Compte-rendu du déjeuner avec Despina Spanou, Directrice à la DG Connect en charge de la société numérique, de la confiance et de la cybersécurité 27 avril 2018

Le 27 avril, les membres du Cercle des Réseaux Européens ont rencontré Despina Spanou, Directrice en charge de la société numérique, de la confiance et de la cybersécurité au sein de la DG Connect. Le déjeuner a été l'occasion d'échanger sur les enjeux européens en matière de cybersécurité, les attentes du secteur privé mais également de dossiers numériques connexes comme la directive PSI révisée présentée le 26 avril.

Jean-Claude Juncker, Président de la Commission européenne, a placé les questions de cybersécurité en tant que priorité politique. Il a été soutenu dans sa démarche par les chefs d'Etat et de gouvernement lors du Sommet Numérique demandant une action forte de la Commission européenne. Dans un contexte où les cyber-attaques continuent de se multiplier (on dénombre 4000 attaques en 2016), dont certaines de grande amplitude, la directive NIS est très importante car elle constitue la 1ère loi sur la cybersécurité en Europe et vise à harmoniser la résilience face à ces pratiques. Selon les estimations, 50 % des infractions sont de nature informatique. Les propositions présentées par la Commission en septembre dernier visent à compléter cette directive.

La directive NIS

La Directive NIS, instaurant des règles communes au sein de l'Union permettant aux entreprises de mieux résister aux menaces en ligne, est entrée en vigueur le 19 juillet 2016 et doit être transposée par les Etats membres au plus tard le 9 mai prochain. La France semble être déjà alignée avec les obligations liées à la transposition. L'unité de Despina Spanou a un rendez-vous avec des représentants français la semaine du 2 mai pour s'assurer que les mesures sont adéquates. Globalement, la France a toujours eu un rôle d'impulsion positive sur les sujets de cybersécurité.

A l'heure actuelle, quelques Etats membres discutent et échangent des informations en matière de cybersécurité, mais il n'existe pas encore de vraie collaboration. La directive NIS et le renforcement de l'ENISA ont pour objectif d'instaurer une réelle coopération entre les Etats membres. **Il est important également de prendre compte le fait que la volonté des Etats membres a changé depuis l'adoption de la directive NIS : ils étaient auparavant en faveur d'un cadre moins strict alors qu'ils favorisent aujourd'hui le recours à la régulation.**

Les Etats membres doivent aider les opérateurs à se protéger de manière adéquate contre les cyber-menaces. La directive leur laisse **jusqu'au 9 novembre prochain pour identifier et lister les opérateurs de services essentiels** (énergie, transports, banques, infrastructures de marchés financiers, santé, fourniture et distribution d'eau potable, et infrastructures numériques) en se fondant sur les critères qu'elle définit. Ces opérateurs devront ensuite mettre en œuvre des mesures techniques et organisationnelles pour gérer les risques menaçant la sécurité des réseaux et des systèmes d'information.

Une équipe sera créée pour suivre l'application de la directive, non seulement sur le délai de transposition mais sur la qualité de cette transposition car les menaces sont de nature pan-européenne et nos systèmes sont interconnectés.

Révision du mandat de l'ENISA

L'agence était beaucoup critiquée car elle disposait d'un mandat d'action limité et n'était pas partie prenante des discussions lorsqu'une crise éclatait. Ce qui a conduit à la révision de l'ENISA.

Elle a cependant évolué dans le temps. La Commission a évalué les forces et les faiblesses de l'agence avant de présenter les propositions de révision publiées en septembre dernier. Il est proposé que l'ENISA ait désormais, après une meilleure

définition des tâches qui lui incombent et les avoir modernisées, **un rôle d'appui lorsque les Etats membres et les entreprises en auront besoin. Il y a actuellement une réflexion autour de la création d'une liste d'experts à solliciter en cas de besoin.**

L'un des premiers chantiers de l'ENISA sera **l'éducation et la formation sur la cybersécurité afin d'accroitre l'expertise européenne dans ce domaine.**

