الأمن السيبراني للجيل الخامس

فترة الدراسة
2025-2022

المسألة 3/2

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

ناتج مرحلي
2024

ملخص تنفيذي

يؤكد هذا الناتج المرحلي على الجوانب الرئيسية للأمن السيبراني للجيل الخامس نظراً لتزايد التهديدات السيبرانية العالمية والطبيعة الحرجة للبنية التحتية للاتصالات. وتقدم تكنولوجيا الجيل الخامس، بفضل برمجياتها المتقدمة ومعماريتها القائمة على السحابة وإمكانات التوصيلية المكثفة، **نماذج أمنية جديدة**. وتقدم فوائد كبيرة، ولكنها تجلب أيضاً مخاطر جديدة، مما يستلزم اتخاذ تدابير قوية بشأن الأمن السيبراني للحماية من التهديدات.

وتتطلب تعقيدات شبكات الجيل الخامس استراتيجيات أمنية متقدمة والتعاون بين مختلف أصحاب المصلحة. وقد بدأت **منظمات وضع المعايير** (SDO) في تقييس جوانب الأمن السيبراني لشبكات الجيل الخامس، ولكن من الضروري التعاون والتواصل بشكل مستمر لتجنب ازدواجية الجهود.

وتعد **تدابير الأمن السيبراني الاستباقية** بالغة الأهمية في جميع مراحل نشر الشبكات، حيث يتحمل البائعون والمشغلون مسؤوليات بشأن إدارة مخاطر الأمن السيبراني.

ويجري وضع **مجموعة متنوعة من السياسات واللوائح الوطنية للأمن السيبراني للجيل الخامس**. وتبنت العديد من البلدان بالفعل نُهجها لتخفيف المخاطر الأمنية وتركز الآن على أنظمة التنفيذ والامتثال الخاصة بها.

ويعتبر **الاستثمار في التعليم والتدريب** حيوياً لتلبية الطلب المتزايد على المتخصصين المهرة في مجال الأمن السيبراني.

وتطلعاً إلى المستقبل، يؤكد **التخطيط لشبكات الجيل السادس** على تعزيز الأمن السيبراني والقدرة على الصمود منذ البداية. ويعكس إطار الاتحاد بشأن الاتصالات المتنقلة الدولية لعام 2030 التزاماً بدمج تدابير أمنية قوية لدعم التقدم التكنولوجي في المستقبل.

مقدمة

استُعرضت اختصاصات المسألة 3/2 المسندة للجنة الدراسات 2 لقطاع تنمية الاتصالات "تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني" خلال المؤتمر العالمي الأخير لتنمية الاتصالات، الذي عُقد في كيغالي، رواندا، في يونيو 2022. وكانت إحدى القضايا المحددة للدراسة هي "مناقشة التحديات والنُهج الخاصة بالأمن السيبراني للجيل الخامس".

وتقر الاختصاصات الموافق عليها للمسألة 3/2 بأن تهديدات الأمن السيبراني لا تزال تشكل مصدر قلق كبيراً للحكومات والمنظمات والأفراد في جميع أنحاء العالم. 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[1]. وتكون شبكات الاتصالات، التي تعتبر في العديد من الولايات القضائية مكوناً حيوياً للبنية التحتية الوطنية الحرجة أو الخدمات الأساسية، معرضةً للهجمات السيبرانية التي يمكن أن تعطل الخدمات الأساسية وسلامة الجمهور.

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

وإدراكاً للأهمية الحاسمة لحماية البنية التحتية للجيل الخامس وخدماته، نظمت لجنة الدراسات 2 المعنية بالمسألة 3/2 ورشة عمل مخصصة لمدة يوم كامل في 2 مايو 2024 جمعت واضعي السياسات والهيئات التنظيمية والمشغلين وأعضاء آخرين في صناعة الاتصالات لمناقشة تعقيدات الأمن السيبراني للجيل الخامس، وتبادل الممارسات الحالية، واستكشاف الحلول المبتكرة للتهديدات الناشئة. 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.

ويعكس هذا التقرير المناقشات التي دارت خلال ورشة العمل وكذلك المساهمات التي وردت خلال دورة الدراسة هذه. ولا يهدف إلى أن يكون تقريراً تقنياً عن الأمن السيبراني للجيل الخامس، بل إنه يهدف إلى تبادل الأفكار والممارسات الجيدة التي تم جمعها في سياق مسألة الدراسة والتي يمكن لأعضاء الاتحاد النظر فيها وتنفيذها في سياقاتهم الوطنية. ويركز هذا التقرير أساساً على الأمن السيبراني للجيل الخامس من الشبكات الإلكترونية العامة.

