Note de synthèse et de propositions option Union européenne :

Note à l'attention du directeur départemental

Objet : les enjeux de la cybersécurité au niveau européen

Dès septembre 2017, lors de son discours de la Sorbonne, le président de la République Emmanuel Macron disait « sachons, dans un monde en plein bouleversement, mettre en place des sécurités justes et des régulations efficaces pour le numérique ». Quelques semaines après un sommet sur l'intelligence artificielle (IA) à Paris et alors que la Pologne vient de prendre la présidence du Conseil depuis le 1er janvier 2025 sur le thème des « sécurités », force est de constater que la phrase du président Macron est plus que jamais d'actualité.

En termes de souveraineté numérique, la cybersécurité constitue un aspect particulièrement sensible en ce que les menaces sont protéiformes et peuvent toucher aussi bien l'Union européenne (UE), les Etats membres (EM) et leurs institutions, tout autant que les citoyens. Selon l'UE, elle se définit comme les activités nécessaires pour protéger les réseaux et les systèmes d'information ainsi que les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces.

Ainsi, la cybersécurité protège globalement face à ce que l'on appelle les cybermenaces ou cyberattaques. Dans un monde géopolitique instable avec l'invasion de l'Ukraine par la Russie, les tensions entre les Etats-Unis et la Chine, ainsi que la fin annoncée du multilatéralisme, les enjeux des cybermenaces pour l'UE sont forts. Cela est d'autant plus prégnant que l'ère numérique est dans son commencement. Ces menaces dites hybrides sont donc à considérer au niveau stratégique.

Ainsi, au regard de ces éléments de contexte, quels sont les enjeux de la cybersécurité au niveau européen ?

Nouvelles menaces hybrides en pleine expansion, les cyberattaques tiennent en elles des enjeux stratégiques au regard desquels l'UE s'efforce de protéger ses cibles (I). Dans un contexte géopolitique instable, les menaces autour de la cybersécurité ne doivent pas occulter la nécessité de prendre en compte les enjeux économiques et répressifs afin de protéger les valeurs européennes de l'Etat de droit (II).

I - Nouvelles menaces hybrides en pleine expansion, les cyberattaques tiennent en elles des enjeux stratégiques au regard desquels l'UE s'efforce de protéger ses cibles

A - La cyberattaque, une menace hybride en pleine expansion qui peut menacer des cibles stratégiques

1 - Une menace protéiforme en pleine expansion, difficile à canaliser

Les cybermenaces sont protéiformes en ce qu'elles constituent des menaces diverses et variées. L'agence de l'UE pour la cybersécurité

(ENISA) identifie ainsi 9 menaces principales : les logiciels rançonneurs, les logiciels malveillants, le minage clandestin (pour produire de la cryptomonnaie à l'insu du propriétaire), les attaques par e-mail, les menaces sur les données, les attaques par déni de service et enfin les attaques sur les chaines d'approvisionnement.

Ces attaques sont actuellement en pleine expansion au sein des EM de l'UE. En France, en 2021, selon le groupement d'intérêt public « Action contre la cybermalveillance » (acteurs privés et publics), le piratage des comptes en ligne a augmenté de 139%. Autre exemple en Angleterre où des cyberattaques ont complétement déréglé le système de lampadaires dans la ville de Leicester. Le contexte géopolitique instable implique enfin une hausse de celles-ci, comme ce fût le cas en Nouvelle-Aquitaine avec une augmentation de 25% entre 2023 et 2024.

2 - Une menace qui peut toucher des cibles stratégiques

Les cyberattaques sont des menaces protéiformes qui peuvent toucher des cibles variées, principalement celles à haute teneur stratégique. Sont ainsi notamment concernés les établissements publics, les collectivités territoriales, les administrations publiques ou encore les entreprises privées. Les infrastructures dites sensibles, qui participent notamment à la continuité de la vie de la Nation, peuvent constituer des cibles de choix. Par exemple, en septembre 2021, l'Assistance publique des Hôpitaux de Paris (AP-HP) s'est fait voler les données d'1,4 million de personnes qui avaient passé un test PCR en Ile-de-France. Les particuliers peuvent aussi être touchés.

