Sécurité des réseaux 5G : l'UE dégaine sa « boîte à outils »

Peut-on rêver, dans l'Union européenne, d'une approche coordonnée sur la sécurité des réseaux 5G ?

Bruxelles a franchi une étape de plus dans ce sens avec l'approbation, ce 29 janvier 2020, d'une « boîte à outils commune ».

Elle regroupe une trentaine de mesures destinées à répondre aux risques qu'ont identifiés les États membres.

Un rapport d'octobre 2019 liste les risques en question.

	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*

Les mesures figurant dans la « boîte à outils » sont de deux natures : stratégique et technique.

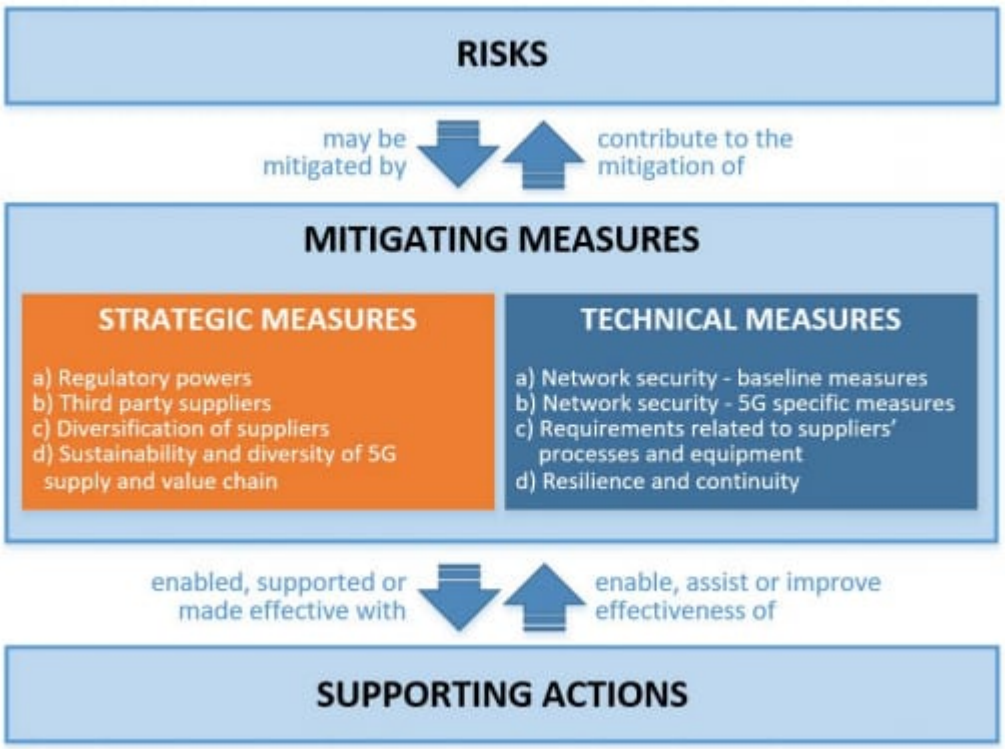
Sur le volet stratégique sont abordés entre autres :

- Le renforcement du rôle des autorités nationales
- L'audit des opérateurs de réseaux mobiles
- L'évaluation du profil de risque des fournisseurs d'équipements, mais aussi des

fournisseurs de services
- La diversité de ces fournisseurs
- La nécessité d'une chaîne d'approvisionnement et de valeur « durable et diversifiée »

