Cybersécurité 5G

Période d'études 2022-2025

Question 3/2

Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité

Produit intérimaire 2024

Résumé analytique

Ce produit intérimaire met l'accent sur les aspects essentiels de la cybersécurité 5G au vu de la hausse des cybermenaces dans le monde et de la nature critique des infrastructures de télécommunication. Avec ses logiciels élaborés, son architecture basée sur le nuage et sa connectivité étendue, la technologie 5G introduit de **nouveaux paradigmes de sécurité**. Elle offre des avantages significatifs, mais comporte également de nouveaux risques, nécessitant des mesures de cybersécurité robustes pour se protéger contre les menaces.

La complexité des réseaux 5G exige des stratégies de sécurité évoluées et une collaboration entre les différentes parties prenantes. Les **organisations de normalisation** (SDO) ont commencé à normaliser les aspects de cybersécurité des réseaux 5G, mais une coopération et une communication constantes sont nécessaires afin d'éviter tout chevauchement d'activités.

Des mesures de cybersécurité proactives sont cruciales à toutes les étapes du déploiement du réseau, les fournisseurs et les opérateurs étant responsables de la gestion des risques de cybersécurité.

Un ensemble de politiques et de réglementations nationales relatives à la cybersécurité 5G sont en cours d'élaboration. De nombreux pays ont déjà adopté leurs propres approches pour atténuer les risques sécuritaires et se concentrent désormais sur leurs systèmes de mise en œuvre et de conformité.

Il est essentiel d'**investir dans l'éducation et la formation** pour répondre à la demande croissante de professionnels qualifiés dans le domaine de la cybersécurité.

Pour l'avenir, la **planification de la 6G** met l'accent sur le renforcement de la cybersécurité et de la résilience dès le départ. Le cadre IMT-2030 de l'UIT reflète l'engagement d'intégrer des mesures de sécurité robustes pour soutenir les progrès technologiques futurs.

Introduction

Le champ d'application de la Question 3/2 confiée à la Commission d'études 2 de l'UIT-D, intitulée "Sécurisation des réseaux d'information et de communication: Bonnes pratiques pour créer une culture de la cybersécurité", a été examiné lors de la dernière Conférence mondiale de développement des télécommunications, qui s'est tenue à Kigali (Rwanda) en juin 2022. L'un des thèmes à étudier était "Examiner les enjeux et les approches concernant la cybersécurité de la 5G".

Le champ d'application approuvé pour la Question 3/2 reconnaît que les menaces à la cybersécurité continuent d'être une préoccupation majeure pour les gouvernements, les organisations et les particuliers dans le monde entier. Au niveau mondial, la cybersécurité est classée au quatrième rang des risques à court terme les plus graves, selon le Rapport sur les risques mondiaux 2024 du Forum économique mondial[1]. Les réseaux de télécommunication, qui, dans de nombreuses juridictions, sont considérés comme une composante vitale des infrastructures nationales essentielles ou des services essentiels, sont vulnérables aux cyberattaques, qui peuvent perturber les services essentiels et la sécurité publique.

L'introduction de la technologie 5G représente un changement important dans les télécommunications, offrant des vitesses plus élevées et une meilleure connectivité qui ont le potentiel d'améliorer les industries, d'étendre les applications de l'Internet des objets (IoT) et d'apporter de nouvelles approches en matière de communication numérique. Cependant, l'architecture sophistiquée qui permet ces avancées s'accompagne de défis complexes en matière de cybersécurité qui nécessitent une compréhension globale et des mesures de protection robustes.

Conscients de l'importance cruciale de la protection de l'infrastructure et des services 5G, les responsables de la Commission d'études 2 travaillant sur la Question 3/2 ont organisé le 2 mai 2024 un atelier consacré à une journée entière qui a rassemblé des décideurs, des régulateurs, des opérateurs et d'autres membres du secteur des télécommunications pour examiner les complexités de la cybersécurité 5G, échanger des pratiques existantes et réfléchir à des solutions innovantes face aux menaces émergentes. Alors que les réseaux 5G sont déployés à l'échelle mondiale, il est impératif de mettre en place un écosystème sécurisé pour garantir l'intégrité, la disponibilité et la confidentialité des informations, ainsi que pour protéger l'infrastructure devenue l'épine dorsale de l'économie numérique.

Le présent rapport rend compte des débats de l'atelier ainsi que des contributions reçues pendant la période d'études actuelle. Il ne s'agit pas d'un rapport technique sur la cybersécurité 5G, mais plutôt d'un échange de réflexions et de bonnes pratiques recueillies dans le cadre de la Question à l'étude, que les membres de l'UIT peuvent envisager et mettre en œuvre dans leur contexte national. Le présent rapport porte essentiellement sur la cybersécurité 5G des réseaux électroniques publics.

1. La 5G apporte de nouveaux paradigmes de sécurité pour les réseaux de télécommunication

Aperçu général de la cybersécurité 5G

La 5G se caractérise par ses systèmes logiciels avancés qui permettent une configuration plus souple et une connectivité massive des abonnés et des appareils. Cette technologie prend en charge des applications à faible temps de latence, telles que la réalité augmentée, la téléchirurgie et les services Internet intégrés qui s'appuient sur un réseau robuste et fiable. L'un des principaux cas d'utilisation de la 5G est l'Internet des objets (IoT), qui tire parti de la capacité de la 5G à connecter un grand nombre de points de terminaison. La technologie 5G est sur le point de révolutionner la connectivité, ce qui présente également des risques et des défis nouveaux et dynamiques en matière de cybersécurité.