1. تكنولوجيا الجيل الخامس تقدم نماذج أمنية جديدة لشبكات الاتصالات

لمحة عامة عن الأمن السيبراني لشبكات الجيل الخامس

تتسم تكنولوجيا الجيل الخامس بأنظمة برمجيات متقدمة تتيح التشكيل السهل والتوصيلية الضخمة للمشتركين والأجهزة. وتدعم هذه التكنولوجيا التطبيقات منخفضة الكمون، مثل الواقع المعزز والجراحة عن بعد 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، يقدم الجيل الخامس تحولاً كبيراً نحو المعمارية القائمة على السحابة والشبكات المعرَّفة بالبرمجيات (SDN) والتمثيل الافتراضي لوظائف الشبكة (NFV). ويُنشئ هذا التحول مشهداً أكثر تعقيداً وديناميةً للأمن السيبراني.

ومع زيادة انتشار 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 للجيل 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[2]، ينبغي أن يوضع في الاعتبار أن مصطلح "الأمن السيبراني للجيل 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.

[1] Global Risks Report 2024

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

في الاتحاد، يعرَّف الأمن السيبراني في التوصية X.1205 الصادرة عن قطاع تقييس الاتصالات (ITU-T) على أنه *"مجموع الأدوات والسياسات ومفاهيم الأمن وتحفظات الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات 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 المنقولة 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"*[3].

نشر الشبكات القديمة

غالباً ما يقوم المشغلون مبدئياً بنشر شبكات الجيل الخامس على أساس أنها غير قائمة بذاتها (NSA)، بحيث يستفيدون من البنية التحتية الحالية لشبكة الجيل الرابع قبل نشر شبكة للجيل الخامس من طرف إلى طرف قائمة بذاتها (SA).[4] وستَرِث شبكات الجيل الخامس غير القائمة بذاتها نقاط الضعف القديمة للجيل الرابع أو حتى الجيل الثاني/الجيل الثالث، والتي يجب إدارتها وفقاً لذلك. وبالنسبة لبعض المشغلين، فإن ذلك بمثابة "ديون تقنية": إدارة الأنظمة القديمة تعني الحاجة إلى وضع مجموعة من الضوابط الأمنية المقيَّسة لقياس الحالة الأمنية لمكونات البنية التحتية في مختلف مراحل نضجها الجيلي.[5]

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[6،7].

2. يجري العمل على وضع المعايير من أجل تأمين الجيل الخامس في الكثير من منظمات وضع المعايير (SDO)، لذا تحتاج هذه المنظمات إلى بذل جهود متضافرة للتواصل وتجنب ازدواجية العمل

منظمات وضع المعايير النشطة في مجال الأمن السيبراني للجيل الخامس

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

وللمساعدة في ربط هذه الأنشطة المختلفة وإرشاد اتجاه أعمال تقييس الشؤون الأمنية المتعلقة بتكنولوجيا الجيل الخامس في قطاع تقييس الاتصالات، أعدت لجنة الدراسات 17 (SG17) تقريراً تقنياً لربط المعايير القائمة وتلك الجاري وضعها في منظمات وضع المعايير وتطبيقها في شبكات الجيل الخامس[8]. 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 للجيل الخامس.

ونشرت لجنة الدراسات 11 توصية بشأن أمن الجيل الخامس، استناداً إلى المساهمات التي أعدها المشغلون والبائعون ومصنعو الهواتف الذكية ومقدمو المحتوى وغيرهم، وتركز 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 المشروع 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[9].

[3] https://www.itu.int/rec/T-REC-X.1205-200804-I

[4] توصل الأجهزة العاملة على شبكات الجيل الخامس غير القائمة بذلتها عادةً بترددات الجيل الخامس لإرسال البيانات عند الحاجة إلى عرض نطاق أكبر وكمون أقصر (مثل الاتصال بين السيارات الذكية)، أو لتقليل استهلاك الطاقة على الأجهزة المدعمة بإنترنت الأشياء، ولكنها تظل تعتمد على شبكات الجيل الرابع وحتى الجيل الثاني/الثالث من أجل المكالمات الصوتية والرسائل النصية القصيرة. المصدر: https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf

[5] مواد ورشة العمل – Maxis

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

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

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

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

ونظراً للمصادر العديدة للمعلومات ذات الصلة بأمن الجيل الخامس، نشرت الوكالة الأوروبية للأمن السيبراني، الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)، مستودعاً موحداً للضوابط الأمنية التقنية لشبكات الجيل الخامس، وهو مصفوفة الضوابط الأمنية للجيل الخامس.[10] ويتم نشر 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 مخاطر تداخل وازدواج العمل، مما يجعل التواصل وتبادل المعلومات بين منظمات وضع المعايير أكثر أهمية.