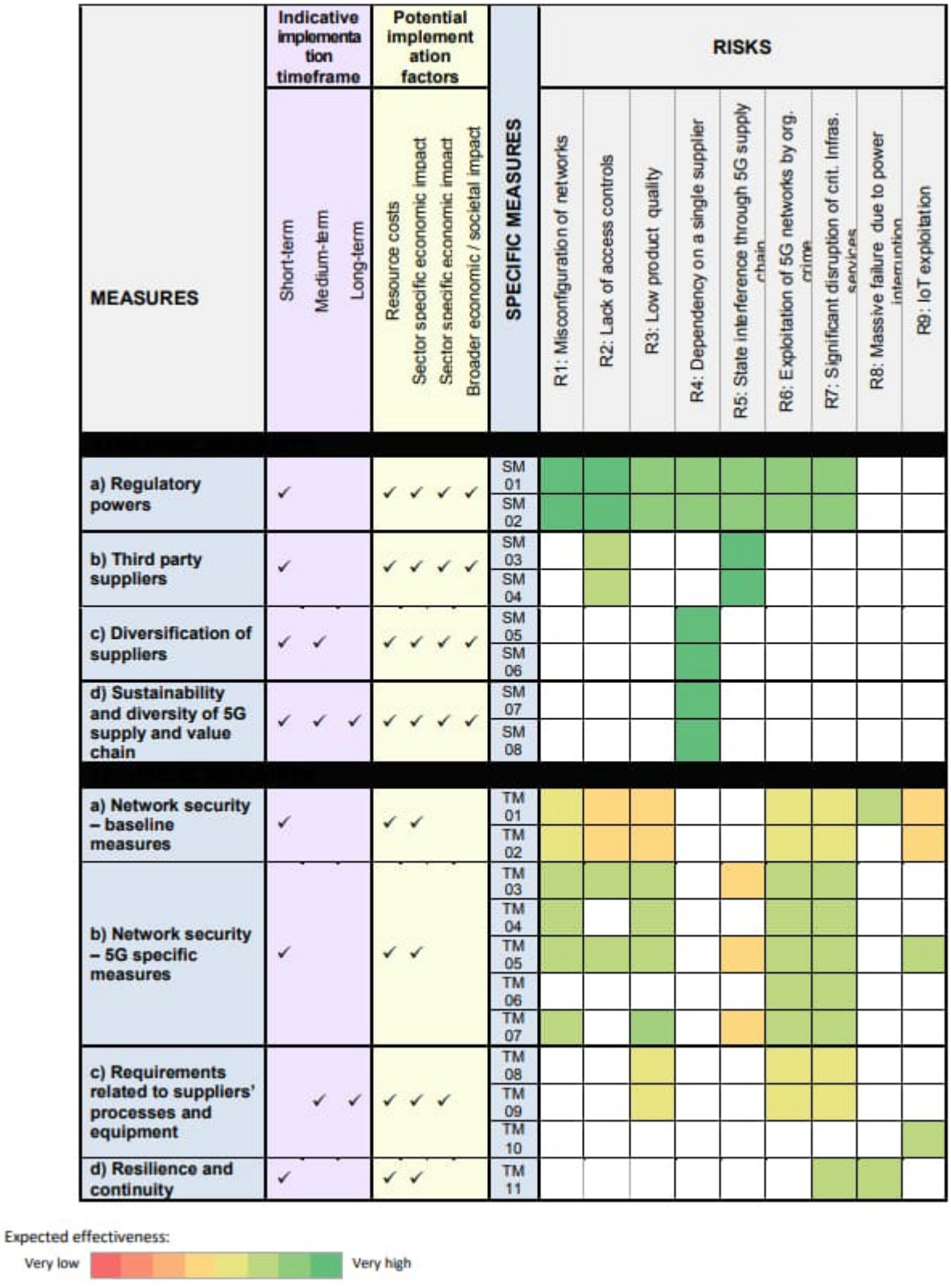
Côté technique, les mesures visent essentiellement :

- Le contrôle d'accès
- Les fonctions réseau virtualisées
- L'orchestration des réseaux
- Leur sécurité physique
- La sécurité des logiciels
- Les certifications



Ces mesures sont censées poser la « base d'une approche coordonnée », à condition d'être combinées de manière appropriée.

La Commission propose, à cet effet, plusieurs options. Elle en évalue le degré d'efficacité, le coût et la durée d'implémentation.



Les États membres sont appelés à mettre en place les mesures adéquates d'ici au 30 avril 2020… s'ils ne l'ont déjà fait.

Bruxelles rappelle que l'implémentation de la plupart des mesures techniques peut être réalisée dans le contexte de la transposition du Code européen des communications électroniques.

Et d'insister sur la nécessité de stratégies multifournisseurs, même au risque d'un accroissement de la surface d'attaque.

Photo d'illustration © Melpomeme – Shutterstock.com