Contrairement aux générations précédentes de technologies hertziennes, la 5G s'oriente considérablement vers une architecture basée sur le nuage, des réseaux pilotés par logiciel (SDN) et la virtualisation des fonctions de réseau (NFV). Ce changement crée un paysage de cybersécurité plus complexe et plus dynamique.

Avec la généralisation de la 5G, l'infrastructure des télécommunications devrait devenir une cible de plus en plus attrayante pour les cyberactivités malveillantes, nécessitant la mise en place de mesures de sécurité évoluées capables de s'adapter à l'évolution des menaces. La cybersécurité pour la 5G devrait viser à accroître la résilience de l'ensemble de l'écosystème, y compris l'infrastructure et les applications. Il s'agit notamment de protéger les appareils connectés, les données et les réseaux contre les cybermenaces.

Étant donné que les différentes organisations utilisent des définitions différentes de la cybersécurité[2], il convient de garder à l'esprit que l'expression "cybersécurité 5G" dont il est fait mention dans le présent rapport renvoie à la cybersécurité dans le contexte de la 5G, avec ses nouveaux paramètres, normes et fonctionnalités technologiques qui doivent être gérés correctement pour protéger l'ensemble de l'écosystème numérique et assurer la cyberrésilience.

[1] Rapport sur les risques mondiaux 2024

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

À l'UIT, la cybersécurité est définie dans la Recommandation X.1205 du secteur de la normalisation des télécommunications (UIT-T) comme suit: "*ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux de sécurité sont les suivants:*

- *disponibilité;*
- *intégrité, ce qui peut inclure l'authenticité et la non-répudiation; et*
- confidentialité"[3].

Déploiements de réseaux traditionnels

Dans un premier temps, les opérateurs ont tendance à déployer les réseaux 5G sur une base non autonome (NSA) et tirent ainsi parti de l'infrastructure 4G existante avant de déployer un réseau 5G de bout en bout autonome (SA)[4]. Les réseaux NSA héritent des vulnérabilités existantes de la 4G ou même de la 2G/3G, qui doivent être gérées en conséquence. Pour certains opérateurs, cela correspond à une "dette technique": la gestion d'anciens systèmes implique la nécessité de développer un ensemble de contrôles de sécurité standardisés pour mesurer l'état de sécurité des composants de l'infrastructure à différentes étapes de la maturité générationnelle[5].

Il est important de souligner que la 5G SA présente des opportunités d'amélioration de la cybersécurité par rapport aux générations précédentes de technologies mobiles: elle est conçue pour être plus sécurisée que la 4G. Des améliorations ont été notées dans des domaines tels que la sécurité et la confidentialité des abonnés, le réseau d'accès radioélectrique (RAN), le réseau central et la sécurité de l'itinérance[6], [7].

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

[4] Les dispositifs fonctionnant sur des réseaux 5G NSA se connectent généralement aux fréquences 5G pour la transmission de données lorsqu'ils auront besoin d'une plus grande largeur de bande et d'une latence plus faible (par exemple pour la communication entre voitures intelligentes) ou pour réduire la consommation d'énergie des appareils compatibles IoT, mais continuent de s'appuyer sur les réseaux 4G et même 2G/3G pour les appels vocaux et les messages SMS.
Source: https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2019/11/5G-Research_A4.pdf

[5] Matériel de l'atelier – 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

2. De nombreuses organisations de normalisation travaillent sur des normes visant à sécuriser la 5G; ces organisations doivent ainsi déployer des efforts concertés pour communiquer et éviter les doubles emplois

Les organisations de normalisation actives dans la cybersécurité 5G

En raison de la complexité de la technologie de la 5G et des questions impliquées, il n'existe aucune organisation de normalisation ayant un mandat exclusif en matière de cybersécurité 5G. Afin d'éviter les doubles emplois, des mécanismes ont été mis au point afin d'échanger des informations entre les organisations de normalisation et coordonner les propositions et les sujets d'étude.

Pour mieux cartographier ces différentes activités et orienter les travaux de normalisation de la sécurité liés à la 5G à l'UIT-T, la Commission d'études 17 (CE 17) a élaboré un rapport technique établissant une correspondance entre les normes existantes et les normes en cours d'élaboration, les organisations de normalisation et leur application dans les réseaux 5G[8]. Le rapport recense les normes de l'UIT-T, du Projet de partenariat de troisième génération (3GPP), de l'Institut européen des normes de télécommunication (ETSI) et de l'IEEE Standards Association (IEEE-SA), ainsi que les ressources non normalisées pertinentes pour la cybersécurité 5G.

La Commission d'études a publié 11 Recommandations sur la sécurité de la 5G, sur la base de contributions rédigées par des opérateurs, des fabricants, des fabricants de smartphones et des fournisseurs de contenu, entre autres. Ces recommandations s'articulent autour de la sécurité dans cinq domaines: la sécurité SDN-NFV, la sécurité du découpage de réseau, la sécurité en périphérie mobile, la sécurité de la gestion des réseaux 5G et la sécurité des services 5G. La CE 17 a établi des liaisons avec d'autres organismes de normalisation (3GPP, IETF) et des groupes industriels travaillant sur des spécifications présentant un intérêt pour la normalisation de la cybersécurité 5G, par exemple la GSMA.

