثة أشهر، مع زيادة هجمات الاحتيال عبر خدمة الرسائل القصيرة، وهي هجمات تصيد احتيالي غير معتمدة على البريد الإلكتروني، بأكثر من سبعة أضعاف في الربع الثاني من عام 2022.[141]

ويصعب أحياناً على مستعملي خدمات الاتصالات تحديد هذا النوع من الهجمات. فباستخدام تقنيات الهندسة الاجتماعية، يرسل المُجرمون رسائل مزيفة إلى الأجهزة المتنقلة، خادعين المُستلِمين للنقر على روابط URL المُضمنة في هذه الرسائل. وقد يستخدم المُجرمون السيبرانيون خدمات اختصار عناوين URL لإخفاء روابط تسجيل الدخول المزيفة، مما يُصعّب تحديد ما إذا كانت الرسالة من مُحتال. وهناك بعض العلامات الرئيسية التي تُشير إلى أن الرسالة احتيالية، مثل عدم وجود علاقة بين الرسالة والمُستلِم؛ أو أن الرسالة مُشبعة بإحساس الإلحاح في معظم الحالات؛ أو أن الرسالة مُرسلة من رقم هاتف غير مألوف؛ أو أن الرسالة تحتوي على أخطاء إملائية ونحوية؛ أو أن الرسالة تحتوي على رابط مُريب.

ويحتاج المستعملون إلى إدراك المخاطر ومعرفة الخطوات التي يُمكنهم اتخاذها لتجنب الوقوع كضحايا لهجوم احتيال عبر خدمة الرسائل القصيرة. كما أن لموردي الخدمات أدوار هامة، وكذلك للقطاع العام، الذي لا يُمكنه فقط العمل مع قطاع الاتصالات لضمان اتباع المعايير والممارسات الجيدة، ولكن أيضاً لتعزيز الوعي بين السكان حول الاحتيال عبر خدمة الرسائل القصيرة.

2.6 النُهُج المتبعة لمكافحة الاحتيال عبر خدمة الرسائل القصيرة

1.2.6 النُهُج القُطرية لمكافحة الاحتيال عبر خدمة الرسائل القصيرة

خلال فترة الدراسة، ركزت الدول الأعضاء في الاتحاد على تطوير اللوائح التنظيمية، ورفع مستوى الوعي، والتعاون مع القطاع الخاص، والمشاركة في التعاون الدولي لمكافحة الاحتيال عبر خدمة الرسائل القصيرة. ورغم كثافة الجهود الجارية للتصدي للتحديات التي يطرحها الاحتيال عبر خدمة الرسائل القصيرة، فمن الواضح أنه لا يوجد حل واحد يناسب الجميع لهذه المشكلة، وأن هناك حاجة إلى نهج متعدد الجوانب، بما في ذلك اعتبار هذه الهجمات جرائم جنائية.

واعتمد **الاتحاد الروسي**[142] هذا النهج الأخير، الذي يُجرّم أفعال المحتالين عبر الهاتف، بما في ذلك المحتالين عبر خدمة الرسائل القصيرة، بموجب المادة 159 من القانون الجنائي للاتحاد الروسي. كما اعتمدت إدارة الاتحاد الروسي تدابير لحظر تأجير أرقام الهواتف المتنقلة الافتراضية، ودخلت هذه التدابير حيز التنفيذ في سبتمبر 2024. وقد اعتُبر تأجير أرقام الهواتف المتنقلة الافتراضية هذه تهديداً أمنياً، إذ تستخدم الجهات الفاعلة الضارة هذه الأرقام المؤقتة لإنشاء حسابات على شبكات التواصل الاجتماعي وتطبيقات الرسائل لنشر التهديدات. ومن الإجراءات الأخرى التي اعتمدتها إدارة الاتحاد الروسي إطلاق منصة لمكافحة الاحتيال تتيح التحقق من المكالمات الهاتفية. وبمساعدة هذه المنصة، يتحقق موردو خدمات الاتصالات الموصولون من الأرقام ويتأكدون من صحتها، ويحظرون المكالمات والرسائل النصية القصيرة المشبوهة قبل وصولها إلى المستلم. والتوصيل بالنظام، وهو إلزامي لجميع خدمات الاتصالات المعتمدة لتقديم خدمات الاتصالات الصوتية، مجاني، ولكن عدم التوصيل سيؤدي إلى غرامة تتراوح بين 600 000 ومليون روبل روسي. كما استُكملت هذه المبادرات بحملات توعية لتمكين المستعملين.

كما اعتمدت حكومة **أستراليا** نهجاً شاملاً يشمل مبادرات الصناعة والحكومة، إلى جانب جهود زيادة. وقد شكّلت مكافحة عمليات الاحتيال عبر خدمة الرسائل القصيرة أولويةً للامتثال في السنوات الأخيرة لهيئة الاتصالات والإعلام الأسترالية (ACMA)، التي أصدرت سلسلةً من القواعد الجديدة. وشملت هذه القواعد: إلزام موردي خدمات الاتصالات بتحديد المكالمات والنصوص الاحتيالية وتتبعها وحظرها؛ وفرض إجراءات أقوى للتحقق من الهوية قبل نقل أرقام الهواتف المتنقلة بين موردي الخدمات؛ وفرض إجراءات أقوى للتحقق من الهوية بالنسبة للمعاملات عالية المخاطر، بما في ذلك تبديل بطاقات SIM وطلبات تغيير الحسابات، وغيرها. وتُجري الهيئة تدقيقاً على موردي خدمات الاتصالات الذين يرسلون رسائل نصية جماعية، وقد كشفت هذه الإجراءات التنفيذية

141 https://www.lookout.com/documents/reports/Global-State-of-Mobile-Phishing-Report.pdf

142 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/158 المقدمة من الاتحاد الروسي

عن استغلال جهات خبيثة للثغرات الأمنية الناجمة عن عدم الامتثال في إرسال رسائل احتيالية رفيعة المستوى عبر خدمة الرسائل القصيرة إلى الأستراليين.[143]

وتشمل أنشطة الإنفاذ الأخرى التي تقوم بها هيئة الاتصالات والإعلام الأسترالية لمكافحة عمليات الاحتيال في مجال الاتصالات ما يلي: إصدار تنبيهات للمستهلكين حول انتحال صفة الوكالات الحكومية وعمليات الاحتيال المتعلقة بالنفاذ عن بُعد؛ والعمل خلف الكواليس مع موردي خدمات الاتصالات والوكالات الحكومية والعلامات التجارية المعروفة لتعطيل عمليات الاحتيال عبر الهاتف؛ والقيام بالتعاون الدولي مع الدول الأخرى والهيئات التنظيمية الدولية لتعزيز المشاركة الاستراتيجية في المكافحة العالمية ضد عمليات الاحتيال والتسويق عبر الهاتف غير المرغوب فيه والرسائل الاقتحامية.

وبالإضافة إلى ذلك، شرعت الحكومة الأسترالية في الطرح التدريجي لتدابير محددة لمكافحة الاحتيال في عام 2023، بما في ذلك إنشاء مركز وطني لمكافحة الاحتيال (NASC)، وإنشاء صفحة ويب مزودة بخاصية إزالة الصفحات المُخصصة لعمليات الاحتيال الاستثماري، وإطلاق سجلّ بمُعرّفات هوية مُرسِلي الرسائل النصية القصيرة.

وقد كان التعاون والشراكة بين مختلف الجهات الفاعلة المعنية نهجاً متسقاً اعتمدته عدة بلدان، ويشكّل حجر زاوية للمبادرات المتخذة في **جمهورية كوريا**. وقد سهّل هذا البلد تبادل معلومات التهديدات المتعلقة بأساليب الاحتيال عبر خدمة الرسائل القصيرة، مما يسمح بتحديد وتخفيف حدة نواقل الهجمات الجديدة بشكل أسرع، بالإضافة إلى أنظمة إبلاغ آلية ليستخدمها المستعملون، ويتشاركونها مع مُوردي خدمات الاتصالات لأغراض الحظر.

ويمكن لأدوات الذكاء الاصطناعي أيضاً أن تساعد في مكافحة الاحتيال عبر خدمة الرسائل القصيرة كما هو الحال في جمهورية كوريا على سبيل المثال، حيث تنفذ وزارة العلوم وتكنولوجيا المعلومات والاتصالات (MSIT) ووكالة الإنترنت والأمن الكورية (KISA) مجموعة من التدابير المصممة خصيصاً لمعالجة الاحتيال عبر خدمة الرسائل القصيرة، بما في ذلك:

- المراقبة في الوقت الفعلي وحظر رسائل الاحتيال عبر خدمة الرسائل القصيرة من خلال نظام الكشف والتصفية القائمة على الذكاء الاصطناعي الذي يحلل أنماط الرسائل النصية القصيرة،
- الإشارة إلى الرسائل المشبوهة لحظرها، والكشف عن عناوين URL الضارة داخل محتوى الرسائل النصية القصيرة؛
- إنشاء قاعدة بيانات للأرقام الضارة التي يحتفظ بها ويتشاركها موردو خدمات الاتصالات؛
- تنفيذ أنظمة تصفية مدعومة بالذكاء الاصطناعي؛
- إنشاء خط ساخن للإبلاغ الوطني (118) وبوابات إلكترونية تديرها وكالة الإنترنت والأمن الكورية.[144]

وتُجسد هذه الأنشطة أهمية معالجة الأبعاد المتعددة للظواهر مع الحاجة إلى إشراك موردي خدمات الاتصالات؛ وتبني التكنولوجيات الجديدة والناشئة للمساعدة في التحليل والتصفية والحظر؛ وتنفيذ الإجراءات والعمليات اللازمة؛ وتطوير نظام إبلاغ وصيانته؛ والاستفادة من بيانات الإبلاغ؛ وكذلك العمل بشكل مكثف على توعية السكان. ولا يمكن الاستهانة بأهمية زيادة وعي المستعملين. فكثيراً ما تقوم الجهات الفاعلة الضارة بتغيير أساليبها وتطويرها وإعادة ابتكارها، والمستعمل المستنير والممكَّن والواعي لديه فرص أكبر في تجنب الوقوع كضحية.

