Note de cadrage

Session V: Vers un renforcement de l'effort collectif de l'UE pour améliorer la cyber-résilience et lutter contre la désinformation

Introduction

Au cours des dernières années, le développement des technologies numériques a atteint un rythme très élevé, sans précédent, et a commencé à affecter visiblement pratiquement tous les aspects de la vie quotidienne, de l'économie et de la politique mondiales. L'Union européenne a donc reconnu assez rapidement que l'un de ses objectifs devait être d'accroître les capacités technologiques et les compétences dans le domaine de la cybersécurité, ainsi que de mettre en place un marché unique numérique solide. Un élément important de l'approche de l'UE en matière de cybersécurité a également été la convergence notable de la compréhension militaire et civile de la cybersphère et le renforcement parallèle de l'Agence de l'Union européenne pour la cybersécurité, créée en 2004. Les décisions de la Commission européenne en 2017, qui a adopté une stratégie en trois volets pour la cybersécurité au sein de l'UE, ont également été une conséquence de la prise de conscience croissante de l'importance de la cybersécurité. Le premier pilier a renforcé la résilience de l'UE face aux cyberattaques, le deuxième a permis de mettre en place une cyberprévention efficace et le troisième a renforcé la coopération internationale dans le domaine de la cybersécurité. C'est pourquoi la stratégie adoptée est souvent appelée « résilience, prévention et défense », ces principes étant des éléments clés de la politique de l'UE en matière de cybersécurité

Les principes clés de l'approche cybernétique sont les suivants: 1) évolution vers un marché unique de la cybersécurité; 2) mise en œuvre et évaluation efficaces de la directive sur la sécurité des réseaux et des systèmes d'information; 3) résilience grâce à une réponse rapide en cas de crise; 4) création d'une base solide de cybercompétences dans l'UE; 5) promotion de la cyberhygiène et de la sensibilisation aux menaces; 6) identification des acteurs malveillants; 7) coopération public-privé dans la lutte contre la cybercriminalité; 8) amélioration de la réponse politique dans la cybersphère; 9) renforcement des capacités dans le domaine de la cybersécurité et 10) accent mis sur la cybersécurité dans les relations extérieures. Sur ce dernier point, une stratégie d'action détaillée a été présentée par l'UE en 2018 à travers, entre autres, la création d'un Observatoire européen des médias numériques pour améliorer la détection des cyberattaques et de la désinformation, travailler avec les plateformes en ligne ainsi que sensibiliser les citoyens et leur permettre de répondre à la désinformation en ligne.

Le fonctionnement de l'Observatoire européen des médias numériques montre que la protection de la cybersphère s'accompagne d'une prise de conscience accrue, au sein de l'UE, des différentes formes d'activités de désinformation en ligne. L'UE considère comme désinformation les contenus faux ou trompeurs diffusés dans l'intention d'induire en erreur ou de tirer un avantage économique ou politique, et susceptibles de porter atteinte à l'intérêt public. L'UE souligne que la désinformation inclut également des contenus trompeurs, partagés certes sans intention malveillante, mais entraînant des effets néfastes du point de vue des sociétés européennes. La diffusion aussi bien de la désinformation que de sa forme particulière qu'est la mésinformation — c'est-à-dire une information trompeuse diffusée sans intention de nuire — peut menacer les démocraties européennes et entraîner de nombreuses conséquences néfastes, telles que la promotion, voire l'amplification, de l'influence d'acteurs hostiles extérieurs, ainsi que l'exposition de la santé, de la sécurité et de l'environnement de l'UE à divers risques aux effets imprévisibles et incalculables. Il convient de garder à l'esprit que les campagnes de désinformation à grande échelle constituent un défi majeur pour l'Europe et nécessitent une réponse coordonnée des pays de l'UE, des institutions européennes, des plateformes en ligne, des médias d'information et des citoyens de l'UE eux-mêmes.

Dans le nouveau cycle institutionnel 2024-2029, la Commission européenne promeut un projet de bouclier pour la démocratie, dont l'une des priorités est la lutte contre la désinformation. L'objectif le plus rècent de l'UE est donc de développer un réseau européen de vérificateurs de faits, pour garantir que ces informations soient disponibles dans tous les États membres et dans toutes les langues officielles de l'UE. Cette initiative visant à renforcer les capacités de ces acteurs s'appuiera sur les travaux de l'Observatoire européen des médias numériques. La mise en œuvre du programme «Europe numérique 2025-2027» est également une nouveauté. Ce programme doit se concentrer sur le déploiement de l'intelligence artificielle (IA) et son utilisation par les entreprises et les gouvernements, l'informatique en nuage et les données, la cyberrésilience et la culture numérique, ainsi que la lutte contre la désinformation.