Bien qu'elle ne soit pas elle-même un organisme de normalisation, la GSMA élabore des spécifications en convoquant ses membres et en collaborant avec les organisations de normalisation pour les améliorer et/ou les adopter comme norme. La GSMA a publié une liste des contrôles de sécurité de base que les opérateurs mobiles peuvent envisager, à titre volontaire, lors du déploiement de réseaux 5G[9].

Compte tenu des nombreuses sources d'information pertinente pour la sécurité de la 5G, l'Agence européenne pour la cybersécurité, l'ENISA, a publié un référentiel unifié des contrôles techniques de sécurité pour les réseaux 5G, à savoir le 5G Security Controls Matrix[10]. Le référentiel est actuellement publié sous forme de tableur, mais l'agence développe également un outil web pour améliorer la convivialité.

[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/

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

Étant donné que les réseaux deviennent toujours plus complexes et que les télécommunications convergent avec les réseaux IP, il devient de plus en plus difficile de confier des travaux de normalisation dans des domaines spécifiques aux différentes organisations de normalisation. Cela accroît le risque de chevauchement et de duplication des travaux, ce qui rend encore plus importante la communication et le partage d'informations entre les organisations de normalisation.

Tenir compte des normes dans les prescriptions réglementaires obligatoires

Les normes contribuent à assurer l'interopérabilité entre les technologies et à réduire le temps nécessaire à une innovation pour atteindre son marché mondial. Les normes de cybersécurité peuvent définir une base commune de sécurité tenant compte des bonnes pratiques universelles. Les normes sont le résultat d'un processus fondé sur le consensus. Elles peuvent être obligatoires, mais, dans la plupart des cas, elles sont facultatives, ce qui laisse aux fournisseurs et aux opérateurs une plus grande latitude dans leurs décisions de déploiement. Dans certains cas, les normes peuvent devenir obligatoires si des réglementations techniques nationales prévoient une norme spécifique dans leurs exigences de sécurité. Les stratégies nationales de cybersécurité 5G devraient refléter un équilibre entre les bonnes pratiques mondiales et les réalités opérationnelles locales. En règle générale, les prescriptions réglementaires nationales devraient s'inspirer des normes internationales reconnues, en les adaptant aux contextes et aux besoins locaux afin d'assurer le succès du déploiement de la 5G et la cybersécurité des réseaux 5G.

3. Les normes et spécifications doivent être complétées par des mesures de cybersécurité proactives aux différentes étapes menant au déploiement du réseau

Considérations de sécurité au niveau du fournisseur

Les normes et les spécifications ne sont qu'un élément de la cybersécurité 5G. La manière dont les fournisseurs et les opérateurs mettent en œuvre ces normes et les configurent définit le niveau de sécurité des réseaux 5G. Ericsson a adopté une approche holistique de la sécurité 5G qui est traitée au niveau de quatre couches: les normes, le développement des produits des fournisseurs, le déploiement des réseaux et l'exploitation des réseaux[11]. L'entreprise considère qu'une telle approche globale peut garantir que les mesures d'atténuation seront mises en œuvre en tenant compte des interdépendances entre les couches ainsi que des besoins spécifiques à chaque couche.

Comme exemple concret de mesure de sécurité 5G, le programme NESAS (Network Equipment Security Assurance Scheme)[12], élaboré par la GSMA et le 3GPP, vise à améliorer les niveaux de sécurité des équipements de réseau mobile en fournissant un système de garantie qui peut être appliqué à l'échelle mondiale. Le programme repose sur un audit d'experts internes et indépendants – combinant une évaluation entre les processus des fournisseurs et une évaluation des produits – qui débouche sur une accréditation. L'objectif de ce programme est d'alléger la charge des tests de sécurité pour les fournisseurs d'équipements de réseau qui opèrent généralement à l'échelle mondiale. Les principaux fournisseurs ont déjà obtenu l'accréditation NESAS. Le programme NESAS est également candidat au programme de certification de cybersécurité de l'UE pour la 5G[13], une certification de niveau européen qui garantirait la conformité dans tous les États de l'UE. Cette certification ne remplacerait pas le système NESAS actuel, mais existerait en parallèle. Il est essentiel d'élaborer des programmes/initiatives de certification de manière à ce qu'ils restent souples et puissent être rapidement actualisés, compte tenu de l'évolution du paysage des menaces.

Au Royaume-Uni, le NCSC recommande d'utiliser le cadre d'évaluation des fournisseurs[14], guide qui aide les opérateurs à évaluer les cyberrisques liés à l'utilisation des équipements des fournisseurs.