دمج المعايير في المتطلبات التنظيمية الإلزامية

تساعد المعايير في 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. ويمكن أن 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 للجيل الخامس توازناً بين أفضل الممارسات 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.

3. ينبغي استكمال المعايير والمواصفات بتدابير الأمن السيبراني الاستباقية في مختلف المراحل التي تسبق نشر الشبكة

الاعتبارات الأمنية على مستوى البائع

المعايير والمواصفات ليست سوى مكون واحد من مكونات الأمن السيبراني للجيل الخامس. وتحدد الطريقة التي ينفذ بها البائعون والمشغلون هذه المعايير ويشكلونها الوضع الأمني لشبكات الجيل الخامس. وقد تبنت شركة Ericsson نهجاً شاملاً إزاء أمن الجيل الخامس يتم تناوله على مستوى أربع طبقات: المعايير، وتطوير منتجات البائعين، ونشر الشبكات، وتشغيل الشبكات[11]. وترى الشركة أن هذا النهج الشامل 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 (NESAS)[12] ، التي وضعتها الرابطة GSMA والمشروع 3GPP، إلى تحسين مستويات أمن معدات الشبكات المتنقلة من خلال توفير خطة ضمان يمكن تطبيقها عالمياً. وتعتمد الخطة 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 الخطة NESAS. كما أن الخطة NESAS مرشحة لخطة اعتماد الأمن السيبراني للاتحاد الأوروبي المتعلقة بالجيل الخامس[13] – وهو اعتماد على مستوى الاتحاد الأوروبي يحقق التوافق عبر دول الاتحاد الأوروبي. ولن يحل هذا الاعتماد محل الخطة NESAS الحالية ولكنهما سيتواجدان جنباً إلى جنب. 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[14]، وهو توجيهات تساعد المشغلين على تقييم المخاطر السيبرانية المرتبطة باستخدام معدات البائع.

الاعتبارات الأمنية على مستوى المشغل

يمكن أن توفر الخطة 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 واستخبارات التهديدات والتحليلات للمساعدة في دعم دفاعهم السيبراني. ويوفر الأمن السيبراني للجيل الخامس فوائد، مثل الأمن في الوقت الفعلي واستراتيجيات من قبيل الثقة الصفرية، والتي تحسن رؤية النظام. ومع ذلك، فإنه يواجه تحديات خاصة به: 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 (على سبيل المثال حقوق النفاذ بين وظائف الشبكة، وحقوق مديري الشبكة، وتشكيل التمثيل الافتراضي). وتتاح للمشغلين ثروة من الأدبيات المتعلقة باستراتيجيات الأمن السيبراني الخاصة بالجيل الخامس يمكنهم النظر فيها.[15]

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

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

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

[13] https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification

[14] https://www.ncsc.gov.uk/report/vendor-security-assessment

[15] 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/

كما أن اختبار شبكات الاتصالات الحية ضروري لتحديد المخاطر السيبرانية الحقيقية التي تواجهها شبكات الاتصالات. ويمكن للمشغلين إجراء بعض أشكال الاختبارات الأمنية على شبكاتهم وأنظمتهم، إما باستخدام الموارد الداخلية، أو الاستعانة 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 الخطة مدى قدرة مزود الاتصالات على اكتشاف مثل هذه الهجمات واحتوائها والتصدي لها. ويتمثل الهدف العام في تحديد نقاط الضعف الأمنية أو نقاط الضعف الأخرى في وظائف المزود 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 لمزودي الاتصالات تحديد مجالات محددة يمكن فيها تحسين أمنهم، وتعمل الهيئة التنظيمية Ofcom معهم للمساعدة في تنفيذ التغييرات المناسبة في الوقت المناسب[16].

ومن الضروري وجود مبرر تجاري قوي بشأن الأمن السيبراني للجيل 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.

تمثل شبكة النفاذ الراديوي المفتوح (Open RAN) تفكيكاً لشبكة النفاذ الراديوي (RAN)، ويمكّن تقييس السطوح البينية التي تربط هذه العناصر المفككة من بناء الشبكات باستخدام معدات من بائعين مختلفين.