2.2.6 نُهج الصناعة لمكافحة الاحتيال عبر خدمة الرسائل القصيرة

اتخذت صناعة الاتصالات خطوات إيجابية لمكافحة وتخفيف آثار الاحتيال عبر خدمة الرسائل النصية القصيرة وعمليات الاحتيال بشكل عام. وفيما يتعلق بالأساليب التقنية، استحدث موردو الخدمات تدابير مثل آليات الإبلاغ، وجدران حماية للرسائل النصية القصيرة، وحظر عناوين مواقع التصيد الاحتيالي المعروفة، وسجلات حماية بمُعرّفات هوية مُرسِلي الرسائل النصية القصيرة. وتستطيع جدران حماية الرسائل النصية القصيرة منع وصول كميات كبيرة من الرسائل غير المطلوبة إلى المستعملين، كما تتيح سجلات مُعرّفات هوية مُرسِلي الرسائل النصية القصيرة للمؤسسات تسجيل وحماية عناوين الرسائل المستخدمة عند إرسال رسائلها النصية القصيرة إلى عملائها، مما يحد من تأثير الاحتيال عبر خدمة الرسائل القصيرة والانتحال. والإبلاغ عن الاحتيال،

[143] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/154 المقدمة من أستراليا
[144] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/312 المقدمة من جمهورية كوريا

عندما ينفذ بطريقة منسقة عبر العديد من مشغلي الاتصالات المتنقلة، هو وسيلة فعالة للتعرف على عمليات الاحتيال وإزالتها. وتتيح خدمة الإبلاغ عبر الرقم 7726 في **المملكة المتحدة** و**كندا** الإبلاغ عن الرسائل المشبوهة للتحقيق فيها.[145] وقام أربعة من مشغلي الاتصالات المتنقلة الرئيسيين في المملكة المتحدة، بالتعاون مع مكتب مفوض المعلومات في المملكة المتحدة، بتنفيذ خدمة الإبلاغ عبر الرقم 7726 التي تمكّن الأشخاص من إعادة توجيه الرسائل النصية المشبوهة، بالإضافة إلى الرسائل الاقتحامية، دون أي تكلفة. وحتى مارس 2025، تم حذف 26 000 رقم احتيالي.[146]

ويُعد الاحتيال في مدفوعات التحويل المباشرة المُصرّح بها (APP) مشكلةً أخرى تُلحق خسائر مالية فادحة بالمستهلكين، نتيجةً لاتصال المجرمين بالضحايا عبر الرسائل النصية القصيرة أو المكالمات الهاتفية، مُدّعين أنهم من جهاتٍ شرعية، مثل البنوك، ثم يحصلون على تحويل مالي منهم. وقد دعت **رابطة النظام العالمي للاتصالات المتنقلة** و**الهيئة المالية للمملكة المتحدة** شركات الاتصالات المتنقلة والبنوك في المملكة المتحدة لتقديم "إشارة احتيال"، وهو حلٌّ يستخدم السطح البيني لبرمجة التطبيقات (API) لتمكين البنوك من تحديد التحويلات الاحتيالية بشكل أفضل وإيقافها.[147]

وفي العديد من بلدان إفريقيا جنوب الصحراء حيث تحظى الخدمات المالية المتنقلة بشعبية كبيرة، يُعد تعزيز الأمن في هذه المنصات محوراً أساسياً. وقد قامت خدمة M-Pesa في **كينيا** والخدمات المماثلة في بلدان أخرى بدمج الاستيقان البيومترية والتجفير المحسن وأنظمة الكشف عن الاحتيال المعززة لحماية المستعملين من هجمات انتحال الهوية والتصيد الاحتيالي[148]. وعلى الصعيد العالمي، ينشر المشغلون في جميع المناطق سطوح بينية مختلفة لبرمجة التطبيقات مثل "التحقق من الرقم" حيث تُغني عن استخدام طريقة استيقان أخرى مثل رمز التعريف الشخصي لمرة واحدة (OTP) وكلمة المرور، وتتحقق بدلاً من ذلك من تفاعل المستعمل مع الخدمة من جهاز يحمل رقم الهاتف المتنقل المسجل مسبقاً/المقترن. وتُستخدم عمليات "اعرف عميلك" (KYC) بشكل متزايد لتوفير عملية إدخال أكثر أماناً، بما في ذلك الخدمات المالية المتنقلة، من خلال التحقق من صحة معلومات اتصال المستعمل والحد من سرقة الهوية.

وتُشغّل شركة **تيلسترا**، أكبر مُشغّل اتصالات في أستراليا، مُرشّحاً لرسائل الاحتيال عبر خدمة الرسائل القصيرة لمسح محتوى الرسائل، والبحث عن الأنماط والخصائص المُريبة، ثم تحديد الرسائل الخبيثة التي تحتوي على روابط أو أرقام هواتف مُريبة وحظرها.[149] كما يُشارك موردو خدمات الاتصالات مع القطاع المصرفي للتصدي لعمليات الاحتيال عبر الهاتف. فعلى سبيل المثال، أطلقت شركة **أوبتوس**، ثاني أكبر مُشغّل اتصالات في أستراليا، مبادرة "إيقاف المكالمات" بالتعاون مع بورصة الجرائم المالية الأسترالية وأعضاء البنوك، بما في ذلك البنوك الكبرى.[150] ويستهدف البرنامج عمليات الاحتيال عبر معاودة الاتصال، حيث يمنع عملاء أوبتوس من الاتصال برقم الاحتيال المُحدّد، ثم يُحوّل المكالمة إلى رسالة آلية لتحذيرهم من مخاطر الاحتيال. كما تُزوّد البنوك ومُشغّلو الاتصالات المستعملين بالطرق الوقائية لتوحيد جهود مكافحة الاحتيال عبر خدمة الرسائل القصيرة والاحتيال عبر الاتصالات.

وتُسهّل الرابطة **GSMA** التعاون وتبادل المعلومات من خلال فريق عمل الاحتيال والأمن (FASG) [151] ومركز تبادل وتحليل معلومات الاتصالات (T-ISAC).[152] وكلاهما منصتان آمنتان تُسهّلان تبادل المعلومات في الوقت الفعلي على نطاق عالمي.

وتتطلب جهود مكافحة الاحتيال عبر خدمة الرسائل القصيرة وعمليات الاحتيال عبر الاتصالات شراكات قوية بين جميع أصحاب المصلحة. فالحكومة وحدها لا تستطيع عرقلة أنشطة الاحتيال. وبعد تسجيل هيئة الاتصالات والإعلام الأسترالية وإنفاذها لقواعد تحديد وحظر مكالمات الاحتيال في ديسمبر 2020، ورسائل الاحتيال النصية

145 https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/7726-reporting-scam-texts-and-calls/ ؛ https://www.getcybersafe.gc.ca/en/blogs/reporting-spam-text-messages-7726

146 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/393 المقدمة من المملكة المتحدة

147 https://www.gsma.com/newsroom/press-release/mobile-and-banking-industries-join-forces-to-fight-fraud/

148 https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/social-engineering-and-impersonation-fraud/; https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/05/Mobile-Money-Fraud-Typologies-and-Mitigation-Strategies-20.05.24.pdf

149 وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/154 المقدمة من أستراليا

150 المرجع نفسه.

151 https://www.gsma.com/get-involved/working-groups/fraud-security-group/

152 https://www.gsma.com/solutions-and-impact/technologies/security/t-isac/

في يوليو 2022، أفاد موردو خدمات الاتصالات بحظر أكثر من 1,4 مليار مكالمة احتيال وأكثر من 257 مليون رسالة احتيال حتى نهاية يونيو 2023.[153]

وعلاوةً على ذلك، ينبغي النظر في تنظيم حملات إعلامية عامة بشأن الإبلاغ عن عمليات الاحتيال من أجل زيادة عدد البلاغات. ففي **المملكة المتحدة**، أعلنت بعض المنظمات، مثل المركز الوطني للأمن السيبراني وبعض قوات الشرطة المحلية، عن وجود خدمة الإبلاغ عبر الرقم 7726، كما وضعت Ofcom، هيئة تنظيم الاتصالات، تعليمات مبسطة على شكل فيديو تعليمي خطوة بخطوة، توضح فيه كيفية الإبلاغ عن الرسائل النصية والمكالمات إلى الرقم 7726 على معظم نماذج الهواتف الذكية الرئيسية. وفي الآونة الأخيرة، أدى إدخال زر للإبلاغ عن الرسائل الاقتحامية في الغالبية العظمى من الهواتف الذكية في سوق المملكة المتحدة إلى زيادة كبيرة في معدل الرسائل الاقتحامية المبلغ عنها، حيث تعمل هذه الوظيفة الجديدة بنفس طريقة إبلاغ الخدمة عبر الرقم 7726، مع تقاسم المعلومات مع مشغلي الاتصالات المتنقلة من خلال قاعدة بيانات مشتركة تابعة لجهة خارجية. وقد أدى هذا التغيير إلى زيادة في عدد البلاغات بنسبة تقارب 800 في المائة خلال عام واحد.[154]

ونظراً لأن الإجراءات المتخذة حتى الآن حققت نتائج إيجابية، ينبغي النظر في اتباع نهج شامل يشمل مختلف أصحاب المصلحة بما في ذلك الجهات الحكومية والبنوك وشركات تشغيل الاتصالات، بالإضافة إلى المستعملين

[153] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/154 المقدمة من أستراليا
[154] وثيقة لجنة الدراسات 2 لقطاع تنمية الاتصالات 2/393 المقدمة من المملكة المتحدة

الخلاصة

لقد كان لاستخدام الاتصالات/تكنولوجيا المعلومات والاتصالات دورٌ بالغ الأهمية في تعزيز التنمية والنمو الاجتماعي والاقتصادي عالمياً. ويُعدّ تأمين شبكات المعلومات والاتصالات وتطوير ثقافة الأمن السيبراني أمراً بالغ الأهمية في عالم اليوم، لا سيما مع تزايد اعتماد واستخدام الاتصالات/تكنولوجيا المعلومات والاتصالات. وخلال فترة الدراسة هذه، تناولت المسألة 3/2 جوانب عديدة للأمن السيبراني، حيث نظرت في مساهمات أعضاء الاتحاد، وعقدت ورشتي عمل استرشد بهما هذا التقرير وخلاصته.