Concernant le cadre de certification, même s'il est volontaire, **l'objectif est de parvenir à une reconnaissance mutuelle des certificats avec l'établissement d'un guichet unique qui serait l'ENISA. Il ne serait donc pas question d'exclure les systèmes actuels, qu'ils soient nationaux ou transfrontaliers**. Le cadre européen dépendra des autorités nationales qui composeront le groupe d'expert qui travaillera à ce sujet, mais également des parties prenantes qui seront invitées à apporter leur expertise. Dans cet esprit, un système national de certification pourrait très bien devenir européen en devenant un point de référence du fait de son efficacité. L'objectif est d'avoir un système européen flexible afin de pouvoir couvrir des problèmes futurs que l'on n'imagine pas encore aujourd'hui.

Il y a encore beaucoup de travail à faire pour cette uniformisation car il y a une forte disparité entre les Etats membres en ce qui concerne leur capacité / compréhension, mais également leurs ressources.

Les discussions au Conseil et au Parlement européen avancent bien et il est probable qu'une adoption soit finalisée avant la fin de l'année.

Création d'un réseau de centres de compétence

La Commission envisage la création d'un centre de compétence en matière de cybersécurité. Cette démarche a provoqué beaucoup de discussions. Il n'y a actuellement pas de coordination en matière de recherche et d'innovation d'où cette idée de créer un centre de compétence puis un réseau. Il résulte de cette situation qu'il existe un manque d'expertise en matière de cybersécurité. L'objectif final de ce réseau est de maîtriser la chaine de création de valeur.

Il existe actuellement plus de 700 centres d'excellence de cybersécurité en Europe mais qui ne sont pas connectés entre eux. Il **est important de mettre en place une synergie entre les secteurs industriels, de la recherche, des entreprises privées…**

Un board composé de parties prenantes sera formé pour apporter un avis sur les projets spécifiques proposés dans le cadre du déploiement de ce réseau. Il y aura un appel à manifestation d'intérêt. Ce centre pourra ensuite gérer des fonds européens sur la base de priorités politiques définies dans le cadre du futur programme cadre.

Financement des propositions

Des propositions visant à financer le réseau de compétence susmentionné seront **présentées en juin, en même temps que d'autres proposition législatives budgétaires qui seront publiées dans le cadre du CFP post 2020.** Il existe une réelle synergie avec le domaine de la défense et il est question de coupler les moyens sur les sujets rassemblant les deux domaines. **Il était par ailleurs initialement question d'insérer dans le CFP un programme numérique européen au sein duquel la cybersécurité serait un gros pilier, chose qui restera à confirmer en juin.**

L'ENISA pourra également proposer des projets à subventionner une fois son mandat révisé.

Révision de la directive PSI

Les modifications proposées par la proposition de révision de la directive PSI présentée le 25 avril dernier par la Commission européenne sont progressives. **Il est question ici d'accéder à plus d'informations du secteur public à un coût modéré, facilitant ainsi la réutilisation de données ayant un intérêt public.**

Le champ d'application a été étendu aux entreprises publiques mais les entreprises privées ont été exclues, la Commission a ainsi tenu compte des retours exprimés dans la consultation. ***Les participants au déjeuner ont fait part de leur crainte que l'évolution des discussions sur cette révision devienne désavantageuse*** : le Parlement européen pourrait bien

demander à ce que les entreprises privées soient aussi inclues dans le champ d'application de la directive car elles ont les mêmes enjeux afin de rétablir une certaine égalité. Ils se sont également interrogés sur le réel bénéfice de cette révision qui pourrait apporter de la matière première numérique à la Chine et aux Etats-Unis sans développer substantiellement les entités européennes. Il a été fait remarquer qu'il manquait, dans la proposition actuelle, des gardes fous empêchant toute distorsion de concurrence avec des acteurs non-Européens.

Confidentialité et e-privacy

La proposition a été présentée il y a 14 mois. Le processus est très long alors qu'il s'agit de la modernisation d'une directive existante qui sera fortement impactée par le GDPR. **Cette révision permettra par ailleurs d'inclure des opérateurs jusqu'ici en dehors du champ d'application de la directive, à l'image de skype ou de Whatsapp.**

***