فمن ناحية، يمكن أن تجلب شبكات Open RAN المزيد من التعقيد إلى سلسلة توريد شبكات الاتصالات. وتتطلب هذه المعمارية، التي تشجع تنوع البائعين في الشبكة RAN، المزيد من جهود التكامل على امتداد سلسلة توريد الشبكة ويمكن أن تزيد ناقلات الهجمات. ومن ناحية أخرى، تضيف شبكة Open RAN 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 الشبكات Open RAN، على المواصفات الأمنية لمعمارية الشبكة Open RAN ويهدف إلى تقييس هذه المواصفات في المعهد الأوروبي لمعايير الاتصالات (ETSI).

ويعتبر المشغل NTT Docomo (اليابان) واحداً من المشغلين الذين تبنوا معمارية الشبكة Open RAN 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 RAN التقليدية وشبكة Open RAN وخلص إلى وجود اختلاف أمني ضئيل بينهما.[17]

4. شبكات الجيل الخامس والأمن السيبراني للجيل الخامس هما محور تركيز المبادرات السياساتية والتنظيمية الأخيرة التي وصلت إلى مراحل مختلفة من التنفيذ

مثال على السياسات واللوائح الوطنية لتأمين شبكات الجيل الخامس

بالإضافة إلى المعايير والممارسات التي يتبعها البائعون والمشغلون، يمكن وضع 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 يفرضها الجيل الخامس بما في ذلك المخاطر السيبرانية. وينبغي أيضاً النظر إلى أنظمة التنفيذ والامتثال كجزء من الإطار العام.

وتقدم القائمة أدناه لمحة عامة عن مختلف الإجراءات وحالتها الراهنة.

- يركز النهج الشامل الذي تتبعه **البرازيل** إزاء الأمن السيبراني للجيل الخامس على إدارة المخاطر مع المشغلين. وبموجب شروط مزاد طيف الجيل الخامس ولوائح الأمن السيبراني لقطاع الاتصالات[18]، 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. كما أقامت الوكالة الوطنية للاتصالات في البرازيل (Anatel) شراكة مع الهيئات الأكاديمية لإجراء دراسات في هذا الصدد.[19]
- 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[20] ويمنح وزير الدولة سلطات جديدة لوضع اللوائح وإصدار مدونات

[16] https://www.itu.int/md/D22-SG02.RGQ-C-0074/

[17] 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

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

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

[20] باستثناء الكيانات بالغة الصغر.

- الممارسة، والتي تم تطويرها منذ ذلك الحين وإرشادها من خلال التشاور العام[21]. ويتضمن القانون أيضاً أحكاماً تعزز السلطات التنظيمية لهيئة Ofcom لمراقبة وإنفاذ كيفية امتثال المزودين لواجباتهم الجديدة.
- يسلَّم بأن لوائح وسياسات الأمن السيبراني للجيل الخامس في **جمهورية كوريا** من بين الأكثر صرامة على مستوى العالم، مما 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 للجيل الخامس مع أفضل الممارسات العالمية.
- يشمل الإطار القانوني والتقني في **الهند** المتعلق بتعزيز الأمن السيبراني للجيل الخامس ما يلي:
  - التوجيهات الأمنية الوطنية بشأن قطاع الاتصالات، والتي توفر ضماناً لمعالجة الشواغل ومواطن الضعف في سلاسل توريد الاتصالات الموثوقة ومصادرها؛
  - الاختبار الإلزامي لمعدات الاتصالات واعتمادها، بما يضمن الامتثال للمتطلبات الأمنية الأساسية لكل وظيفة من وظائف شبكات الجيل الخامس؛
  - شروط ترخيص مقدمي خدمات الاتصالات، التي تضمن المراجعات الأمنية الدورية للبنية التحتية للاتصالات.

لدعم ما سبق، تم إنشاء 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 للحوادث الأمنية الحاسوبية (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. ويؤكَّد على التعاون وتبادل المعلومات مع الشركاء الدوليين والبائعين والهيئات الأكاديمية وأصحاب المصلحة الآخرين لتعزيز تدابير الأمن السيبراني. وبالإضافة إلى ذلك، تم وضع 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 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 التركيز 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.
- تتناول **زمبابوي** الأمن السيبراني للجيل الخامس، مع التركيز على الأهمية الناشئة لحوسبة الحافة واستكشاف اعتماد تكنولوجيا شبكات النفاذ الراديوي المفتوح (open RAN) 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 البلاد. وستعمل زمبابوي على مواءمة ممارساتها الأمنية مع المعايير الدولية مثل المعيار 27001 للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية ومعايير المعهد 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

[21] https://www.legislation.gov.uk/uksi/2022/933/contents/made وhttps://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

المتنقلة وأمنها. وتعتزم الهيئة الاستفادة من خبرة مختلف أصحاب المصلحة وأفضل الممارسات 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** مجموعة أدوات لتدابير تخفيف المخاطر[22] بهدف تحديد مجموعة مشتركة من التدابير لتخفيف المخاطر الرئيسية للأمن السيبراني للجيل الخامس، والمساعدة في 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[23]. ويتضمن إطار الاعتماد للاتحاد الأوروبي التطوير المستمر لنظام إصدار شهادات الأمن السيبراني للجيل الخامس[24].