Défis actuels

L'ampleur du défi de la cybersécurité est parfaitement démontrée par le dernier rapport de l'Agence de l'Union européenne pour la cybersécurité présenté en mars 2025. Ce rapport évalue la maturité et la résilience des secteurs critiques couverts par la directive concernant les mesures visant à garantir un niveau élevé commun de cybersécurité sur le territoire de l'Union (NIS2) face aux cybermenaces. Ce qui est important, c'est que cette analyse révèle des disparités importantes : alors que les secteurs de l'énergie, de la banque et des télécommunications sont en tête, d'autres, comme l'administration publique, la santé ou

l'espace, restent dans ce que l'on appelle la « zone à risque ». Ce rapport constitue la première analyse complète dans laquelle la maturité et la résilience des secteurs visés par la directive NIS2 ont été évaluées, fournissant à la fois un comparatif général et une analyse détaillée de chaque secteur. Ce document vise à aider les États membres et les autorités nationales à identifier les lacunes et à hiérarchiser l'utilisation efficace des ressources afin de garantir un niveau élevé de cybersécurité dans l'ensemble de l'Union. L'étude est basée sur des données provenant des autorités nationales, des entreprises et des institutions de l'UE telles qu'Eurostat. Le rapport ne se contente pas d'identifier les lacunes et les risques existants, il propose également un ensemble complet de recommandations stratégiques destinées aux États membres, aux autorités de régulation et aux secteurs concernés par la directive NIS2. Les secteurs les mieux notés dans l'étude ont bénéficié d'une surveillance réglementaire importante, d'investissements mondiaux, d'orientations politiques et de solides partenariats public-privé, et leur résilience est essentielle pour la stabilité sociale et économique. Parmi les secteurs ayant atteint un niveau suffisant de maturité, le rapport inclut notamment les infrastructures numériques, telles que les services Internet de base, les services de confiance, les centres de données et les services en cloud. Certes, il reste encore des défis à relever en raison de l'hétérogénéité inhérente et de la nature transfrontalière du secteur ainsi que de l'inclusion d'entités qui n'étaient pas réglementées auparavant, mais le niveau de cyber-résilience est relativement élevé.

En outre, quatre secteurs et deux sous-secteurs situés dans la « zone à risque » ont été identifiés. Il s'agit de 1) la gestion des services TIC; 2) l'espace; 3) l'administration publique; 4) le secteur maritime; 5) la santé et 6) le gaz. Ces secteurs doivent faire l'objet d'une attention particulière afin de s'assurer que les écarts de maturité identifiés soient traités de manière à permettre aux entités qui les composent de faire face efficacement à des défis supplémentaires. Le rapport montre que tous les secteurs sont confrontés à des défis pour développer leur propre maturité et répondre aux exigences de la directive NIS2. Pour mieux les soutenir, une coopération plus étroite au sein de ces secteurs et entre eux est recommandée, ainsi que l'élaboration de lignes directrices sectorielles pour la mise en œuvre de mesures de gestion des risques.

Ces recommandations ont mis en évidence la nécessité de développer les capacités nationales en matière de cybersécurité, en mettant l'accent sur les secteurs situés dans la « zone à risque ». L'une des options est de mettre en place des programmes spécifiques de soutien technique et de contenu pour les régulateurs et les organisations du secteur public. Il est également important d'accroître la disponibilité de formations spécialisées, d'exercices sur la cybersécurité et d'outils d'analyse des risques et de réponse aux incidents. En outre, l'Agence de l'Union européenne pour la cybersécurité met fortement l'accent sur la nécessité de promouvoir le partage d'informations et la coopération intersectorielle. Il est suggéré

d'élargir le rôle de structures telles que les ISAC (*Information Sharing and Analysis Centres*), qui devraient fonctionner non seulement au niveau national mais aussi au niveau européen. Le rapport souligne que des exercices conjoints, la mise en commun de scénarios de menace et le développement de plateformes d'échange d'informations sont essentiels pour accroître la sensibilisation et la préparation. Enfin, l'intégration des analyses des risques sectoriels dans les processus décisionnels au niveau des politiques publiques revêt une importance cruciale pour garantir la cybersécurité. Certains secteurs comme l'énergie ou la banque utilisent déjà ces approches, mais il est nécessaire d'étendre cette pratique à davantage de branches, en particulier dans des secteurs sensibles comme la santé, l'administration publique ou les services TIC. Cela devrait permettre une meilleure planification des ressources et des investissements ainsi qu'une mise en œuvre plus efficace des stratégies de sécurité numérique. Le rapport recommande également de poursuivre le développement d'exercices de cybersécurité au niveau paneuropéen. Les exercices Cyber Europe, qui comprennent des scénarios de défaillance intersectorielle, devraient être élargis pour inclure des éléments de technologie opérationnelle, des chaînes d'approvisionnement et des dépendances intersectorielles critiques. L'intégration de secteurs qui ont jusqu'à présent rarement participé à de tels événements, comme l'espace, le chauffage urbain et l'hydrogène, revêt une importance particulière.