وكشف الفصل الأول أن مبادرات التوعية بالأمن السيبراني تراوحت بين برامج شاملة تستهدف شرائح سكانية مختلفة، وتدخلات محددة تُركز على مواضيع مثل نظافة الأمن السيبراني والتوعية من عمليات الاحتيال. وبالمثل، كشفت سياسات الدول الأعضاء في مجال التثقيف والتدريب في مجال الأمن السيبراني عن مستويات متفاوتة من النضج. فقد نفذت بعض البلدان استراتيجيات متكاملة تهدف إلى الحد من نقص المتخصصين في مجال الأمن السيبراني، بينما اختارت بلدان أخرى حلولاً تدريبية أكثر تخصصاً تستهدف فئات من قوة العمل. وقد شددت الدول الأعضاء، عن حق، على مبادرات حماية الأطفال على الإنترنت، من خلال تطبيق أطر قانونية متينة، وتطوير أدوات وبرامج عملية لجعل الإنترنت أكثر أماناً للأطفال.

وتناول الفصل الثاني مجموعة واسعة من ممارسات ضمان الأمن السيبراني التي برزت كعنصر حاسم في حماية الشبكات والأنظمة والبيانات من الأنشطة الضارة. ورغم أنها لا تمنع الهجمات السيبرانية بشكل مباشر، فإن هدفها، إذا طُبقت بشكل صحيح، هو تدنية مخاطر هذه الهجمات. وبينما لا يوجد نهج واحد يُوصى به، فقد أظهرت عينة المبادرات تحولاً مستداماً نحو اعتماد هذه الممارسات في جميع أنحاء العالم، حيث غالباً ما تستخدم السلطات الوطنية مناهج مختلفة ومختلطة، تتراوح من التقييمات الذاتية والمبادئ التوجيهية الطوعية وصولاً إلى مخططات الوسم وفحوصات الامتثال الصارمة.

وسلط الفصل الثالث الضوء على الدور الأساسي الذي تقوم به أفرقة الاستجابة للطوارئ الحاسوبية في زيادة القدرة على الصمود السيبرانية لأي بلد. وينبغي إعطاء الأولوية لإنشاء هذه الأفرقة وتشغيلها في البلدان النامية. ويمكن للاتحاد أن يقدم تقييمات أفرقة الاستجابة للطوارئ الحاسوبية وتطويرها للبلدان التي تهدف إلى زيادة قدرات أفرقتها من أجل تعزيز قدرة البنى التحتية الحرجة على الصمود.

وناقش الفصل الرابع نُهُج وتجارب خرائط الطريق الوطنية التي يمكن أن تُرشد تعزيز أطر الأمن السيبراني الوطنية. وأكد أنه في حين أن مشهد التهديدات السيبرانية يتطور باستمرار، فإن المبادئ الأساسية للتخطيط الشامل، والمشاركة الشاملة لأصحاب المصلحة، والقدرة على التكيف الاستباقي تظل أساسية لنجاح تنفيذ استراتيجية الأمن السيبراني. وفي المستقبل، ستواصل هذه المبادئ تشكيل دفاعات الأمن السيبراني القادرة على الصمود اللازمة لحماية المصالح الوطنية في عالم موصول.

وركز الفصل الخامس على تدابير الأمن السيبراني لتأمين شبكات الجيل الخامس. وقد وُضعت معايير ومواصفات في مختلف المنظمات المعنية بوضع المعايير والمجموعات الصناعية، وينبغي أن يُستكمل تطبيقها بتدابير استباقية للأمن السيبراني من جانب البائعين والمشغلين، بالإضافة إلى السياسات واللوائح الوطنية. ويمكن أن تتخذ هذه التدابير أشكالاً مختلفة تبعاً للسياقات الوطنية، بما في ذلك تقييم البائعين، والاختبار، وإصدار الشهادات، ووضع المبادئ التوجيهية أو المتطلبات.

وأخيراً، تناول الفصل السادس الجهود المبذولة لمكافحة عمليات الاحتيال عبر الاتصالات، مع التركيز على الاحتيال عبر خدمة الرسائل القصيرة، وشدد على الحاجة إلى شراكات قوية بين القطاعين العام والخاص. وسلط الفصل الضوء على أمثلة ناجحة لمبادرات للحكومات والصناعة في التصدي لتزايد الاحتيال عبر خدمة الرسائل القصيرة. كما أشار الفصل إلى أن توعية المستعملين وتثقيفهم أمراً بالغ الأهمية، لا سيما مع تزايد تعقيد هذه الهجمات وصعوبة اكتشافها.

أما بالنسبة لمستقبل المسألة 3/2، فطالما استمر تطور مشهد الأمن السيبراني العالمي، ستظل الحاجة إلى تبادل المعلومات والنُهُج المتعلقة بالأمن السيبراني حيوية. وهناك مزايا في الإبقاء على هذا الموضوع في فترة الدراسة القادمة، مع مراجعة الاختصاصات التي تُركز بشكل أكبر على قضايا محددة في مجال الأمن السيبراني، بما يعكس ولاية وجمهور لجنة دراسات قطاع تنمية الاتصالات.

Annexes

Annex 1: List of contributions and liaison statements received on Question 3/2

Contributions for Question 3/2

Web	Received	Source	Title
2/408	2025-04-29	RIFEN	Securing contractualization and deed production during the real estate sales process via blockchain technology and machine learning: practices and use cases
Describes the integration of blockchain technology and machine learning solutions for securing real estate transactions. Together, these technologies strengthen stakeholder confidence, while improving the efficiency of real estate transactions. This contribution takes into account existing work and provides an overview of the system we have implemented in Cameroon for the sale of real estate.			
2/405	2025-04-28	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
This contribution provides an update on the activities currently being undertaken by BDT to enhance cybersecurity in ITU Member States. It also highlights future actions envisaged and new initiatives being formulated.			
2/393	2025-04-23	United Kingdom	Scam reporting within the UK
Summarises how the largest mobile operators in the United Kingdom voluntarily provide the 7726 reporting service, as a way of identifying, removing, and preventing scams calls and messages.			
2/392	2025-04-2025	RIFEN	Developing countries: strengthening cybersecurity
Describes how developing countries face multiple and complex cybersecurity challenges, but with limited means to address the question of how they can ensure that disparities in technical capabilities and funding do not hamper their efforts to enhance cybersecurity.			
2/370	2025-04-14	China	Jointly building cybersecurity: typical practices of safeguarding cyberspace security
Provides an overview of the laws and regulations enacted by China to safeguard cyberspace security, the national campaigns launched to raise people's awareness of cybersecurity, as well as the international initiatives proposed by China on cybersecurity, with the aim of providing reference practices and paths for the world to build secure cyberspaces together.			
2/350	2025-02-27	RIFEN	Artificial intelligence for the detection and reporting of online cyberbullying
Presents the challenge to combat online harassment and the opportunity to integrating artificial intelligence, particularly deep learning techniques, as a promising avenue for improving the protection of sensitive data. The contribution highlights the advantages of designing an intelligent system capable of proactively and automatically identifying threats by combining advanced analysis techniques with proactive cybersecurity strategies.			
2/346	2025-02-04	Tanzania	Best practices for coordinating efforts and developing cybersecurity culture
Highlights good practices for coordinating efforts to promote a culture of cybersecurity in Tanzania. It outlines how various legal, technical, organizational, and capacity development measures, along with cooperation, have been vital in enabling Tanzania to achieve a "Tier 1" ranking and be recognized as a "role model" in the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU). It also identifies areas for continuous improvement, especially in technical and capacity development measures.			
2/TD/10 +Ann.1	2024-11-12	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States

(تابع)

Web	Received	Source	Title
Reports on the recently conducted CIRT Maturity Assessments in Azerbaijan, Bhutan, Sierra Leone, and Tanzania, the cyberdrills carried out in 2024 to enhance incident response readiness across different regions, the launch of the 5th edition of the Global Cybersecurity Index, BDT assistance in countries and territories in the assessment of their cybersecurity strategies, the Women in Cyber Mentorship Programme and the Her CyberTracks programme, the launch of new online safety tools for children and ongoing capacity building efforts, and other initiatives.			
2/339	2024-11-07	Republic of the Congo	Online communication and transactions via new and emerging telecommunications/ICTs, such as the Internet of Things (IoT)
Outlines challenges in consumer protection with the rise of IoT technology. It highlights issues with data protection, privacy, fair business practices, and device security. Various international responses include legislation, certification, monitoring, and technical standards to safeguard consumer rights and ensure device security.			
2/329	2024-10-29	Egypt	Egypt capacity building centre for African countries (EG-ATRC)
Details Egypt's dedication to enhancing African nations' communication and information technology skills via the Egyptian African Telecom Regulatory Training Centre (EG-ATRC), providing ITU-accredited training and hosting 381 participants from 30+ countries.			
2/322	2024-10-29	NRD Cyber Security	Strengthening cyber resilience: the role of Lithuania's national CIRT in critical infrastructure protection
Presents a case study on Lithuania's National Computer Incident Response Team within the National Cyber Security Centre, highlighting its functions in critical infrastructure protection through monitoring, incident handling, threat analysis, and collaboration efforts, including European Union initiatives.			
2/320	2024-10-29	Australia	Mandating a minimum standard for consumer-grade smart devices
Describes Australia's transition to mandatory smart device security standards from voluntary security standards, prompted by poor guideline adoption. A Bill proposes enforceable Internet of Things standards, requiring compliance statements from manufacturers and suppliers, and introduces a regulatory model with update flexibility.			
2/312	2024-10-28	Republic of Korea	Challenges and approaches to addressing smishing and SMS incidents in South Korea
Examines smishing threats in the Republic of Korea, detailing the Ministry of Science and ICT and Korea Internet & Security Agency countermeasures, challenges, and government strategies such as AI detection, awareness campaigns, and international cooperation, with recommendations for improvement.			
2/309	2024-10-25	Albania	Creation of a safer cyber ecosystem in a country: the case of Albania
Summarizes Albania's post-cyberattack cybersecurity reforms, including legal and strategic updates, new operations centres, human capital investment, and enhanced international cooperation with entities like the UN and NATO, leading to stronger legal frameworks and preparedness.			
2/301	2024-10-22	China	Mobile anonymous subscription service based on data security protection
Proposes a service for user privacy protection by using temporary numbers and anonymous IDs, with a focus on balancing privacy and digital economy growth, detailing a system architecture that ensures availability, scalability, reliability, usability, observability, and audit logs.			
2/300	2024-10-22	China	Based on anonymous data exchange network, release the value of telecommunications data