Considérations de sécurité au niveau de l'opérateur

Les systèmes NESAS peuvent fournir une certaine garantie qu'un élément de l'équipement de réseau est sécurisé avant son déploiement. À mesure que les opérateurs déploient et exploitent leurs réseaux, d'autres considérations de sécurité doivent être intégrées, par exemple la détection des attaques et la réponse automatisée. C'est là que les opérateurs devraient envisager de tirer parti de l'IA, des renseignements sur les menaces et de l'analyse pour soutenir leur cyberdéfense. La cybersécurité 5G offre des avantages, tels que la sécurité en temps réel et des stratégies telles que le Zero Trust, qui améliorent la visibilité du système. Cependant, elle pose des défis qui lui sont propres, à savoir le maintien de la connectivité entre différents réseaux avec différents niveaux de sécurité, le travail avec des composants hérités et divers types de réseaux, et la complexité de l'intégration de l'IA dans les mesures de sécurité. L'application de contrôles d'accès stricts conformément au principe des "moindres privilèges" garantit que les différents droits dans le réseau (par exemple les droits d'accès entre les fonctions du réseau, les droits des administrateurs de réseau, la configuration de la virtualisation) sont minimisés. Il existe une abondante littérature sur les stratégies de cybersécurité spécifiques à la 5G que les opérateurs peuvent envisager[15].

[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] Voir par exemple: https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf et https://www.5gamericas.org/security-for-5g/

Les tests des réseaux de télécommunication en direct sont également essentiels pour déterminer les cyberrisques réels auxquels sont exposés les réseaux de télécommunication. Les opérateurs peuvent effectuer certaines formes de test de sécurité sur leurs propres réseaux et systèmes, soit en faisant appel à des ressources internes, soit en faisant appel à des sous-traitants extérieurs indépendants. Au Royaume-Uni, TBEST est un programme de tests d'intrusion basé sur les résultats qui simule les techniques et tactiques que les cyberattaquants disposant de ressources suffisantes peuvent utiliser. Il évalue la capacité d'un prestataire de communication à détecter et contenir une telle attaque et à y répondre. L'objectif général est d'identifier et de corriger les failles de sécurité ou d'autres faiblesses dans les fonctions, processus, politiques, systèmes ou réseaux d'un fournisseur qui pourraient être utilisées ensemble pour compromettre les systèmes critiques d'une entreprise avant la détection. En se soumettant au programme TBEST volontaire, les fournisseurs de services de communication peuvent identifier des domaines spécifiques dans lesquels leur sécurité pourrait être améliorée, et l'Ofcom, le régulateur, travaille avec eux pour les aider à mettre en œuvre les changements appropriés en temps voulu[16].

Une solide analyse de rentabilisation pour la cybersécurité 5G est essentielle. Bien que les opérateurs aient besoin que leurs investissements dans les services 5G soient rentabilisés, il convient de reconnaître qu'il est indispensable de se conformer aux mesures de sécurité de base et d'allouer un budget à cet égard en conséquence.

Le réseau RAN ouvert désigne la désagrégation du réseau d'accès radioélectrique (RAN) et la normalisation des interfaces connectant ces éléments désagrégés; il est ainsi possible de construire des réseaux à partir d'équipements provenant de différents fournisseurs.

D'une part, l'architecture d'un réseau RAN ouvert peut compliquer davantage la chaîne d'approvisionnement des réseaux de télécommunication. Elle donne naissance à une diversité des fournisseurs et à de nouveaux vecteurs d'attaque, et exige donc des efforts d'intégration supplémentaires tout au long de la chaîne d'approvisionnement. D'un autre côté, le réseau RAN ouvert apporte plus de transparence dans les chaînes d'approvisionnement, offre une plus grande visibilité aux opérateurs et leur permet de surveiller et de détecter les risques de sécurité. En résumé, il aide les opérateurs à mieux comprendre l'architecture et les équipements de réseau, rendant possible une analyse et une gestion des vulnérabilités plus approfondies. L'O-RAN Alliance, la principale source de spécifications des réseaux RAN ouverts, travaille à l'élaboration de spécifications de sécurité pour l'architecture RAN ouverte et vise à faire normaliser ces spécifications par l'ETSI.

NTT Docomo (Japon) est l'un des opérateurs à avoir adopté l'architecture RAN ouverte en raison de la souplesse de choix des équipements. Cette décision a soulevé des questions du point de vue de la sécurité, car on considère généralement que l'ouverture signifie plus de possibilités d'attaque. Toutefois, l'opérateur a comparé le réseau RAN traditionnel et le réseau RAN ouvert et a conclu qu'il y avait peu de différence en matière de sécurité entre les deux[17].

4. Les réseaux 5G et la cybersécurité sont au cœur d'initiatives politiques et réglementaires récentes, qui se trouvent à différents stades de mise en œuvre

Exemple de politiques et de réglementations nationales visant à sécuriser les réseaux 5G

En plus des normes et des pratiques des fournisseurs et des opérateurs, des politiques et des réglementations pour sécuriser les réseaux 5G peuvent être proposées au niveau national. Celles-ci peuvent se présenter sous différentes formes, telles que des évaluations des fournisseurs, des tests, des certifications, ou des directives ou des exigences. Bien que les approches diffèrent selon les contextes nationaux, ces initiatives visent toutes à atténuer les risques pour la sécurité que présente la 5G, y compris les cyberrisques. Les régimes de mise en œuvre et de conformité devraient également être pris en compte dans le cadre général.

Les exemples ci-dessous donnent un aperçu des différentes actions et de leur état actuel.

