FRANCE22
FRENCH PRESIDENCY OF THE COUNCIL OF THE EUROPEAN UNION

Réunion informelle des ministres des télécommunications

Nevers, 9 mars 2022

Appel de Nevers à renforcer les capacités de l'UE en matière de cybersécurité

Les récentes cyberattaques qui ont visé l'Ukraine dans un contexte de tensions géopolitiques croissantes ont montré l'importance de la dimension cybernétique dans les conflits actuels. Tout en reconnaissant l'importance pour l'UE de soutenir fermement la cyber-résistance de l'Ukraine, l'effet de débordement possible de ces cyber-attaques sur les réseaux européens souligne également la nécessité pour l'UE d'aller de l'avant avec un plan ambitieux et complet pour sa cybersécurité.

Les infrastructures critiques telles que les réseaux de télécommunications et les services numériques sont d'une importance capitale pour de nombreuses fonctions essentielles de nos sociétés et constituent donc une cible de choix pour les cyberattaques. Les fournisseurs et les opérateurs de ces infrastructures et services sont essentiels pour la cybersécurité de l'UE et il convient de tirer parti de leur rôle en garantissant la cybersécurité de leurs produits et services au moyen de réglementations et d'incitations, et en structurant leur coopération avec les cyberautorités nationales, le cas échéant, afin de mieux détecter et prévenir les cyberattaques.

*

En raison du paysage géopolitique actuel, nous souhaitons entreprendre des actions immédiates de renforcement de la cybersécurité.

En conséquence, nous, ministres en charge des télécommunications, à l'unanimité :

1. **Reconnaissons l'importance de renforcer l'Union et son marché unique** en améliorant la coopération entre le secteur public et les acteurs de confiance en matière de cybersécurité. En outre, les États membres continueront à promouvoir un cyberespace ouvert, libre, stable et sûr dans un modèle multipartite avec le secteur privé et la société civile.

2. **Soulignons que l'UE saisit les possibilités offertes par la révision actuelle de la directive sur la sécurité des réseaux et de l'information,** en s'efforçant de mieux protéger ses entités contre les cybermenaces. **Nous attendons donc l'adoption rapide de la directive NIS2.**

3. **Invitons la Commission à finaliser l'adoption des propositions clés, à mettre rapidement en œuvre la législation déjà existante, notamment l'opérationnalisation du Centre de Compétence,** pour garantir que les infrastructures, les technologies, les produits et les services numériques soient sécurisés, afin d'envoyer un signal clair sur les ambitions de l'UE sur ce sujet, de soutenir et aider les entreprises à relever le défi. D'autres progrès pourraient être réalisés avec la mise en place de normes communes de cybersécurité pour les appareils et services connectés, grâce à la loi sur la résilience en matière de cybersécurité. **Nous souhaitons donc une intégration rapide de ces sujets dans la future loi sur la résilience de la cybersécurité et une publication rapide.**

4. **Exhortons l'Union européenne et ses États membres à assurer la cybersécurité et la résilience des infrastructures et réseaux de communication européens.** En outre, **nous invitons les autorités compétentes, telles que l'Organe des régulateurs européens des communications électroniques (ORECE), l'Agence de l'Union européenne pour la cybersécurité (ENISA) et le Groupe de coopération pour la sécurité des réseaux et de l'information (NIS), ainsi que la Commission européenne, à formuler des recommandations, fondées sur une évaluation des risques,** à l'intention des États membres et de la Commission européenne afin de renforcer la résilience des réseaux et infrastructures de communication au sein de l'Union européenne, y compris la mise en œuvre de la boîte à outils 5G.

5. **Encourageons le renforcement de la coopération de l'UE et renforçons notre solidarité et notre assistance mutuelle en s'appuyant sur les réseaux existants,** tant au niveau technique et opérationnel avec CSIRTs-Network et EU CyCLONe qu'au niveau politique au sein du Conseil, afin d'assurer notre sécurité et notre résilience dans le domaine numérique.

6. **Augmentons les fonds de l'UE pour renforcer de manière significative les efforts des États membres dans l'augmentation du niveau global de cybersécurité, par exemple en encourageant l'émergence de fournisseurs de services de cybersécurité de confiance,** tels que l'audit de cybersécurité et la réponse aux incidents. Encourager le développement de tels fournisseurs européens devrait être une priorité de la politique industrielle de l'UE dans le domaine de la cybersécurité,afin de développer notre écosystème de cybersécurité tout en renforçant la cybersécurité des opérateurs à risque, qui seraient certainement visés en cas de conflit, nous pensons qu'un tel financement serait efficace et permettrait d'augmenter rapidement le niveau de cybersécurité au sein de l'UE.

7. **Approuvons la mise en œuvre d'un nouveau Fonds d'intervention d'urgence pour la cybersécurité qui sera mis en place par la Commission.** Le paysage géopolitique actuel et ses répercussions dans le cyberespace renforcent la nécessité pour l'UE de

se préparer pleinement à faire face à des cyberattaques de grande ampleur. Un tel fonds contribuera directement à cet objectif.

8. **Croyons fermement que les institutions, agences et organes de l'UE devraient prendre des mesures pour renforcer davantage leur cybersécurité et leur sécurité de l'information,** car l'UE est devenue un acteur stratégique clé dont le rôle sur la scène internationale exige de sécuriser ses données et ses informations.

Enfin, nous réitérons notre ferme engagement à maintenir l'infrastructure numérique et les réseaux de télécommunication ukrainiens en état de fonctionnement, tout en renforçant la sécurité des données et des réseaux.