(تابع)

Web	Received	Source	Title
Examines the importance of telecommunications data in the digital economy and the challenges of using it, such as privacy issues and integration with Internet data. It details the China Academy of Information and Communications Technology creation of an anonymous data network, enhancing financial risk management and advertising, and supporting sustainable growth and employment in line with the United Nations Sustainable Development Goals.			
2/299	2024-10-22	China Telecommunications Corporation	Building security capabilities to alert phishing websites
Outlines the difficulties the elderly encounter with digital threats such as phishing, and details the China Telecom security tool, which shields them through gateway plug-ins, cloud engines, and a security database, serving over 10 million users in 31 provinces.			
2/276	2024-09-30	Côte d'Ivoire	Cybersecurity in action: strategies and challenges in a connected world- experience of Cote d'Ivoire
Presents the "O'KOHI" web series by a Platform for the Fight against Cybersecurity (PLCC), designed to educate on cybersecurity via videos. Funded by ARTCI and the *Ministère de l'Economie Numérique, des Télécommunications et de l'Innovation*, it addresses hacking, data protection, and cyberattacks, ensuring content accuracy through expert collaboration.			
2/273	2024-09-29	RIFEN	Machine learning-based CVE and CWE analysis
Highlights the need for machine learning to automate Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) analysis, improve identification and prioritization of software vulnerabilities, and overcome challenges such as data quality and model complexity through solutions including data validation and continuous learning. It advocates for collaboration to enhance cybersecurity.			
2/271	2024-09-29	RIFEN	Cybersecurity and cyberspace protection in developing countries
Examines the Internet and information and communication technology impact on Africa's socio-economic progress, addressing cyberattack risks and the necessity for collaborative security efforts. It discusses Africa-specific challenges, infrastructure vulnerabilities, and advocates for a multi-stakeholder strategy to safeguard essential Internet resources.			
2/268	2024-09-24	RIFEN	Cybersecurity awareness for rural youth through online training organized by RIFEN-SADA
Outlines the RIFEN-SADA (Smart Africa Digital Academy) cybersecurity training, which enhanced awareness and skills in cybersecurity among young Africans through fourteen modules. It fostered a security-conscious culture, practical protection knowledge, and guided talent development, leading to certifications and improved job prospects.			
2/254	2024-09-19	Co-Rapporteur for Question 6/1; Co-Rapporteur for Question 3/2	Report of the workshop on Increasing Consumer Awareness Mechanisms to Promote Informed Consumer Decision: A joint workshop for Question 6/1 and Question 3/2 held in Brasilia from 18-20 June 2024
Presents the workshop on consumer protection in the digital age, discussing infrastructure in underserved regions, security, digital literacy, and data privacy. It stressed digital inclusion, consumer behaviour, and skill gaps, concluding with good practices for ITU deliverables.			
2/246	2024-09-16	RIFEN	Securing the contracting procedure and the production of deeds of purchase in the real estate sale process using blockchain technology and machine learning

(تابع)

Web	Received	Source	Title
Discusses how blockchain technology and machine learning are revolutionizing the real estate industry by enhancing security, efficiency, and decision-making in the sales process. It highlights the benefits of smart contracts and improved market analysis, while acknowledging the challenges of adoption and regulation.			
2/242	2024-09-12	Central African Republic	Operationalization of CSIRT/SOC/PKI platforms and training
Outlines the Central African Republic's cybersecurity measures post-broadband expansion, including the deployment of a Security Operations Centre- Computer Security Incident Response Team (SOC-CSIRT) and public key infrastructure (PKI) systems, and requests Union support for network security.			
RGQ2/218	2024-04-29	Australia	National Office of Cyber Security and the Cyber Security Response Coordination Unit
Presents the Cyber Security Response Coordination Unit, the National Office of Cyber Security and the National Cyber Security Coordinator, entities established by the Government of Australia within the Department of Home Affairs for central coordination, following the Optus and Medibank data breaches of 2022.			
RGQ2/214	2024-04-19	Australia	Critical Infrastructure Uplift Program (CI-UP)
Outlines the Critical Infrastructure Uplift Programme (CI-UP) in Australia, designed to enhance cyber security and resilience of critical infrastructure against cyber-attacks. It details CI-UP activities and emphasizes the voluntary and collaborative nature with industry partners.			
RGQ2/212	2024-04-18	China Mobile Communications Co. Ltd.	China's initiatives to protect the cyber-security rights and interests of minors
Presents the critical nature of cybersecurity for Chinese minors, addressing their high online presence, urban-rural digital divide, and exposure to risks such as addiction and privacy violations. It underscores China's advancements in safeguarding minors' Internet use and the collective role of government, industry, and society in bolstering cyber-security education and safety.			
RGQ2/201	2024-04-16	Saudi Arabia	Cost estimation tool for cybersecurity controls
Outlines the National Cybersecurity Authority (NCA) development of the "ECC Cost Estimation Tool" to aid Saudi organizations in budgeting for cybersecurity compliance. It details the creation process, including research, implementation and testing phases.			
RGQ2/191	2024-04-16	United Kingdom	Considerations in implementing a new and significant regulatory security framework for the telecoms sector: an example from the UK's Telecoms Security Act (TSA)
Outlines the United Kingdom new telecoms security framework under the Telecommunications Security Act 2021, detailing enhanced security duties for providers, a tiered approach based on turnover, and the Ofcom role in ensuring compliance and fostering a collaborative security culture.			
RGQ2/184	2024-04-15	Brazil	Creating cybersecurity capabilities: Hackers do Bem
Describes Brazil's "Hackers do Bem" ("White Hat Hackers") initiative, aiming to train 30 000 students in cybersecurity through a five-level curriculum, with government support, to build a national hub, boost employability, and strengthen the cybersecurity ecosystem.			
RGQ2/183	2024-04-15	Brazil	Cybersecurity in Brazilian National Research and Education Network: CAIS
Outlines the work of the Brazilian National Research and Education Network (RNP), which created the first network security centre in Brazil in 1995 (CAIS). CAIS serves as CSIRT for the Brazilian academic network, being the focal point for security incident notifications and providing coordination and support for the incident handling.			

(تابع)

Web	Received	Source	Title
RGQ2/182	2024-04-15	Brazil	Brazilian Federal Cyber Incident Management Network
Presents the Brazilian Federal Cyber Incident Management Network (ReGIC), presenting the two CSIRTs with national responsibilities, such as the Brazilian National Computer Emergency Response Team (CERT.br) and the Centre for Prevention, Treatment and Response to Government Cyber Incidents (CTIR Gov), as well the CSIRT ecosystem in Brazil.			
RGQ2/181	2024-04-15	Brazil	Brazilian National Cybersecurity Policy
Summarizes Brazil's National Cybersecurity Policy and the formation of the National Cybersecurity Committee, detailing its principles, goals, and tasks like promoting cybersecurity, resilience, education, and global collaboration, with diverse members overseeing policy execution.			
RGQ2/170	2024-04-04	Russian Federation	Implementation of the educational project "Digital Literacy Campaign" in the Russian Federation
Outlines the Russian Federation's "Digital Economy" programme for human capital and economic growth by 2024, including "Digital Literacy Campaign" with partners like Kaspersky Lab to educate children on digital safety through animated videos.			
RGQ2/165	2024-04-02	Brazil	Meaningful connectivity
Summarizes the Anatel 2023 Strategic Planning, highlighting digital transformation and meaningful connectivity, which encompasses a cyber safety perspective. It details cyber hygiene initiatives, including the launch of a dedicated page to combat digital scams and frauds.			
RGQ2/164	2024-03-29	United States	U.S. Pre-Ransomware Notification capability
Details the CISA Pre-Ransomware Notification programme to pre-empt ransomware attacks. It emphasizes early warnings, international cooperation, and the success of the #StopRansomware campaign in averting threats in 2023.			
RGQ2/163	2024-03-26	Syrian Arab Republic	A paper on digital development in Syria and the current reality
Summarizes the Syrian Arab Republic digital transformation strategy for government services, detailing a phased approach from 2021 to 2030, encompassing e-government services, citizen centres, and cybersecurity. It includes strategic axes, programmes, and annexes on Internet capacity and security.			
RGQ2/160	2024-03-26	RIFEN	Initiatives to strengthen digital trust in Côte d'Ivoire
Highlights Côte d'Ivoire's National Digital Development Strategy 2021-2025, aiming to transform the nation into West Africa's digital hub by improving digital skills, cybersecurity, and women's tech inclusion, and by creating a national data centre.			
RGQ2/155	2024-03-26	RIFEN	Building a resilient security culture: a comprehensive approach to cybersecurity enhancement
Highlights the need for a robust cybersecurity culture in organizations, advocating for comprehensive strategies such as employee training, simulations, incident response teams, access control, encryption, and continuous monitoring to combat cyber threats.			
RGQ2/149	2024-03-15	Democratic Republic of the Congo	Development of cybersecurity in the Democratic Republic of Congo: issues and strategies for the protection of ICT infrastructures and digital actors
Outlines the Democratic Republic of the Congo's cybersecurity challenges, including its vulnerability to cyberattacks and the lack of a national strategy, legal framework, and incident reporting. It mentions a workshop for creating a national CIRT and ITU strategy support.			