Sur l'aspect stratégique, l'armée tout comme les forces de l'ordre, le SAMU ou les SDIS constituent des cibles particulièrement sensibles. Le Campus régional de cybersécurité et de confiance numérique de Nouvelle-Aquitaine (C3NA) précise d'ailleurs la vulnérabilité de ces institutions en utilisant par exemple des logiciels de réservation de salles ou de gestion des appels d'urgence. Le SDIS 64 a ainsi été touché en 2023, de même que le SDIS 47 en 2021 et le SDIS 24 en 2019. En l'espèce, c'est bien entendu la protection de l'alerte et du système de gestion opérationnelle qui demeure centrale.

B - Face aux menaces prégnantes envers la cybersécurité, l'UE prend des mesures pour protéger les cibles, notamment celles des EM

1 - Les mesures prises à l'échelle de l'UE

A l'échelle de l'UE, la cybersécurité est prise avec fort intérêt dans la mesure où elle constitue un des éléments de sa souveraineté numérique, et donc de son autonomie stratégique. Ses fondements s'appuient sur la stratégie de cybersécurité de l'UE de 2020 et sur la stratégie de l'UE pour l'union de la sécurité de 2020.

Au niveau de la Commission de l'UE, elle est suivie par la direction générale des réseaux de communication, du contenu et des

technologies (DG Connect). Afin de protéger les cibles, trois directives européennes, adoptées le 14 décembre 2022, visent à lutter contre les menaces qui exposent les infrastructures critiques, le secteur économique et les entreprises et collectivités (NIS 2). L'échéance pour s'y conformer étant fixée au 17 octobre 2024.

En outre, un accord a été trouvé entre les deux co-législateurs que sont le Parlement européen et le Conseil, afin que soit acté le règlement sur la cyberrésilience (décembre 2023). Lorsqu'on y ajoute le premier schéma de certification de cybersécurité pris à l'échelle de l'UE, cela fiabilise notamment le matériel informatique utilisé. En effet, 90% des produits utilisés par l'UE dans le domaine sont importés de Chine, d'où l'enjeu stratégique de garantir cette transparence.

Enfin, avec le règlement de 2019 redéfinissant l'ENISA, la directive NIS 2 vise aussi à renforcer les obligations des entreprises et à introduire des mesures de surveillance plus stricte pour les autorités nationales. Un réseau européen (UE-CyCLONe) a été installé pour améliorer la coordination lors d'incidents de cybersécurité à grande échelle. En décembre 2022, le règlement DORA (Digital operational resilient act) adopté vise lui à renforcer la cybersécurité dans le secteur de la finance.

2 - <u>Le nécessaire accompagnement au sein des Etats membres</u>

Tout d'abord, il est important que les EM informent leurs citoyens et leurs institutions face aux enjeux des cybermenaces. Cette prise de conscience n'est pas toujours pleine et entière comme le montre la 3ème édition du baromètre de la maturité cyber des collectivités. En l'espèce, il convient de noter que les collectivités territoriales de plus de 30 000 habitants constituent les cibles les plus sensibles.

En France, l'ANSSI est chargée d'accompagner cette politique de cybersécurité. Des initiatives locales aident aussi à se mettre en conformité au regard des textes européens. C'est le cas du programme CYBIAH (Cybersécurité et intelligence Artificielle Hub) qui est porté par le Campus cyber et permet, soutenu par la région Ile-de-France et l'UE, de donner les moyens aux petites entreprises et collectivités locales de se protéger. Proposant également des conseils rétribués pour les entités hors d'Ile-de-France, les SDIS pourraient ainsi utilement s'en rapprocher, notamment pour sécuriser leur réponse opérationnelle face aux cybermenaces.

Dans un contexte géopolitique instable, les enjeux autour de la cybersécurité sont également économiques mais aussi répressifs afin de protéger les valeurs démocratiques européennes et l'Etat de droit.

II - Dans un contexte géopolitique instable, les menaces autour de la cybersécurité ne doivent pas occulter la nécessité de prendre en compte les enjeux économiques et répressifs afin de protéger les valeurs européennes de l'Etat de droit

A - La prise en compte indispensable de l'enjeu économique au sein de l'UE où la régulation numérique est prégnante

1 - L'enjeu économique de la cybersécurité

Les enjeux liés à la cybermenace sont significatifs en ce qu'ils peuvent toucher des institutions régaliennes mais aussi dans la mesure où l'activité économique est une cible. Ce sont donc les entreprises qu'il convient de protéger en l'espèce, même si la cybersécurité a un coût. Rien qu'en France, la cybersécurité représente 129 milliards de dollars, soit près de 5% du PIB. Le risque est donc que le coût de la réglementation devienne plus élevé que celui des cyberattaques.

