5G : l'UE se cherche un modèle de certification de sécurité

Comment assurer, à l'échelle de l'UE, une approche coordonnée de la sécurité des réseaux 5G ? Voilà près de deux ans que la Commission européenne a émis une recommandation à ce sujet.

Il en a résulté, en particulier, une « boîte à outils » mise à disposition des États membres début 2020. Elle contient une trentaine de mesures techniques et stratégiques. Leur objectif : minimiser neuf domaines de risque.

	Catégories de risque
Scénarios de risque liés à des mesures de sécurité insuffisantes	*R1: Mauvaise configuration des réseaux*
	R2: Insuffisance des contrôles d'accès
Scénarios de risque liés à la chaîne d'approvisionnement de la 5G	*R3: Faible qualité des produits*
	R4: Dépendance à l'égard d'un seul fournisseur au sein de certains réseaux ou manque de diversité au niveau national:
Scénarios de risque liés au modus operandi des principaux auteurs d'actes malveillants	*R5: Ingérence de l'État dans la chaîne d'approvisionnement de la 5G*
	R6: Exploitation des réseaux 5G par la criminalité organisée ou groupe criminel organisé visant des utilisateurs finaux
Scénarios de risque liés aux interdépendances entre les réseaux 5G et d'autres systèmes critiques	*R7: Perturbation importante d'infrastructures ou de services critiques*
	R8: Défaillance massive des réseaux en raison d'une interruption de l'alimentation électrique ou d'autres systèmes d'appoint
Scénarios de risque liés aux équipements des utilisateurs finaux	*R9: Exploitation de l'internet des objets*

Sur le volet stratégique, il s'agit notamment :

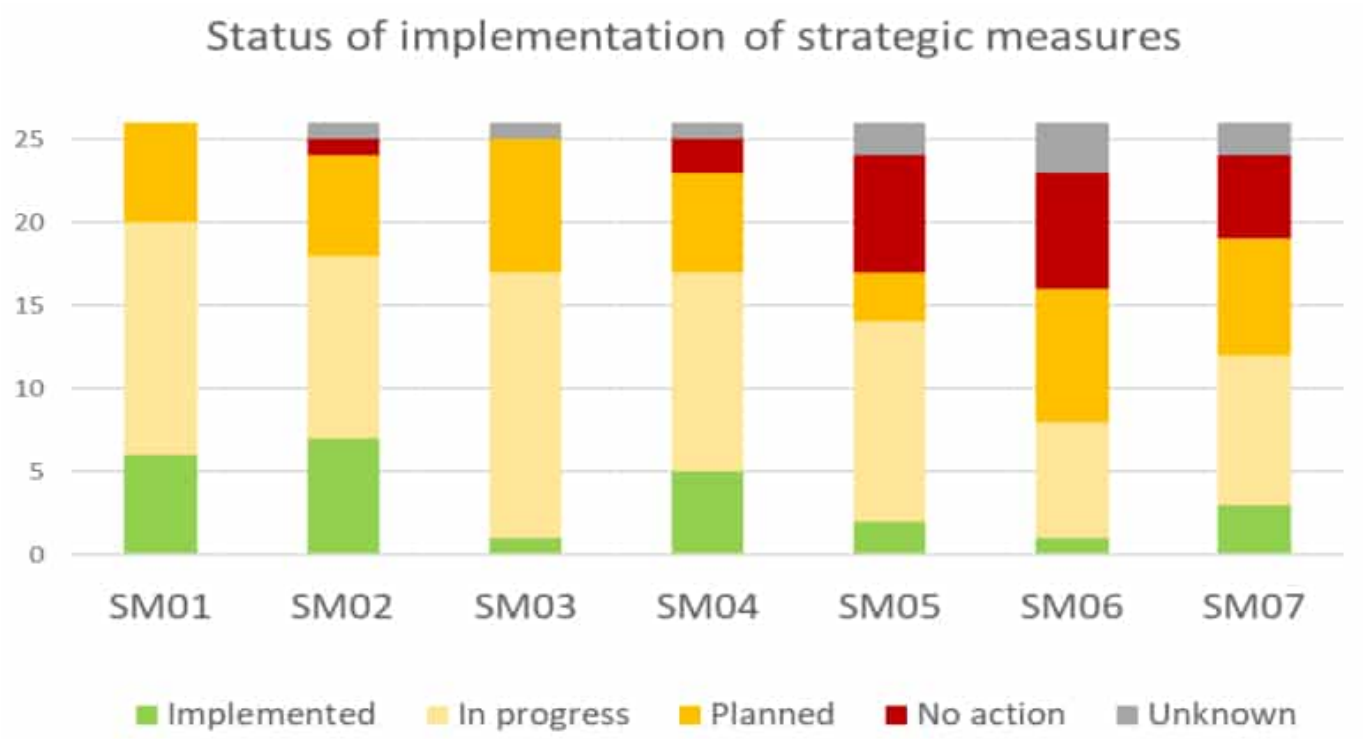
- de renforcer le rôle des autorités nationales ;
- d'auditer les opérateurs de réseaux mobiles ;
- d'évaluer les profils de risque des fournisseurs d'équipements et de services ;
- de garantir la diversité de ces mêmes fournisseurs.

Côté technique, les mesures englobent le contrôle d'accès, les fonctions réseau virtualisées ou encore la sécurité des logiciels. Elles abordent aussi la question des certifications. En premier lieu pour les composants, spécifiques ou non aux réseaux 5G.

La Commission vient d'engager une initiative sur ce point. Elle a chargé l'ENISA (Agence de l'UE pour la cybersécurité) de développer un mécanisme de certification. Le Cybersecurity Act, en application depuis la mi-2019, ouvre la voie à une telle démarche. La stratégie européenne de cybersécurité le complète. Sa dernière actualisation remonte à la mi-décembre. Elle inclut un bilan sur l'implémentation de la « boîte à outils ».

Une prime à la loi « anti-Huawei »

La Commission souhaiterait que le processus soit finalisé d'ici à la mi-2021. Pour l'accompagner, elle n'exclut pas de mettre à contribution des leviers de financement tels que le programme Digital Europe. Le point d'étape publié en juillet 2020 a donné une idée de l'avancement des États membres sur la mise en place des différentes mesures.



La France se distingue sur trois mesures stratégiques. En l'occurrence, le renforcement du pouvoir des autorités, ainsi que la capacité de contrôle des fournisseurs « à risque » et de l'externalisation des fonctions réseau. Sa principale arme : la loi du 1er août 2019 qu'on a surnommée « anti-Huawei ». Elle impose une autorisation gouvernementale pour la fourniture, le déploiement et à l'exploitation d'équipements 5G jugés stratégiques.

Au niveau européen, le niveau de maturité à l'été 2020 était encore bas sur trois mesures stratégiques :

- Diversifier les fournisseurs pour éviter toute dépendance
- Assurer un équilibre adéquat de ces fournisseurs à des fins de résilience nationale
- Détecter les investissements étrangers dans la chaîne de valeur de la 5G

Sur les mesures techniques, la France n'est pas citée en exemple. Au global, le niveau d'avancement est bas sur :

- Les travaux d’intégration de la sécurité dans les standards 5G
- La sécurité des fonctions réseau virtualisées
- L’intégration d’exigences de sécurité dans les cahiers des charges des opérateurs

Illustration principale © Melpomeme – shutterstock.com