(تابع)

Web	Received	Source	Title
RGQ2/140	2024-03-11	RIFEN	Internet and ICT: development levers and cybersecurity challenges in developing countries
Highlights the importance of Internet and ICTs for development, stressing security against cyberthreats. It combines research with expert opinions, identifies vulnerabilities, and addresses Africa's connectivity issues, advocating for information sharing, legislation, and collaboration to protect digital infrastructure.			
RGQ2/134	2024-03-05	Burundi	Implementation of a national cybersecurity strategy
Outlines the significance of information management and ICTs for a country's progress, emphasizing the necessity of cybersecurity measures in light of rising cybercrime. It details Burundi's efforts, supported by ITU, to create a national cybersecurity strategy by 2040, concentrating on legal structures, infrastructure security, and skill development.			
RGQ2/130	2024-02-29	RIFEN	Côte d'Ivoire's cybersecurity initiatives
Outlines Côte d'Ivoire's cybersecurity strategies, including the Platform for Combating Cybercrime and CI-CERT, stressing public awareness and education to foster a cybersecurity culture and safeguard the online space, particularly during events like the African Cup of Nations.			
RGQ2/128 +Ann.1	2024-02-29	Syrian Arab Republic	Cybersecurity strategy in Syria
Summarizes the Syrian Arab Republic cybersecurity strategy, focusing on creating a strong infrastructure, handling threats, legal development, capability enhancement, research, governance, and international collaboration via six programs, while stressing the importance of multi-layered protection.			
RGQ2/121	2024-02-29	Haiti	Taking control of cybersecurity in Haiti
Outlines Haiti's Haitian Institute for Statistics and Information and the CONATEL partnership to create a national cybersecurity strategy, aided by the World Bank and Inter-American Development Bank, including forming a working group, evaluating cybersecurity maturity, and establishing a CERT to enhance digital security.			
RGQ2/117 +Ann.1	2024-02-28	Dominican Republic	Cyberskills Center for Latin America and the Caribbean LAC4: Knowledge exchange, training and training in best practices at LAC4
Describes how the Latin America and Caribbean Cyber Competence Centre has enhanced cybersecurity in over 25 Latin American and Caribbean countries through workshops, legal framework support, and promoting regional cooperation, including empowering women and raising cyber awareness.			
RGQ2/114 +Ann.1	2024-02-27	Zambia	The role of the Authority in Child Online Protection in Zambia: A Zambia case study on the implementation of the National COP Strategy- Lessons learnt
Summarizes Zambia's dedication to child online safety by adopting ITU Resolution 179 and executing a national child online protection strategy, focusing on legal frameworks, education, combating exploitation, stakeholder cooperation, and ensuring effective oversight.			
RGQ2/104	2024-01-24	Democratic Republic of the Congo	Making Congolese cybersecurity a lever for integration and socio-economic growth
Describes the Democratic Republic of the Congo's strategy for using cybersecurity to enhance integration, governance, and growth, focusing on infrastructure, cybercrime, and digital services. It advocates for expert capacity building and ITU partnership for a secure digital transformation.			
2/212	2023-10-31	Republic of Korea	Misuse of Personally Identifiable Information

(تابع)

Web	Received	Source	Title
Presents the Republic of Korea's data protection mechanism that has been updated to address concerns related to the misuse and abuse of personal identifiable information (PII). The Personal Information Protection Act (PIPA) amended the existing PII Anonymization Guidelines on 28 April 2022, which aim to offer six step-by-step guidelines for the treatment (de-identification) of personal information. The Republic of Korea highlighted the challenge of crafting guidelines that guard against the abuse and misuse of PII without jeopardizing the benefits of new technologies.			
2/201	2023-10-17	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Discusses ongoing efforts to improve cybersecurity in ITU Member States, including future plans and new initiatives as well as how the Global Cybersecurity Agenda, launched in 2007, promotes international cooperation, and how BDT works with Member States and global organizations to establish national and regional CIRTs, measures cybersecurity commitments, supports strategy development, encourages diversity, and works to protect children online through the child online protection initiative.			
2/199	2023-10-17	United Kingdom	Building local capacity to adopt secure connected place technology: the UK's Secure Connected Places Playbook
Recognizes the benefits that connected places ("smart cities") technology can bring societies and local areas. However, it also recognizes that this interconnectivity creates cyber vulnerabilities and the potential for cyberattacks. Through its National Cyber Strategy 2022, the United Kingdom has been developing a 'Secure Connected Places Playbook'. This product, currently in alpha phase, has been developed in partnership with a diverse set of local government authorities and an industry consortium. The Playbook provides guidance on: i) governance; ii) procurement and supply chain management; and iii) risk and threat analysis. The United Kingdom has identified several good practices, including: i) working hand-in-hand with intended beneficiaries; ii) using a "test and iterate" approach; and iii) co-developing and testing with local government authorities. The United Kingdom has now begun beta testing, working with 13 local authorities.			
2/196	2023-10-17	United States	U.S. proposed Cyber Trust Mark Program: certifying that IoT products meet U.S. cyber standards
Presents the proposed Cyber Trust Mark program, by the United States Federal Communications Commission (FCC), a voluntary cybersecurity labelling initiative for IoT products. The programme aims to help consumers make informed decisions, differentiate trustworthy products, and encourage manufacturers to meet higher cybersecurity standards. The FCC seeks input on various aspects of the programme, including eligible devices, oversight, security standards, and consumer education. Certified products could be available for purchase by the end of 2024.			
2/187	2023-10-16	Republic of Korea	Privacy by Design certification in South Korea
Shares its contribution on Privacy by Design (PbD), a proactive approach to embedding privacy into the design and operation of information technologies and systems. The Personal Information Protection Committee (PIPC) of the Republic of Korea is piloting a PbD certification system to strengthen the safety of personal information collection devices. The certification helps organizations demonstrate their commitment to user privacy, increasing consumer trust and reducing the risk of privacy breaches.			
2/167	2023-10-11	Australia	eSafety Youth Council
Presents the eSafety Youth Council, established in April 2022, that consists of 24 members aged 13-24 from diverse backgrounds in Australia. It aims to involve young people in decision-making processes for policies and programmes impacting them. The Council is informed by the Western Sydney University Youth Engagement Report and follows six good practice principles. Members engage in various activities, including conferences, resource launches, and discussions with technology companies. The Council priorities include collaboration, improved reporting processes, age-appropriate content access, and increased engagement on online safety.			
2/158	2023-10-09	Russian Federation	Challenges and approaches to addressing smishing and SMS incidents. Combating illegal use of virtual mobile numbers

(تابع)

Web	Received	Source	Title
Contextualize smishing as a type of phishing attack that uses SMS messages to trick users into downloading malware or revealing personal information. The rise of mobile services and the pandemic have increased its popularity. To combat smishing, users should be cautious of unexpected messages, use anti-spam settings, and report suspicious messages. Governments, banks, and telecommunication operators are also working together to fight smishing through regulations, public awareness campaigns, and technological solutions.			
2/154	2023-10-05	Australia	Combating telecommunications scams
Presents the Australian Communications and Media Authority (ACMA) work to combats scams through regulatory powers, new rules, and international cooperation. Initiatives include varying the telecommunications numbering plan, registering the Reducing Scam Calls and Scam SMS Code, and mandating stronger identity verification processes. ACMA also collaborates with other nations and industries to fight scams. Despite progress, SMS scams remain a significant issue. A holistic approach involving industry, government, and consumer awareness is needed.			
2/150 +Ann.1	2023-09-29	Argentina	Promoting cybersecurity in Argentina: challenges, strategies and advances in the digital era
Presents the growing reliance on ICT for essential services highlighting the need for governments to prioritize cybersecurity. Challenges include fostering a cybersecurity culture and promoting safe cyberspace usage. Efforts include a National Cybersecurity Awareness Campaign, a joint publication on cybersecurity issues, training programmes for civil servants, strengthening legal frameworks, and addressing the gender gap in ICT access and use through national and international initiatives.			
2/141	2023-09-28	Central African Republic	Criminal aspects of physical protection of information and communication network infrastructures
Central African Republic shares the implementation of legislative reforms and creation of agencies to control and secure information systems. However, the country faces vandalism and theft on its new fibre optic network. Proposed solutions include adopting laws against theft, fraud, and vandalism in public information networks and establishing a national CIRT team to coordinate incident management.			
2/137	2023-09-14	Côte d'Ivoire	Cybercrime: Continuing campaign on child online protection
Discusses the digital knowledge challenge facing Côte d'Ivoire, that is hindering its development in the digital world. To address this, public and private sectors, along with international organizations, have launched an awareness campaign for middle and high school students. The campaign aims to educate and raise awareness about online risks, promote responsible digital behaviour, and provide support for reporting abuse. Over 1 000 students participated in the campaign, which emphasizes the importance of a safer digital environment for all citizens.			
2/120	2023-09-07	Timor-Leste	Advancing cybersecurity for Timor-Leste's digital transformation
Presents Timor-Leste digital transformation journey, focusing on improving government services, inclusivity, and crucial sectors such as healthcare, education, and agriculture. However, as a least developed country (LDC), it faces significant cybersecurity challenges, including weak frameworks, limited awareness, and inadequate resources. To enhance digital resilience, Timor-Leste must invest in infrastructure, capacity building, legal frameworks, public-private partnerships, awareness, incident response, and international cooperation. Addressing these challenges is crucial for sustainable development and economic growth in the digital era.			
2/119	2023-09-06	Kenya	The Authority's Child Online Protection and Safety Programme in Kenya: A case study on the implementation of the ITU's Guidelines on Child Online Protection

(تابع)