Cette inquiétude des entreprises se pose dans un contexte où la compétitivité se trouve au cœur des enjeux européens, comme l'a souligné Mario Draghi dans le rapport qu'il a rendu à ce sujet en septembre 2024. C'est aussi ce que souligne la boussole de la compétitivité présentée récemment par Ursula Von der Leyen, la présidente de la Commission. Cela doit notamment être pris en compte dans le cadre des budgets pluriannuels (CFP) et dont l'actuel, de 2021 à 2027, prévoit 1,6 milliard d'euros pour la cybersécurité. Des fonds, non utilisés par le plan NextGenerationEU et ses 750 milliards d'euros, pourraient utilement être redirigés. Une partie des 150 milliards de subvention de « ReArmEU » également.

2 - Un enjeu économique à concilier avec une régulation numérique déjà prégnante

De façon plus globale, il est important de souligner que la cybersécurité doit s'inscrire au sein de la souveraineté numérique de l'UE. Celle-ci est déjà fournie, même si contrairement aux Etats-Unis (GAFAM) et à la Chine (BATX), elle ne comprend pas de champion européen. Une régulation existe déjà en effet et elle est unique dans le monde avec le règlement général de protection des données (RGPD), le Digital markets act (DMA), le Digital services act dit DSA (où ce qui est illégal hors ligne est illégal en ligne) et le récent AI act. Seul l'ePrivacy, prévu pour accompagner le RGPD dans l'échange des données, n'est à ce jour pas entré en vigueur.

B - La nécessité de développer le volet répressif afin de protéger les valeurs européennes de l'Etat de droit

1 - Le développement du volet répressif

En l'espèce, l'UE prévoit d'installer des « centres opérationnels de sécurité » (SOC) associés à l'IA et qui pourraient s'apparenter à des

« policiers » du monde numérique. Par ailleurs, un centre européen spécialisé dans la lutte contre la cybercriminalité a été créé au sein d'Europol. Il se concentre sur les crimes perpétrés en ligne, la pédocriminalité et la fraude financière.

De même, Eurojust peut avoir son rôle à jouer tout comme le parquet européen qui a récemment été créé. A ce jour, ses missions sont limitées à des aspects financiers de défense des intérêts de l'UE. Pour autant, son succès avec près de 2 000 dossiers traités fin 2023 et un préjudice estimé entre 15 et 20 milliards d'euros, doivent permettre d'envisager son expansion à d'autres domaines. La cybercriminalité constitue un domaine clef qui peut en faire partie.

2 - <u>L'Etat de droit, cible silencieuse des cyberattaques</u>

La cybersécurité constitue un enjeu politique fort. C'est en ce sens que Thierry Breton et le secrétaire à la sécurité des Etats-Unis ont fait une déclaration commune sur la cyberrésilience le 30 janvier 2024. Les américains étant particulièrement sensibles à cette question, eux qui disposent d'un commandement dédié au cyberespace et qui craignent un « Pearl Harbor numérique ». C'était il y a un an et depuis les préoccupations américaines ont changé.

En Europe, l'invasion russe a, en plus de la guerre à haute intensité en Ukraine, accéléré un mouvement à basse intensité qui consiste à tenter de déstabiliser les démocraties européennes, fondées sur les valeurs de l'Etat de droit. Le groupe de hackers APT28, lié aux services de renseignements russes, aurait d'ailleurs diffusé des documents sur le président français (« MacronLeaks »). Plus récemment, l'annulation de l'élection en Roumanie, sur fond de campagne expresse sur TikTok, ne fait guère de doute sur les tentatives de déstabilisations. C'est donc une menace silencieuse qui cible l'Etat de droit européen et avec lui ses valeurs, les droits et libertés démocratiques. La vigilance est d'autant plus grande que certains Etats de l'UE, comme la Hongrie, n'y verront rien à redire.

Soumise à de nombreux enjeux stratégiques, la cybersécurité nécessite une prise en compte totale de l'UE afin de protéger ses institutions, ses EM et toutes leurs composantes publiques et privées ainsi que les citoyens. Ce qui est en jeu, au-delà de la souveraineté numérique et de l'autonomie stratégique de l'UE, c'est la notion même de l'Etat de droit en Europe.

Ainsi, pour rester pleinement vigilant, on se rappellera la formule d'Hubert Védrine, « les européens sont des sortes de bisounours qui ne savent pas qu'ils vivent dans Jurassic Park ».