Le groupe de coopération NIS a été créé dans le cadre du lancement, par le Parlement européen le 6 juin 2016, de la directive sur la sécurité des réseaux et des systèmes d'information (Directive on Security of Network and Information Systems), appelée directive NIS. Constitué des représentants des membres de l'Union européenne, de la Commission européenne et de l'agence de cybersécurité de l'Union (l'ENISA – European Network and Security Agency), **il a pour mission d'assurer une coopération stratégique**, passant par l'échange d'informations, entre les États membres en matière de cybersécurité.

Le groupe a publié en octobre 2019 un rapport intitulé « Évaluation coordonnée par l'Union européenne des risques liés à la cybersécurité des réseaux 5G ». **Ces réseaux de télécommunications de nouvelle génération vont jouer un rôle central dans la transformation numérique de la société,** et de l'économie en particulier, au sein de l'Union européenne, allant bien au-delà de la fourniture de services de télécommunications aux particuliers, avec une large gamme de nouvelles applications et d'objets connectés, activités dont les revenus atteindraient 225 milliards d'euros en 2025.

L'une des caractéristiques des réseaux 5G est d'améliorer les fonctionnalités de communication des objets connectés à la périphérie des réseaux, leur architecture est de ce fait moins centralisée que celle des réseaux de génération antérieure. « *Certaines fonctions des réseaux centraux peuvent être intégrées dans d'autres parties des réseaux, ce qui rend les équipements correspondants plus sensibles* ». Une architecture moins centralisée « *augmente donc la surface d'éventuelles attaques et le nombre de points d'entrée potentiels pour les attaquants* ». En outre, les réseaux 5G requièrent un plus grand nombre de logiciels pour faire fonctionner les équipements, ce qui entraîne « *des risques accrus liés aux processus de développement et de mise à jour des logiciels,* […] *et de nouveaux risques d'erreurs de configuration* ».

Ce sont les principales raisons pour lesquelles les opérateurs de télécommunications risquent de devenir plus dépendants de leurs fournisseurs extérieurs. Aussi le groupe NIS préconise-t-il d'en diversifier le nombre pour éviter une dépendance trop grande vis-à-vis d'un seul. **De l'avènement des réseaux 5G vont dépendre de « *nombreuses applications informatiques critiques* »,** non seulement en matière de confidentialité des données et de respect de la vie privée, mais également en matière d'intégrité et de disponibilité de ces réseaux, une source de « *préoccupations majeures en termes de sécurité nationale et défi majeur pour la sécurité dans une perspective européenne* ».

Le groupe NIS estime que **ces défis créent « *un nouveau paradigme de sécurité,* ***ce qui rend nécessaire une réévaluation de la politique actuelle et du cadre de sécurité applicable au secteur et à son écosystème et indispensable pour que les États membres prennent les mesures d'atténuation nécessaires*** ». Dans une phase ultérieure, le groupe veillera à l'application de ces recommandations et proposera une « *boîte à outils de mesures de gestion des risques appropriées, efficaces et proportionnées pour atténuer les risques en matière de cybersécurité* ». En outre, les experts soulignent l'importance de disposer d'une capacité industrielle européenne en termes de « *développement de logiciels, de fabrication d'équipements, d'essais en laboratoire, d'évaluation de la conformité, etc*. ».

Sans jamais citer le groupe chinois Huawei, premier fournisseur mondial d'antennes de téléphonie mobile, dénoncé depuis 2018 par les services de renseignement des États-Unis, du Canada, du Royaume-Uni, d'Australie et de Nouvelle-Zélande (les *« 5 eyes »*, voir *La rem* n°49, p.101), les auteurs du rapport qui identifient les grands défis en matière de sécurité, que l'avènement des réseaux 5G est susceptible d'engendrer ou d'intensifier, **mettent en garde les membres de l'Union quant à leur choix en matière de fournisseurs de matériels,** notamment ceux qui sont liés à un pays non démocratique.

La France s'est d'ailleurs déjà dotée, en juillet 2019, d'une nouvelle législation en matière de cybersécurité, dite loi Huawei, qui soumet les opérateurs de télécommunications français à un régime d'autorisation préalable, délivrée par le Premier ministre, à l'exploitation d'équipements pour leurs réseaux 5G.

EU coordinated risk assessment of the cybersecurity of 5G networks, NIS Cooperation Group, October 9, 2019.