Web	Received	Source	Title
Shares the implementation of child online protection initiatives since 2011, by the Communications Authority of Kenya (CA), focusing on raising awareness and promoting responsible Internet usage. The CA has launched two campaigns, "Be The COP" and "*Huwezi Tucheza, Tuko Cyber Smart*," targeting parents, guardians, teachers, and children. The authority collaborates with various stakeholders, including government agencies, industry players, and NGOs, to implement the ITU Guidelines on Child Online Protection. Initiatives include legal and regulatory frameworks, reporting mechanisms, research and surveys, national strategies, industry initiatives, educational resources, capacity building, and national awareness campaigns.			
2/115	2023-09-04	Democratic Republic of the Congo	Digitalization of public services in the Democratic Republic of the Congo: key challenges and requirements for information security and cyberdefence
Presents the implementation of cybersecurity measures, including the enactment of Law No. 20/017 in 2020, and the adoption of a digital code in 2023. The country is working on creating a computer incident response team (CIRT) and improving its broadband infrastructure with a planned 50 000 km of optical fibre network. Cooperation and public awareness-raising are also essential components of their cybersecurity strategy.			
2/112	2023-08-21	Kenya	CSIRT/CIRT approaches and experiences towards the resilience of critical infrastructure in Kenya
Introduces the establishment of the National Computer Incidents Response Team (KE-CIRT) by the Communications Authority of Kenya to mitigate cyber threats and ensure a safer cyberspace. The country has a legal framework defining critical infrastructure and has adopted a cybersecurity framework supported by policy and operational frameworks. Challenges faced include a rapidly evolving threat landscape, lack of international cooperation, insufficient expertise, limited resources, balancing privacy and security, coordination and information sharing, technological advancements, insider threats, public-private collaboration, and public awareness and education.			
2/98	2023-07-25	Australia	Australia's national online safety awareness campaign
Introduces the Online Safety Act 2021, to keep pace with new technology and emerging online threats. The Online Safety campaign aimed to raise public awareness of the Online Safety Act and the strengthened laws for online safety. The campaign targeted various audience groups and successfully drove traffic to the eSafety Commissioner website.			
RGQ2/85	2023-05-18	Beihang University	Development of policies and legislation to protect consumer rights and interests in China in the digital era
China attaches great importance to the protection of consumer rights and interests. Firstly, in terms of policy guidance, the goal is to improve the consumer environment, strengthen consumer rights protection, and achieve social fairness and justice, adhering to the equal emphasis on development and regulation; Secondly, in terms of the legal system, China has steadily promoted the formulation and implementation of laws, regulations, and standards related to consumer rights protection. It has continuously strengthened the protection of consumers' digital rights and focused on the special protection of vulnerable consumers, gradually forming a comprehensive and three-dimensional legal system for consumer rights protection to adapt to the new development and needs of consumer rights protection. The content of this paper is based on the policy and legislative protection of consumer rights in China's new development pattern, so as to provide assistance for the international consumer rights protection cause.			
RGQ2/80	2023-05-10	Russian Federation	Information sharing practices to protect children from disruptive online content- Award "For a Safe Digital Childhood"
Presents its contribution which contained information on some practices on the exchange of information between two Russian Federation federal executive bodies to protect children from destructive online content, as well as information about the award "For a Safe Digital Childhood" by Alliance for the Protection of Children in the Digital Environment, aimed at supporting projects to develop a safe digital environment throughout the Russian Federation.			

(تابع)

Web	Received	Source	Title
RGQ2/79	2023-05-10	Russian Federation	National computer incident response and coordination centre- information security leaders
Presents a contribution on the operation of its National Computer Incident Response & Coordination Centre (NCIRCC) to ensure a stable critical infrastructure, as well as approaches regarding the appointment of leaders in the field of information security. In response to questions received during the meeting, the Russian Federation clarified that NCIRCC is not the only such centre, and the main criteria for leaders in the field of information security is not only their professional degree, but also wide-ranging experience and relevant professional skills.			
RGQ2/74	2023-05-09	United Kingdom	TBEST: an example of outcome-based pen-testing for communications providers to help improve their network security posture
Contribution on the TBEST scheme, an example of cybersecurity assurance practice that Ofcom, the United Kingdom regulator, runs voluntarily with communications providers. TBEST is a penetration testing that aims to stimulate a cyber-attack in telecommunications networks in order to identify security vulnerabilities which can then be, through a process of remediation, addressed to improve the operators' network security posture. The contribution provides an overview of the process, and the various stakeholders involved. More broadly, this scheme is an example of supervisory policy approach that Ofcom is taking, which stresses the importance of building collaborative relationships with the industry that Ofcom regulates. To date, all communications providers in the United Kingdom have already or are undergoing the TBEST scheme voluntarily and have implemented changes as a result. TBEST is not a "standard" nor a certification process. The goal is to enable communications providers to gain awareness of cyber threats and implement appropriate changes in a timely manner to improve their cyber defence capabilities. By being aware of, and addressing such vulnerabilities and weaknesses, the operator is in a much stronger position to protect their networks.			
RGQ2/66	2023-05-10	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Provides an update on the activities currently being undertaken to enhance cybersecurity in ITU Member States. It also highlights future actions envisaged and new initiatives being formulated. The presentation addressed the ITU cybersecurity mandate, and through BDT, work on the national CIRT programme, regional and national cyberDrills, the Global Cybersecurity Index (GCI), national cybersecurity strategy (NCS) assistance, Women in Cyber, Her CyberTracks, child online protection, partnerships and collaboration, and Cyber for Good. The document emphasizes the importance of collaboration, partnerships, and resource mobilization to allow ITU to fulfil its mandate, considering the extensive list of tasks that membership have requested BDT to undertake. BDT also presented information about the 5th edition of the Global Cybersecurity Index.			
RGQ2/58	2023-04-27	Brazil	Cybersecurity assurance practices- Brazil experience
Introduces the contribution referring to the efforts of the Brazilian National Telecommunications Agency (ANATEL) regarding the establishment of cybersecurity minimum requirements for telecommunication equipment. ANATEL initially adopted a non-mandatory approach (Act 77/2021), which evolved into a cybersecurity compulsory certification requirement for a specific set of equipment (Act 2436/2023). This evolution was only possible with a comprehensive debate within the sector.			
RGQ2/57	2023-07-27	Brazil	Brazilian cybersecurity-related policies and regulations
Presents an overview on the cybersecurity-related policies and regulations that have been developed in Brazil in recent years, including the National Information Security Policy, the National Cybersecurity Strategy, the Cybersecurity Regulation for the Telecommunication Sector, the Federal Cyber Incident Management Network, and the 5G Spectrum Auction Notice. There were questions about the modular approach adopted by the National Information Security Policy, and the Brazilian delegation explained that in Brazil cybersecurity is one of the elements of Information Security.			
RGQ2/53	2023-04-25	Mexico	Privacy reports on user information in the use of digital platforms

(تابع)

Web	Received	Source	Title
Presents the Privacy Reports, which purpose is to make available in a clear, simple and transparent manner the privacy policies of operating systems, terminal equipment, social networks, and digital platforms that enable the provision of services such as: online commerce, transport and entertainment. These reports published by the Federal Telecommunications Institute help users to learn about the information that is collected by the platforms, and how this information is treated, and helps users make responsible use of such platforms. The Reports also empower users by providing transparent information about privacy policies.			
RGQ2/51	2023-04-25	Mexico	Internet of Things Devices Catalog
The *Internet of Things Devices Catalogue* is an electronic tool that allows users of telecommunication services to know the main characteristics of IoT devices, as well as the privacy policies defined by the manufacturers. The IoT devices published are those that are marketed in Mexico and have been certified by the Federal Telecommunications Institute. The tool allows users to be empowered with transparent information about privacy policies and the characteristics of terminal equipment that comply with technical regulations, for informed decision-making and for the proper use of IoT equipment.			
RGQ2/48	2023-04-25	Access Partnership Limited	Cybersecurity assurance practices- international standards and satellite communications
Contains information related to developing cybersecurity assurance practices for commercial satellite operators, as well as highlighting some of the existing general cybersecurity assurance practices which may be adopted by any commercial satellite operator, including ISO 27001. The contribution noted some of the unique cybersecurity threats which need to be overcome in satellite operations, including the cross-jurisdictional nature of satellite operations, and the vulnerabilities of ground stations. The contribution explained specific technical standards including the ETSI technical standard 103 732 and its measures to protect consumer mobile devices, as an example of standards towards specific technology which could inform the further development of standards for commercial satellite operators.			
RGQ2/44	2023-04-24	South Africa	The domain name cybersecurity culture
Provides a contribution concerning the security of the country code top-level domain name (.za). The South African Domain Name Authority (ZADNA) manages the .za domain namespace under the mandate of the Electronic Communications and Transactions Act (ECTA). Its policy framework was designed to ensure a secure, resilient, and efficiently managed domain namespace, promoting stakeholder engagement, growth of the namespace, policy compliance, and entrance of new Internet service providers. ZADNA also addresses cybersecurity threats through education and awareness programmes, alternative dispute resolution (ADR) workshops and regulations, and DNS training courses. Additionally, it adheres to international standards for dispute resolution, working in line with the World Intellectual Property Organization (WIPO) and organizations such as the South African Institute of Intellectual Property Law (SAIIPL) and the Arbitration Foundation of Southern Africa.			
RGQ2/38	2023-04-13	Australia	Sharing advice from Australia on securing smart places
Shares information on the lessons learned by the Australian Cyber Security Centre in response to risks identified for smart places. The contribution defined smart places as those designed to provide enhanced services through the use of smart information and ICT enabled systems and devices. The contribution noted that the highly connected nature of smart places makes them vulnerable to intrusions. This is exacerbated when the system scales. The contribution gave examples of Australian policies used to protect the various aspects of smart cities including IoT, supply chains, operational technology and cloud computing. The contribution also raised several examples of strategies which may be employed to mitigate security risks as well as ensuring operational redundancy.			
RGQ2/34	2023-04-06	Republic of Korea	Cloud Security Assurance Program (CSAP) in South Korea

(تابع)