- L'approche globale adoptée par le **Brésil** en matière de cybersécurité 5G se concentre sur la gestion des risques avec les opérateurs. En vertu des conditions de mise aux enchères du spectre 5G et du Règlement sur la cybersécurité du secteur des télécommunications[18], les opérateurs 5G sont tenus de respecter le cadre réglementaire, qui comprend des principes, des lignes directrices et des contrôles ex ante pour garantir la cybersécurité dans l'ensemble du secteur. Les contrôles combinent la gouvernance de la cybersécurité, la notification obligatoire des incidents, le partage d'informations, les cycles d'évaluation des vulnérabilités, la notification des infrastructures essentielles et d'autres dispositions. L'Agence nationale des télécommunications du Brésil (Anatel) s'est également associée à des établissements universitaires pour mener des études dans ce domaine[19].

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

[17] Pour de plus amples renseignements sur la sécurité des réseaux RAN ouverts, voir par exemple 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 et https://informacoes.anatel.gov.br/legislacao/resolucoes/2024 (les deux ressources en portugais).

[19] Certains des résultats sont disponibles à l'adresse suivante: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/estudos-e-pesquisas (en portugais)

- Le gouvernement du **Royaume-Uni** a mis en place un cadre de sécurité à l'intention des fournisseurs de réseaux ou de services publics de communications électroniques par le biais de la loi de 2003 sur les communications, telle qu'amendée par la loi de 2021 sur la sécurité des télécommunications (TSA). Ce cadre s'applique à la 5G et à tous les autres réseaux: alors que le Royaume-Uni passe à la 5G et à tous les réseaux en fibre optique, de nombreux fournisseurs de réseaux intègrent des technologies plus anciennes dans leurs infrastructures. La TSA a défini de nouvelles obligations en matière de sécurité pour tous les fournisseurs publics de télécommunications[20] et dote le Secrétaire d'État de nouveaux pouvoirs en ce qui concerne l'élaboration de réglementations et la publication de codes de pratique, qui ont depuis été élaborés et éclairés par une consultation publique[21]. La loi comprend également des dispositions renforçant les pouvoirs réglementaires de l'Ofcom pour surveiller et faire respecter la manière dont les fournisseurs se conforment à leurs nouvelles obligations.
- Les réglementations et politiques en matière de cybersécurité 5G de la **République de Corée** sont reconnues comme faisant partie des plus strictes au monde, ce qui reflète la position de leader du pays dans l'adoption de la technologie 5G. Le gouvernement national, par l'intermédiaire du ministère des Sciences et des TIC (MSIT) et de l'Agence coréenne Internet et de sécurité (KISA), a mis en place un cadre complet pour protéger les réseaux 5G. Ce cadre impose des exigences strictes aux opérateurs de télécommunication pour qu'ils sécurisent l'infrastructure de réseau, protègent les données des utilisateurs et atténuent les risques en matière de cybersécurité. Cette réglementation souligne la nécessité de sécuriser les chaînes d'approvisionnement, d'élaborer des normes de chiffrement évoluées et d'intégrer des principes de sécurité dès la conception dans l'architecture des réseaux. En outre, la République de Corée collabore avec des partenaires internationaux et des organisations de normalisation pour veiller à ce que ses mesures de sécurité pour la 5G soient conformes aux bonnes pratiques mondiales.
- Le cadre juridique et technique établi dans le but de renforcer la cybersécurité 5G en **Inde** comprend:
  - les directives de sécurité nationale relatives au secteur des télécommunications, qui garantissent la fiabilité des chaînes d'approvisionnement et des origines des télécommunications;
  - les tests et certifications obligatoires des équipements de télécommunication, afin de garantir le respect des exigences essentielles de sécurité de chaque fonction du réseau 5G; et
  - les conditions d'octroi de licences aux fournisseurs de services de télécommunication, qui prévoient que le gouvernement procède à des audits publics périodiques de la sécurité de l'infrastructure de télécommunication.

  À cette fin, divers mécanismes institutionnels ont été mis en place: un Centre national pour la sécurité des communications (NCCS), chargé d'élaborer des exigences/normes de sécurité des télécommunications (Indian Telecom Security Assurance Requirements (ITSAR)) et ses laboratoires d'essais et de certification de la sécurité associés; création d'une équipe d'intervention en cas d'incident de sécurité informatique (CSIRT) pour le secteur national des télécommunications; et plusieurs mesures de gestion de la fraude et de protection des consommateurs centrées sur les citoyens, etc. S'agissant des protocoles et des normes de sécurité comme le 3GPP, l'Inde a examiné les spécifications proposées par les normes du secteur pour le contrôle de la conformité et les autres conditions de licence de télécommunication comprenant des audits de sécurité réguliers sur les réseaux des fournisseurs de services.
- Aux **Émirats arabes unis**, la sécurisation des réseaux 5G s'appuie sur une stratégie sur plusieurs fronts qui comprend des cyberexercices rigoureux et une formation à l'échelle nationale, la création d'un centre national d'opérations de sécurité (SOC) chargé de détecter et de réagir en temps réel face aux menaces, et l'initiative Cyber Pulse, qui vise à sensibiliser et à former le personnel aux principales stratégies de défense. L'accent est mis sur la collaboration et le partage d'informations avec les partenaires internationaux, les fournisseurs, les établissements universitaires et d'autres parties prenantes afin de renforcer les mesures de cybersécurité. En outre, un cadre de cybersécurité résilient conforme aux normes internationales telles que l'ISO et le NIST a été mis en place pour garantir la conformité dans l'ensemble du secteur des télécommunications. Pour renforcer la confiance des consommateurs et des entreprises dans la sécurité de la 5G, les Émirats arabes unis ont instauré des politiques, des procédures et des lois de gouvernance qui promeuvent les principes de sécurité dès la conception et les pratiques de sécurité responsables parmi les fournisseurs. Enfin, les Émirats arabes unis ont adopté une approche de la cybersécurité centrée sur les personnes, en mettant l'accent sur la formation, la sensibilisation et l'assistance pour donner aux individus et aux organisations les moyens de lutter contre les cybermenaces, consolidant ainsi une défense solide contre les menaces potentielles auxquelles est confronté le réseau 5G.
- Le **Zimbabwe** s'attaque à la cybersécurité 5G, en mettant l'accent sur l'importance croissante de l'informatique en périphérie et en explorant l'adoption de la technologie de réseau RAN ouvert pour la flexibilité des fournisseurs. Bien qu'il n'existe pas de loi spécifique sur la sécurité de la 5G, la législation existante en matière de protection des données et un document en cours sur la gouvernance de l'IA sous-tendent l'approche du pays. Le Zimbabwe alignera ses pratiques de sécurité sur les normes internationales telles que les normes ISO/CEI 27001 et NIST, en veillant à