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 نظام أمن الاتصالات الخاص بها وتتعاون مع الأفرقة التنظيمية والتقنية لدى مزودي الاتصالات. وتعتبر الهيئة التنظيمية أن التنفيذ لا يتعلق بالتدابير التقنية فحسب، بل يتطلب تحولاً ثقافياً في طريقة تفكير مزودي 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.

وفي **ماليزيا**، وافقت الحكومة على مشروع قانون جديد بشأن الأمن السيبراني ينص على أن وكالة واحدة ستدير جميع البنى التحتية الحيوية، بما في ذلك البنى التحتية للاتصالات. والهيئة التنظيمية بصدد وضع مجموعة من المتطلبات للمشغلين للإبلاغ عن الامتثال الأمني. وسلط أحد مشغلي الاتصالات في البلد الضوء على أن تنفيذ السياسة الجديدة قد يكون صعباً، حيث 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.

5. لا يزال الاستثمار في تعليم وتدريب القوى العاملة على التعامل مع تعقيدات الأمن السيبراني للجيل الخامس من الأولويات الرئيسية

وفقاً لشركة Allied Market Research[25]، من المتوقع أن تصل قيمة السوق العالمية لأمن 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 للجيل 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 الاستثمار في تعليم وتدريب القوى العاملة القادرة على إدارة تعقيدات أمن الجيل الخامس. وفي إطار هذا الالتزام، تم إنشاء موقع الاختبار المفتوح لوادي الجيل الخامس من قبل مؤسسات رئيسية، منها هيئة تكنولوجيا المعلومات والاتصالات، وجامعة الشرق الأوسط التقنية، وجامعة İhsan Doğramacı Bilkent ، وجامعة Hacettepe، ومشغلي الاتصالات Türk Telekomünikasyon A.Ş. وTurkcell İletişim Hizmetleri A.Ş. وVodafone 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 يمكن من خلالها للأكاديميين والباحثين وطلاب الدكتوراه والشركات الناشئة المشاركة في العمل المتعلق بتكنولوجيا الجيل الخامس وما بعده، فإن موقع الاختبار المفتوح 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.[26]

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

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

[24] https://certification.enisa.europa.eu/index_en

[25] https://www.alliedmarketresearch.com/5g-security-market-A12820

[26] https://5gtrforum.org.tr/en

الشكل 1: قدرات الاتصالات المتنقلة الدولية-2030

قدرات الاتصالات المتنقلة الدولية لعام 2030

ملاحظة: نطاق الأرقام الخاصة بالقدرات هي تقديرات مستهدفة للبحث والتحقيق بشأن الاتصالات المتنقلة الدولية لعام 2023

المصدر: توصية قطاع الاتصالات الراديوية M.2160

6. 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[27]، المعروفة تجارياً باسم الجيل السادس.

يسلط 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 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".*

لقد أصبح من الواضح أن العمل جار على تصور الجيل السادس وأن عمليات تقييسه يجري تصورها بقلق 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 [28]، يتضح جلياً التحول في التفكير مع إقرار الحاجة إلى تناول الأمن السيبراني والقدرة السيبرانية على الصمود بشكل صحيح كركيزة تمكينية للتحول الرقمي والاقتصاد الرقمي.

[27] التوصية M.2160 لقطاع الاتصالات الراديوية متاحة على: https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en

[28] التوصية M.2083 لقطاع الاتصالات الراديوية متاحة على: https://www.itu.int/rec/R-REC-M.2083-0-201509-I

تابع أعمال **المسألة 3/2 للجنة الدراسات 2 بقطاع تنمية الاتصالات للفترة 2022-2025** "تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني"

الموقع الإلكتروني للمسألة 3/2
http://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/questions/Question-3-2.aspx

القوائم البريدية: d22sg3q2@lists.itu.int سجل هنا

الموقع الإلكتروني للجنتي دراسات قطاع تنمية الاتصالات: www.itu.int/itu-d/sites/studygroups/

قدّم تعليقاتك بالبريد الإلكتروني في العنوان devSG@itu.int أو بالهاتف على الرقم 5999 730 22 41+

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

منشورات ITU
نُشرت في سويسرا، جنيف، 2024