Dans le cas de la désinformation, les défis sont fonction de la complexité du phénomène lui-même. En principe, elle se présente sous trois formes: 1) la désinformation diffusée par des acteurs extérieurs (États ou organisations, par exemple); 2) la désinformation locale, qui reproduit souvent la désinformation extérieure, mais ce n'est pas nécessairement la règle; et 3) la désinformation qui implique la diffusion de contenus manipulateurs ou faux par des individus, souvent à leur insu, par le biais de divers moyens de communication (Tik Tok, plateforme X, Facebook). Afin de lutter efficacement contre la désinformation et la mésinformation, un certain nombre d'actions et de mesures sont nécessaires, parmi lesquelles : 1) le financement et le soutien d'entités qui identifient et enregistrent des cas spécifiques de désinformation, par exemple les « fake news » (*fact-checking*); 2) le développement des ressources humaines, principalement en recrutant du personnel qualifié; 3) une communication efficace, y compris la création de récits véridiques et intéressants et la diffusion efficace de messages qui atteignent le public; 4) la construction des relations et de la confiance, car les acteurs de la lutte contre la désinformation doivent constamment renforcer leur crédibilité et mener des campagnes positives pour susciter la confiance et l'engagement des citoyens, tout en comprenant leurs besoins et en tenant compte de l'équilibre délicat dans une société démocratique pluraliste aux opinions et aux points de vue différents (car la lutte contre la désinformation ne peut être un moyen d'imposer une vision unique du monde: si elle est perçue ainsi, elle deviendra elle-même une forme de

désinformation; 5) la transformation numérique, qui donnera accès à des outils numériques efficaces pour l'acquisition et la visualisation de données, la conception graphique et le montage vidéo, ce qui permettra de vérifier le contenu et donc d'assurer la compétence d'esprit critique.

L'importance de la question de la sécurité a été soulignée dans le « Warsaw Call », c'est-à-dire la déclaration commune adoptée par les ministres de l'UE en charge de la cybersécurité le 5 mars 2025 lors d'une réunion informelle organisée par le ministère du Numérique. L'appel de Varsovie est un point de référence important pour l'action future de l'Union européenne en matière de protection de l'espace numérique à une époque où les défis géopolitiques sont de plus en plus nombreux. Il attire l'attention sur les actions spécifiques de l'UE dans les domaines suivants: 1) renforcement de la gestion des crises par l'adoption sans heurts du Cybersecurity Blueprint; 2) renforcement de la coopération civilo-militaire dans le domaine de la cybersécurité, y compris entre l'UE et l'OTAN; 3) adoption d'une feuille de route pour les nouvelles technologies et la prospective stratégique dans le domaine de la cybersécurité; 4) accroissement des efforts de lutte contre la pénurie de cyberspécialistes dans l'UE.

Un défi particulier dans le domaine de la cybersécurité et de la désinformation consiste à renforcer la résilience des sociétés démocratiques face aux situations critiques. Une protection particulière devrait être accordée à toutes les procédures démocratiques, telles que les élections ou les référendums, qui, par définition, deviennent la cible d'attaques et de manipulations accrues. La pratique montre que ce sont des moments particuliers pendant lesquels des acteurs extérieurs désireux d'influencer la scène politique des États membres de l'UE deviennent actifs. De leur côté, les institutions qui défendent la démocratie doivent, dans ce cas, agir de manière particulièrement prudente et mesurée afin de ne pas entamer la confiance du public et de ne pas commencer à être perçues participant à un vaste et complexe processus de désinformation.

Questions à débattre

1. Quel est le rôle de l'Union européenne et de ses institutions dans le renforcement de la résilience de l'UE face aux menaces pesant sur les cyber-infrastructures et aux activités de désinformation?
2. Comment renforcer la cyber-résilience des secteurs dits à risque, tels que la gestion des services TIC, l'administration ou la santé?
3. Quel devrait être le rôle des plateformes numériques dans la garantie de la cybersécurité des sociétés de l'UE?
4. Comment renforcer les organisations de la société civile dans une lutte efficace contre la désinformation?

5. Comment adapter les outils de lutte contre la désinformation lorsque celle-ci évolue et s'ajuste aux changements sociopolitiques?
6. Comment mettre en place des canaux de communication efficaces visant à susciter la confiance dans l'information, ce qui sensibilisera davantage le public au risque de désinformation ou de mésinformation?
7. Quelles sont les possibilités d'utilisation de l'intelligence artificielle (IA) pour garantir un niveau adéquat de cybersécurité et lutter efficacement contre la désinformation?