[20] Sauf les micro-entités.
[21] https://www.legislation.gov.uk/uksi/2022/933/contents/made et https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

ce que les nouvelles interfaces radioélectriques 5G soient conformes aux protocoles de sécurité établis. L'Autorité de régulation des postes et des télécommunications du Zimbabwe veille à l'application des directives en matière de sécurité et sensibilise le secteur à la préservation de l'intégrité de l'infrastructure nationale des télécommunications.

- Le **Kenya** a adopté sa feuille de route et sa stratégie pour la 5G dans les communications mobiles en avril 2022. La stratégie reconnaît que la sécurité est un aspect important de l'architecture des réseaux 5G. La nature évolutive des services connectés et l'augmentation importante attendue du nombre et des types de dispositifs connectés donnent encore plus d'importance à la confidentialité des données, à la protection des données et à la cybersécurité au Kenya, notamment à la détection des menaces, à l'authentification des utilisateurs et aux bonnes pratiques de fonctionnement. La 5G offre une meilleure sécurité dès la conception en intégrant des exigences de sécurité renforcées sur la base de l'évolution des réseaux et de l'adaptation des enseignements tirés des technologies antérieures. L'Autorité des communications du Kenya a adopté une norme internationale approuvée, élaborée par l'UIT et par le 3GPP pour assurer l'interopérabilité et la sécurité des systèmes mobiles. L'Autorité prévoit de tirer parti de l'expertise de diverses parties prenantes et des bonnes pratiques internationales en matière de cybersécurité pour élaborer des codes techniques et appliquer une liste de contrôle d'évaluation de la sécurité minimale normalisée afin de garantir que les réseaux 5G répondent aux normes techniques les plus récentes et sont conformes aux normes mondiales en matière de sécurité de la 5G.
- À la suite d'un large examen des risques de cybersécurité pour les réseaux 5G, l'**Union européenne** (UE) a élaboré une boîte à outils de mesures d'atténuation des risques[22] dans le but d'identifier un ensemble commun de mesures visant à atténuer les principaux risques pour la cybersécurité 5G et à aider à hiérarchiser les mesures d'atténuation dans les plans aux niveaux européen et national. La stratégie en matière de cybersécurité pour la décennie numérique souligne l'importance de la sauvegarde des réseaux mobiles large bande de prochaine génération, et contient un appendice spécifique sur les prochaines étapes de la cybersécurité des réseaux 5G[23]. Le cadre de certification de l'UE comprend l'élaboration en cours d'un programme de certification de cybersécurité pour la 5G[24].

Défis liés à la mise en œuvre et au contrôle du respect des dispositions

L'élaboration de politiques est essentielle, tout comme mettre l'accent sur une mise en œuvre efficace. Des mécanismes de signalement, le respect des normes internationales et des mesures d'application pratiques sont nécessaires pour garantir la robustesse de la cybersécurité des réseaux 5G. De nouveaux cadres introduisant des changements importants pour la sécurité des réseaux de télécommunication exigeront que les fournisseurs s'acquittent en permanence d'un processus de conformité et, par conséquent, d'un engagement étroit avec l'industrie. Au **Royaume-Uni**, l'Ofcom utilise un modèle de surveillance dans le cadre de son régime de sécurité des télécommunications et collabore avec les équipes réglementaires et techniques des fournisseurs de télécommunication. Le régulateur considère que la mise en œuvre n'est pas uniquement une question de mesures techniques. Elle nécessite un changement culturel dans la façon dont les fournisseurs de télécommunications conçoivent la sécurité, à savoir les obliger à identifier et à assumer la responsabilité des parties de leurs réseaux et services qu'ils ont sous-traitées. La participation au niveau de la direction et l'obtention de l'engagement et du parrainage de la part du gouvernement, des régulateurs et de l'industrie sont une condition préalable pour réussir.