Web	Received	Source	Title
Introduces the Cloud Security Assurance Programme (CSAP), a security certification for cloud computing services that meet security certification standards to improve and guarantee information protection levels. The purpose of the CSAP is to provide private cloud services with proven safety and reliability to national and public institutions. Also, it aims to implement an objective and fair security certification system for cloud services to address user security concerns and secure competitiveness of cloud services. The CSAP provides a number of benefits. By certifying the security level of a cloud system, CSAP helps to improve the cyber resilience of national and public institutions. This can also help to ensure that sensitive information is protected and that cloud services are reliable.			
RGQ2/29	2023-03-30	Côte d'Ivoire	Policy and strategy of Côte d'Ivoire for building a trusted digital space
Shares the initiatives taken by Côte d'Ivoire in its efforts to build digital trust, which concerns all economic sectors that use ICTs, such as media and communication, transport, health, industry, telecommunications and computing, distribution of goods and consumption, construction, finance and insurance, tourism, agriculture and e-commerce. To consolidate the freedom of online public communication and ensure interactions are secure, Côte d'Ivoire has enhanced the means for combating cybercrime and protecting personal data in order to build trust in cyberspace. Cybersecurity has become an issue of privacy, competitiveness and national sovereignty. A capacity to anticipate, build trust and protect personal data is essential. In this sense, the country has updated its legal and institutional framework, setting a visionary policy to enhance digital trust by 2025. The country has established a Consultative Committee for Digital Trust (CCCN) and a Consultative Committee for the Protection of Personal Data (CCDCP).			
RGQ2/20	2023-03-22	Nigeria	Child Online Protection practices in Nigeria
Presents its efforts in regard to child online protection through the Nigerian Communications Commission (NCC), the independent national regulatory authority for the telecommunication industry, in collaboration with the Office of the National Security Adviser in Nigeria who works with other stakeholders to ensure child protection in Nigeria's cyber space. It was decided by the meeting to liaise with the Council Working Group on Child Online Protection (CWG-COP) to share the relevant experiences shared by Nigeria.			
2/80	2022-11-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
Provides an update on the activities currently being undertaken by BDT and new initiatives to enhance cybersecurity in ITU Member States: CIRT programme, regional and national cyberdrills, national cybersecurity strategy (NCS) , work related to Bridge the Cybersecurity Divide: Cyber for Good project, work on promoting a diverse and inclusive cybersecurity community through the Women in Cyber Mentorship Programme and Youth4Cyber initiative, child online protection, and partnerships and collaboration initiatives.			
2/77	2022-11-22	United Kingdom	Sharing experience from the UK on promoting and developing cybersecurity skills
Outlines the country's policy approach to address the cyber skills gap which, in addition to the final report of the study cycle, can also be included in a future repository of good practices as agreed through Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference. The United Kingdom's initiatives are focused in three areas: (1) cyber skills for young people, (2) cyber skills for adults, and (3) developing the cyber profession.			
2/74	2022-11-18	World Bank	World Bank Study Group 2 Submission: Digital transformation
Highlights their readiness to support the least developed client countries with a special emphasis on fragility, conflict and violence (FCV) and small island developing states (SIDS). Through the analytical work programme and strategic partnerships, the World Bank is working closely with client countries on issues related to the SG2 Questions' scopes. Relevant examples from the World Bank around using ICT services and applications for the promotion of transformative and sustainable development are provided in the contribution. For instance, one relating to cybersecurity is the Cybersecurity Multi-Donor Trust Fund, being a part of the broader Digital Development Partnership umbrella programme, aims at systematically incorporating cybersecurity in the development agenda as well as in World Bank operational programmes. Work includes building global knowledge to better define the cybersecurity development agenda, and country-specific technical assistance.			

(تابع)

Web	Received	Source	Title
2/71 (Rev.1)	2022-11-18	Russian Federation	New practices of the Russian Federation in the field of creating a culture of cybersecurity
Presents the Russian Federation Cyber Hygiene Program, launched in August 2022. The programme is planned for a three year period and includes various activities aimed at attracting the attention of citizens of the Russian Federation to the issues of cybersecurity and the training in skills on safe behaviour on the Internet. Large-scale information campaigns are one part of the programme. Citizens were segmented into age groups, and their online behaviour and the type of digital content consumed were taken into account. Based on this segmenting approach, more specifically targeted means of information dissemination could be applied for the 3 segmented groups of population (12-18 / 18-45 / 45+ years old). The contribution also covers the means of improving the information security literacy of civil servants, as well as the results of an all-Russian Federation study of the citizens' information security literacy.			
2/35	2022-10-12	Rwanda	National cybersecurity initiatives: current status
Highlights the programmes and initiatives put in place to guarantee the security and resilience of Rwanda's cyberspace. To support national economic growth and social mobility, the Government of Rwanda (GoR) is actively deploying various information technologies and has made major investments in ICT infrastructure and applications. GoR established the National Cybersecurity Authority (NCSA) as the authority to spearhead the implementation of National Cyber Security policies and strategies. Additionally, GoR established a law relating to protecting personal data and privacy and passed the prevention and punishment of cybercrimes law. NCSA roles include: coordinating national cybersecurity functions across the private and public sectors; promoting national education programmes and fostering awareness of cybersecurity good practices amongst the Rwandan population; operating the Rwanda Computer Security Incident Response Team (Rw-CSIRT); and overseeing the implementation of the Protection of Personal Data and Privacy Law. Furthermore, the Rwanda Utilities Regulatory Authority (RURA), Regulation No. 010/R/CR-CSI/RURA/020 OF 29/05/2020), Rwanda Information Society Authority (RISA), and capacity building collaborations and initiatives have been put in place to ensure preparation in preventing and responding to evolving cyber threats.			
2/34	2022-10-12	Côte d'Ivoire	Initiatives to support children and young people, national strategy for the protection and empowerment of children and young people online: the experience of Côte d'Ivoire
Presents an initiative undertaken by Côte d'Ivoire to protect children against the dangers and threats of using ICTs. The initiative, www.jemeprotegeenligne.ci is a website targeted at children between 5 and 19 years old as well as teachers and parents with the goal of educating children and young people and raising awareness.			
2/30	2022-10-11	Côte d'Ivoire	Proposal for State actions and initiatives to foster a culture of cybersecurity and ensure that information and communication networks are secure: the case of Côte d'Ivoire
Contextualizes cyberattacks and threats as a major concern for governments in this increasingly connected world, particularly in developing countries. Cybersecurity is now the priority issue for many States. This contribution gives an overview of the cybersecurity situation in developing countries, notably Côte d'Ivoire, and highlights strategies for raising user awareness and experience-sharing among Member States.			

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
2/410 +Ann.1	2025-04-30	ITU-T Study Group 17	Liaison statement form ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 LS on update on the work of the Correspondence Group on Child online protection (CG-COP)
2/409	2025-04-30	ITU-T Study Group 17	Liaison statement form ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on request to update security contacts and to provide information on security-related Recommendations or other texts under development
2/241	2024-09-11	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Groups 1 and 2 on SG17 update on the work of the Correspondence Group on Child online protection (CG-COP)
RGQ2/151	2024-03-18	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 1 Question 6/1 and ITU-D Study Group 2 Question 3/2 on Establishment of the Correspondence Group on Child online protection (CG-COP)
RGQ2/107	2024-02-12	Chairman, ITU Council Working Group on COP	Liaison statement from ITU Council Working Group on COP to ITU-D Study Group 2 Question 3/2 on child online protection
RGQ2/83	2023-03-08	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on status of security studies in ITU-T SG17
2/20	2022-06-16	ITU-T Study Group 17	Liaison statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on request to update security contacts and to provide information on security-related Recommendations or other texts under development

Annex 2: List and summary of BDT on-going cybersecurity activities

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Data	Global Cybersecurity Index v5	ITU Member States	GCI Expert Group	Global Cybersecurity Index report and country reports. Link
Governance	Capacity-building sessions for the cybersecurity ecosystem in Guinea-Bissau	Guinea-Bissau	Government of Guinea-Bissau	Capacity-building sessions for the cybersecurity ecosystem in Guinea-Bissau with the aim to empower Guinea-Bissau's cybersecurity ecosystem by guiding key national stakeholders in developing strategic approaches to CIRT implementation and enhancing cybersecurity in Guinea-Bissau
Governance	Mauritania's Cybersecurity Governance Development	Mauritania	Government of Mauritania	Sessions to enhance of a national cybersecurity governance framework to enable Mauritania to strengthen the protection of the critical information systems of official institutions and vital operators, the fight against cybercrime, awareness raising, training, confidence-building in digital, more effective regional and international integration through cooperation.
Governance	National cyber risk assessment	Lesotho	Ministry of Communications Science and Technology	Workshop to enhance strategic thinking on cybersecurity governance among key national stakeholders, thereby advancing the objectives of Lesotho's National Cybersecurity Strategy.
Governance	Strengthening Critical Information Infrastructure Resilience	Cambodia	Ministry of Post and Telecommunications Cambodia (MPTC, Japan International Cooperation Agency (JICA)	Workshops on technical incident response, national cybersecurity strategy, and crisis management for critical information infrastructure stakeholders
Governance	Tabletop Exercise and a Cybersecurity Incident Simulation Exercise	ITU Arab States region Member States	CSC UAE	Tabletop exercise centred around cyber-attack directed at a financial institution.
Incident Response	13th Event of Cyber Capacity Building in America - Andino	ITU Americas region Member States	Ministry of Popular Power for Science and Technology of Venezuela, National Commission of Information Technologies (CONATI), Superintendency of Electronic Certification Services (SUSCERTE)	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	Americas Regional CyberDrill	ITU Americas region Member States	INICTEL-UNI, Peruvian Ministry of Transportation and Communications, General Secretariat of the Andean Community	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	CIRT Establishment in Bahamas	Bahamas	Government of Bahamas	Building and deploying the technical capabilities and related training necessary to develop Bahamas national cybersecurity strategy and to establish its National Cybersecurity Incident Response Team (CIRT). Link