En **Malaisie**, le gouvernement a approuvé un nouveau projet de loi sur la cybersécurité, qui prévoit la création d'une agence unique pour la gestion de toutes les infrastructures critiques, y compris les télécommunications. Le régulateur élabore actuellement un ensemble d'exigences à l'intention des opérateurs pour rendre compte de leur conformité en matière de sécurité. L'un des opérateurs du pays a souligné que la mise en œuvre de la nouvelle politique peut être difficile, car elle implique de communiquer sur les risques et d'articuler des exigences de sécurité minimales qui demandent du temps, de l'argent et beaucoup de travail en concertation, et influe souvent sur les considérations pour les actionnaires. Pour les opérateurs actionnaires, les structures, politiques et réglementations en matière de sécurité ne sont pas toujours cohérentes, ce qui peut poser un défi aux équipes de sécurité, d'où la nécessité d'impliquer toutes les équipes, y compris les responsables de niveau supérieur, lors de la réflexion sur les nouveaux cadres de sécurité.

5. L'investissement dans l'éducation et la formation de la main-d'œuvre pour gérer les complexités de la cybersécurité 5G reste au premier rang des priorités

Selon Allied Market Research[25], le marché mondial de la sécurité 5G devrait atteindre 37,8 milliards USD d'ici 2031, et s'accompagner d'une demande croissante de professionnels de la cybersécurité, en particulier ceux qui ont des compétences spécialisées pour protéger les réseaux 5G. Les pays, les organisations et les institutions doivent accorder la priorité à la formation et au recrutement de la main-d'œuvre pour assurer la progression de la cybersécurité 5G. Il est actuellement difficile de trouver les compétences spécialisées nécessaires sur le marché du travail; en outre, il est difficile d'atteindre la parité hommes-femmes lors de l'embauche. Si la main-d'œuvre n'est pas prête, la transition vers la 5G ralentira et deviendra de plus en plus difficile. Alors que

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

les pays devraient accorder la priorité à la formation et à l'éducation par le biais de programmes nationaux, le secteur privé peut également envisager des programmes de formation et de perfectionnement des compétences, car la participation de l'ensemble du secteur est nécessaire pour garantir que les besoins sont satisfaits.

Un exemple de pays qui trouve des solutions aux défis de la main-d'œuvre est la **Türkiye**, qui a augmenté ses investissements dans l'éducation et la formation d'une main-d'œuvre capable de gérer les complexités de la sécurité 5G. Dans le cadre de cet engagement, un site d'essai ouvert 5G Valley a été créé par des institutions clés, notamment l'Autorité des technologies de l'information et de la communication, l'Université technique du Moyen-Orient, l'Université İhsan Doğramacı Bilkent, l'Université Hacettepe et les opérateurs de télécommunication Türk Telekomünikasyon A.Ş., Turkcell İletişim Hizmetleri A.Ş. et Vodafone Telekomünikasyon A.Ş. Ce site est une plate-forme essentielle pour la recherche, le développement et les tests des technologies 5G et postérieures, offrant des possibilités de collaboration entre le monde universitaire et le secteur. Le Conseil d'Administration de la 5G Valley, composé de représentants des institutions précitées, assure la mise en œuvre effective de cette initiative. En fournissant une plate-forme où les universitaires, les chercheurs, les doctorants et les start-ups peuvent s'engager dans des travaux liés aux technologies 5G et postérieures, le site d'essai ouvert favorise non seulement l'innovation, mais contribue également au développement d'une main-d'œuvre hautement qualifiée. Cette initiative s'inscrit dans la stratégie de la Türkiye visant à donner la priorité à la sécurité des réseaux 5G et à renforcer leur sécurité grâce à des investissements continus dans l'éducation, la formation et la recherche[26].

6. Au-delà de la 5G : définir l'orientation de la cybersécurité 6G

Bien que la 5G en soit encore à l'étape de planification et de déploiement dans de nombreux pays et régions, dans les activités de recherche-développement et de normalisation, l'attention se porte déjà au-delà des réseaux 5G. À cet égard, à la fin de 2023, le Secteur des radiocommunications de l'UIT (UIT-R) a approuvé le cadre et les objectifs généraux du développement futur des IMT à l'horizon 2030 et au-delà[27], que l'on appelle commercialement la 6G.

Ce cadre souligne que les IMT-2030 devraient contribuer de manière importante à l'amélioration de la sécurité et de la résilience. Il est censé être sécurisé de par sa conception et avoir la capacité de continuer de fonctionner pendant un événement perturbateur, qu'il soit naturel ou causé par l'homme, et de s'en remettre rapidement. Le document réaffirme également que la sécurité et la résilience des systèmes IMT-2030 sont fondamentales pour atteindre les objectifs sociétaux et économiques plus larges.

Dans le contexte des IMT-2030, la sécurité est définie par le cadre comme étant la "*préservation de la confidentialité, de l'intégrité et de la disponibilité des informations, telles que les données d'utilisateur et la signalisation, et la protection des réseaux, dispositifs et systèmes contre les cyberattaques telles que le piratage, le déni de service distribué, les attaques par intercepteur, etc.*". La résilience est définie comme étant la "*capacité des réseaux et des systèmes à continuer de fonctionner correctement pendant et après une perturbation naturelle ou causée par l'homme, telle qu'une perte de la source principale d'alimentation, etc.*".

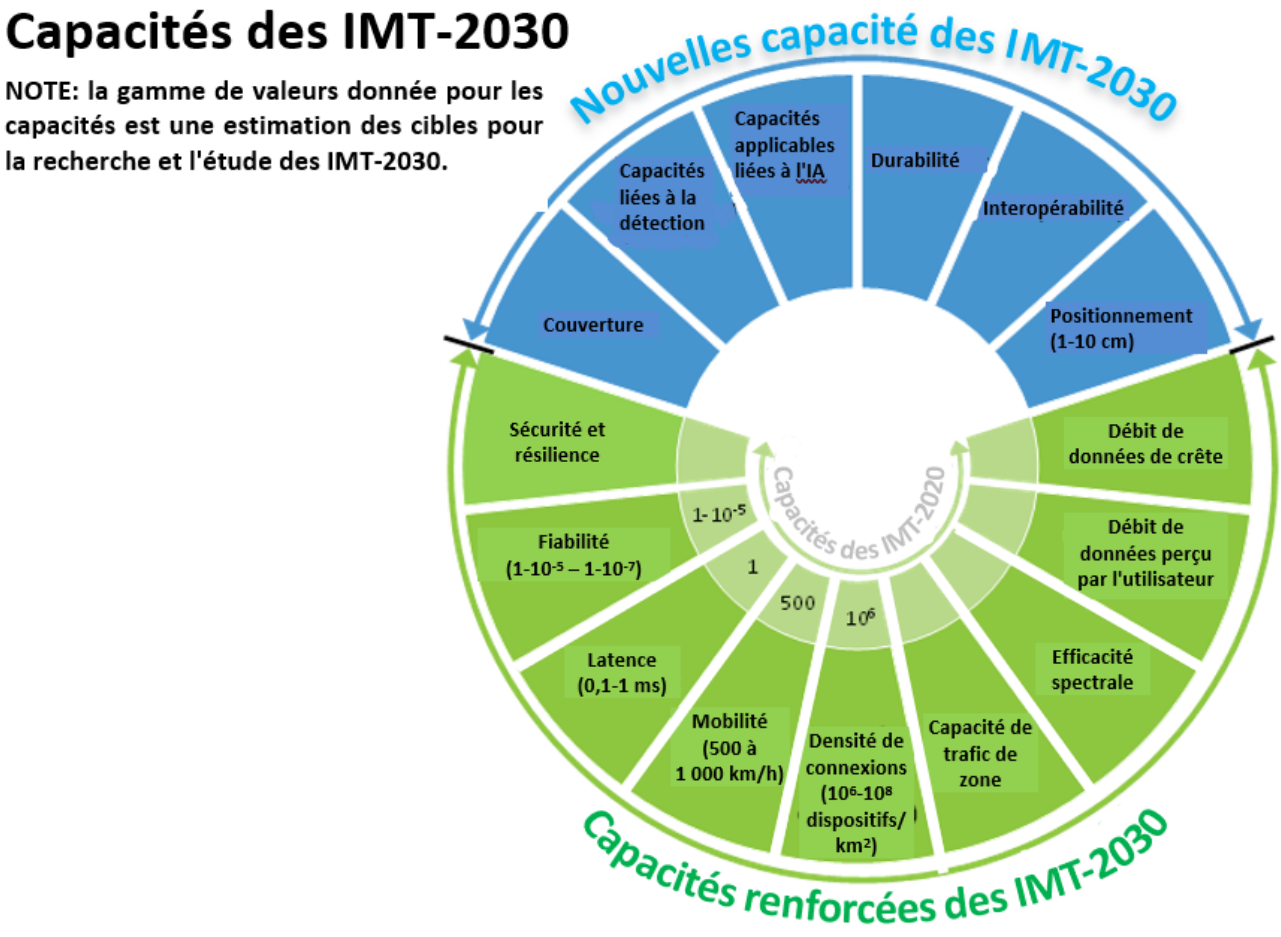
Il est devenu évident que la 6G est envisagée et que le début de ses processus de normalisation est conçu avec une forte préoccupation liée à la sécurité et à la résilience, à la différence des premières étapes de conception de la technologie 5G, y compris du point de vue de la normalisation. Une comparaison avec les IMT-2020 (commercialement connue sous le nom de 5G) approuvée en 2015[28] illustre de façon saisissante le changement d'approche avec la prise en compte de la nécessité d'aborder comme il se doit la cybersécurité et la cyberrésilience, en tant que piliers de la transformation numérique et de l'économie numérique.

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

[27] Recommandation UIT-R M.2160, disponible à l'adresse https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en.

[28] Recommandation UIT-R M.2083, disponible à l'adresse https://www.itu.int/rec/R-REC-M.2083-0-201509-I.

Figure 1: Capacités des IMT-2030



Source: Recommandation UIT-R M.2160

Suivez les travaux sur la **Question 3/2** "Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité" confiée à la **Commission d'études 2 de l'UIT-D pour la période d'études 2022-2025**

Site web sur la Question 3/2:
http://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/questions/Question-3-2.aspx.

Listes de diffusion: d22sg3q2@lists.itu.int, cliquez ici pour vous abonner.

Site web des commissions d'études de l'UIT-D: www.itu.int/itu-d/sites/studygroups/.

Faites-nous part de votre avis en nous écrivant à devSG@itu.int. Tél.: +41 22 730 5999.

ITUPublications
Published in Switzerland, Geneva, 2024

ITU Disclaimer: https://www.itu.int/en/publications/Pages/Disclaimer.aspx

International Telecommunication Union
Place des Nations, CH-1211 Geneva Switzerland