(تابع)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Incident Response	CIRT Maturity Assessment	Timor-Leste	ANC	Conducted Maturity Assessment of country CIRT through series of workshops, discussions, and inventories, providing recommendations for the Timor-Leste computer security incident response team (TLCSIRT) in collaboration with the Autoridade Nacional de Comunicações (ANC) to ensure TLCSIRT can enhance its cybersecurity maturity level. Link
Incident Response	Cyber 100x Global CyberDrill 2024	ITU Member States	Cyber Security Council United Arab Emirates	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	CyberQ	ITU Member States	United Arab Emirates Cybersecurity Council	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Included specific trainings for women. Link
Incident Response	Cybersecurity Forum and CyberDrill for Europe and the Mediterranean	ITU Europe region and Arab States region Member States	Ministry of Transport and Communications of Bulgaria, Ministry of Electronic Governance of Bulgaria	Cybersecurity forum featuring trends and challenges, CSIRTs capacity-building training, and two days of cyberdrill exercises with emerging attack scenarios and collaborative learning sessions. Link
Incident Response	ITU National CyberDrill for Armenia	Armenia	Ministry of High-Tech Industry of Armenia	Incident response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	ITU Regional Asia-Pacific CyberDrill	ITU Asia and the Pacific region Members States	Cyber Security Brunei (CSB)	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	ITU Regional Cybersecurity Readiness Exercise	ITU Arab States region Member States	Directorate General for Information Systems Security (DGSSI) Morocco	Incident response trainings, discussions, and information sharing. Link
Incident Response	National CIRT Establishment in Gambia	Gambia	Ministry of Information and Communication Infrastructure (MOICI)	Assist MOICI in building and deploying the technical capabilities and related trainings necessary to establish its national CIRT. Link
Incident Response	National Computer Incident Response Team (CIRT) Implementation – Suriname	Suriname	e-Government Directorate, Cabinet of the President of Suriname	Support for operationalization of Computer Incident Response Team. Link
Incident Response	Regional Cybersecurity Week	ITU Arab States region Member States	ARCC Oman	Regional Cybersecurity Conference focusing on "Cybersecurity as an enabler for the Digital Economy", the FIRST Organization Seminar, and the Regional and OIC-CERT Cyber Drill. Link
Incident Response	Rwanda National CyberDrill	Rwanda	Rwanda National Cyber Security Authority, Ministry of Foreign Affairs of the Czech Republic	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link
Incident Response	Twelfth Edition of the Regional Cyberdrill for Africa Region (ITU-INTERPOL CyberDrill)	ITU Africa region Member States	Ghana's Cyber Security Authority (CSA), INTERPOL	Incident Response trainings, discussions, and information sharing for cybersecurity professionals. Link

(تابع)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Partnerships	Cyber for Good	Least developed countries (LDCs)	Axon Consulting, BitSight Technologies, CTM360, DreamLab Technologies, ImmuniWeb, WelchmanKeen	Tools, trainings, and services offered for free to Least Developed Countries. Link
Skills Development	Child Online Protection National Assessment - Andorra	Andorra	SWGfL/UK Safer Internet Centre	Child Online Protection National Assessment with the national stakeholder consultation event
Skills Development	Child Online Protection Train the Trainers and Cybersecurity briefings - Maldives	Maldives	National Centre for Information Technology (NCIT)	Trainings on Child Online Protection as well as briefings on key topics. Link
Skills Development	Creating a Safe and Prosperous Cyberspace for Children	ITU Member States	CTO, CNIL, Council of Europe, European Commission, EC-Council, EBU, Europol, ILO, Interpol, MICITT, NCA KSA, OECD, United Nations Human Rights Special Procedures, UNICRI, UNESCO, UNICEF, UNODC, WIPO, World Bank, UC Berkley, LSE, Middlesex University London, Western Sydney University, Youth and Media, BBC, Disney, Ericsson, worldwide Group, Facebook, IBM, IEEE, Microsoft, Sony, TIM, Privately, Tencent, TrendMicro, Twitter, ASCSA, ACOPEA, 5Rights Foundation, ASDRA, Child Helpline International, Child Rights Connect, Family Online Safety Institute, Childhood, ChildOnline Africa, DeafKidz International, DISC Foundation, Families Europe, Halley Movement, End Violence Against Children, DOInstitute, ecpat, Fard Digital, HABLATAM, Cuber Coluntarios.org, Global Kids Online, GSMA, iKeepSafe, Inclusion international, InHope, Ins@fe, International Centre for Missing & Exploited Children, International Disability Alliance, Internet Matters, Internet Watch Foundation (IWF), Human Trafficking Front, ParentZone, Plan International, RNW media, Save the Children, Paniamor, Stiftung digitale chancen, SWGfL, Tech Coalition, terre des hommes suisse, United Kingdom Safer Internet Centre, WeProtect Global Alliance, Wise Kids, World Economic Forum, YouthIGF, Together Against Cybercrime	Advocacy, research, and in-country programmes related to Child Online Protection. Link

(تابع)

Activity type	Activity	Targeted / invited countries	Partners	Outputs
Skills Development	Her CyberTracks 2024	Algeria, Angola, Bahrain, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cabo Verde, Central African Republic, Comoros, Chad, Côte d'Ivoire, Democratic Republic of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Iraq, Jordan, Kenya, Kuwait, Lebanon, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Oman, Qatar, Republic of the Congo, Rwanda, São Tomé and Príncipe, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, State of Palestine*, Sudan, Syrian Arab Republic, Tanzania, Togo, Tunisia, Uganda, United Arab Emirates, Yemen, Zambia, Zimbabwe	GIZ, Microsoft	Her CyberTracks provides specialized, targeted training, maintaining the essential mentorship and role modelling aspects. The programme is poised to propel the next generation of women in cybersecurity into roles of leadership, ensuring that their voices and expertise shape the future of this critical field through training, mentorship, and inspiration across three tracks: Policy & Diplomacy, Incident Response, and Criminal Justice (implemented by UNODC). Link
Skills Development	Translation of Child online protection guidelines and capacity building activities - Albania	Albania	National Authority on Electronic Certification and Cyber Security	Child online protection guidelines translated into Albanian and the roll out of capacity-building activities
Skills Development	Translation of Child online protection guidelines and capacity building activities - Malta	Malta	SWGfL/UK Safer Internet Centre	Child online protection guidelines translated into Maltese and the roll out of capacity-building activities

Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland
البريد الإلكتروني: bdtdirector@itu.int
الهاتف: +41 22 730 5035/5435

Office of the Deputy Director
Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland
البريد الإلكتروني: bdtdeputydir@itu.int
الهاتف: +41 22 730 5131

Digital Networks and Environment Department (DNE)
البريد الإلكتروني: bdt-dne@itu.int
الهاتف: +41 22 730 5421

Digital Knowledge Society Department (DKS)
البريد الإلكتروني: bdt-dks@itu.int
الهاتف: +41 22 730 5900

Projects, Partnerships and Digital Skills Department (PPS)
البريد الإلكتروني: bdt-pps@itu.int
الهاتف: +41 22 730 5447

إفريقيا

إثيوبيا

International Telecommunication Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

البريد الإلكتروني: itu-ro-africa@itu.int
الهاتف: +251 11 551 4977
الهاتف: +251 11 551 4855
الهاتف: +251 11 551 8328
الفاكس: +251 11 551 7299

الكاميرون

Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

البريد الإلكتروني: itu-yaounde@itu.int
الهاتف: + 237 22 22 9292
الهاتف: + 237 22 22 9291
الفاكس: + 237 22 22 9297

السنغال

Union internationale des télécommunications (UIT)
Bureau de zone
8, Route du Méridien Président
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

البريد الإلكتروني: itu-dakar@itu.int
الهاتف: +221 33 859 7010
الهاتف: +221 33 859 7021
الفاكس: +221 33 868 6386

زمبابوي

International Telecommunication Union (ITU) Area Office
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

البريد الإلكتروني: itu-harare@itu.int
الهاتف: +263 242 369015
الهاتف: +263 242 369016

الأمريكتان

البرازيل

União Internacional de Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

البريد الإلكتروني: itubrasilia@itu.int
الهاتف: +55 61 2312 2730-1
الهاتف: +55 61 2312 2733-5
الفاكس: +55 61 2312 2738

بربادوس

International Telecommunication Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

البريد الإلكتروني: itubridgetown@itu.int
الهاتف: +1 246 431 0343
الفاكس: +1 246 437 7403

شيلي

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

البريد الإلكتروني: itusantiago@itu.int
الهاتف: +56 2 632 6134/6147
الفاكس: +56 2 632 6154

هندوراس

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

البريد الإلكتروني: ituteguciglpa@itu.int
الهاتف: +504 2235 5470
الفاكس: +504 2235 5471

الدول العربية

مصر

International Telecommunication Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

البريد الإلكتروني: itu-ro-arabstates@itu.int
الهاتف: +202 3537 1777
الفاكس: +202 3537 1888

آسيا والمحيط الهادئ

تايلاند

International Telecommunication Union (ITU) Regional Office
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

البريد الإلكتروني: itu-ro-asiapacific@itu.int
الهاتف: 8 – +66 2 574 9326
+66 2 575 0055

إندونيسيا

International Telecommunication Union (ITU) Area Office
Gedung Sapta Pesona
13th floor
Jl. Merdeka Barat No. 17
Jakarta 10110
Indonesia

البريد الإلكتروني: bdt-ao-jakarta@itu.int
الهاتف: +62 21 380 2322

الهند

International Telecommunication Union (ITU) Area Office and Innovation Centre
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

البريد الإلكتروني:
Area Office: itu-ao-southasia@itu.int
Innovation Centre: itu-ic-southasia@itu.int
الموقع الإلكتروني: ITU Innovation Centre in New Delhi, India

كومنولث الدول المستقلة

الاتحاد الروسي

International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

البريد الإلكتروني: itu-ro-cis@itu.int
الهاتف: +7 495 926 6070

أوروبا

سويسرا

International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland

البريد الإلكتروني: eurregion@itu.int
الهاتف: +41 22 730 5467

الاتحاد الدولي للاتصالات
مكتب تنمية الاتصالات
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-41106-0

نُشرت في سويسرا
جنيف، 2025
Photo credits: Adobe Stock