NOTE	Compte-rendu de la journée Cybersécurité : Centre de Compétences Européen et projets pilotes
Date	09/10/2019
Auteur(es)	Ivan Meseguer (IMT), Eric Foucher (CPU), Odile Arbeit de Chalendar (IFSTTAR), Geoffroy Meillon (CLORA)
Référence	2019/09

Cybersécurité Européenne : quels enjeux ?

Henri Verdier, Ambassadeur de France pour le numérique Despina Spanou, Directrice Direction H « Digital Society, trust and Cybersecurity, DG Connect, Christian Mrugalla, Chef d'unité « International Cybersecurity and cyber security research, Ministère Féderal de l'intérieur, de la construction et de l'habitat, Allemagne

Henri Verdier : en France, une diplomatie du numérique est nécessaire. Celle-ci doit être géographiquement étendue. Différentes équipes travaillent sur ce sujet au sein du MEAE (Ministère de l'Europe et des affaires étrangères, cf. économie diplomatique, enjeux de Cybersécurité, révolution numérique avec l'accès au numérique…).
L'objectif est de réunifier tous ces sujets et négocier au sein du gouvernement et avec les partenaires. Henri Verdier est en charge d'effectuer un exercice de synthèse de ce sujet majeur. Les risques se sont accrus dans nos sociétés. Les IT ont rapidement changé et revêtent des enjeux économiques, politiques et sociétaux majeurs.

Le constat actuel est le suivant :

- Concentration de bases de données (cible plus facile à attaquer) ;
- Beaucoup de dirigeants d'entreprises ne connaissent pas les infrastructures de recherche et se contentent de copier les systèmes existants ;
- Augmentation importante et croissante d'attaques de Cybersécurité ;
- Différences entre les États membres : certains pensent qu'ils sont assez forts pour faire face, d'autres ne disposent pas des mêmes moyens.

Il y aura des attaques, et il y aura des conséquences qui pourront s'avérer être graves. Mais il ne s'agit pas d'une situation de guerre froide : on ne développe pas des armes de Cybersécurité pour riposter, d'autant que l'impact de la « riposte » est difficilement identifiable. L'Europe a besoin d'une stratégie globale (y compris en répondant aux besoins de recherche, d'innovation.). Elle doit être forte et protéger. La diplomatie doit permettre la mise en place de lois internationales dans le cyberspace alors que l'on assiste à des initiatives russes et américaines qui complexifient la donne.

En France, le ministère de la défense a publié un guide pour se protéger[1]. La transparence permettra elle aussi de savoir comment se défendre. Mais il faut aussi **responsabiliser** les acteurs privés.

350 compagnies, 100 ONG, se sont réunies pour échanger sur la responsabilité du secteur privé et celle des citoyens. La responsabilité est globale et concerne l'ensemble des acteurs : cela commence au niveau des citoyens.
Pour avancer, il y a également un besoin de standards, d'échanges de bonnes pratiques et d'interagir avec la chaine d'approvisionnement.
Une discussion est amorcée sur ces sujets au sein de l'OCDE[2] depuis décembre dernier.

[1] https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/
https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation

La Cybersécurité n'est plus seulement une question de sécurité nationale ! L'Union européenne doit participer à élever le niveau de Cybersécurité, en renforçant les capacités et les moyens, sur la base de la réglementation, mais aussi de l'industrie à l'échelle du marché unique. Soutenir la recherche et l'industrie Européenne

L'approche française insiste sur la nécessité pour l'Union Européenne d'adopter une stratégie numérique industrielle ambitieuse, soutenue par les acteurs publics et privés, afin de renforcer la sécurité et la confiance dans le marché unique numérique, en phase avec les valeurs européennes.[3]

Despina Spanou

Mme Despina Spanou remercie le CLORA, plate-forme des acteurs de la recherche française.

La Commission n'est pas toujours informée au plus près des activités des acteurs.

Où en est l'Europe pour la stratégie ? La Commission Européenne a commencé à travailler prudemment sur ce sujet depuis 2015 car la sécurité des ICT est longtemps restée avant tout une compétence des états membres. Le marché unique a changé la donne et renforcé la pertinence d'une intervention à l'échelle européenne. Rappel des principaux éléments historiques relatifs à la Cybersécurité par la DG Connect :

- Existence d'une stratégie depuis 2013 ;
- Plan Juncker sur le sujet depuis 2015 relatif à la Hard Cyber security ;
- Le RGPD ;
- Souhait d'un cadre de certification pour les objets connectés qui soit élevé.

La Commission Européenne a lancé en 2015 l'initiative « numérisation du marché unique [4]». Rapidement les besoins de sécurité ont été identifiés. Le GDPR est important, les initiatives européennes resteront sans portée réelle (ndlr : les deux étant liées, par exemple dans le cas de la vie privée, c'est une composante essentielle de la sécurité des personnes, car c'est à travers les *credentials*, ou les identités, que l'on peut générer des failles de sécurité).

Ainsi la collecte des données personnelles représente un enjeu important. Nous avons appris par exemple qu'un opérateur télécom[5] était attaqué depuis 2017 alors qu'il collectait des métadonnées – c'est à dire ici la géolocalisation… Les métadonnées sont très sensibles parce qu'elles sont stratégiques. Les Fake news, quant à elles, montrent également la nécessité d'un plus haut niveau de protection.

---

[2] https://cybercercle.com/comptes-rendus/la-nouvelle-recommandation-de-locde/
L'OCDE s'est penchée sur cette question depuis plusieurs années. La Cybersécurité ne doit pas freiner le développement économique et social mais au contraire, elle doit le favoriser. L'OCDE produit des Recommandations et des analyses pour les États sur cette question.

[3] https://infossl.com/blog/2018/12/

4 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-impact-digital-transformation-eu-labour-markets

[5] https://www.mobileworldlive.com/featured-content/home-banner/global-operators-hit-by-security-attack/

Cela induit un réel besoin de stratégie et de législations ainsi que moyens concertés de réaction en cas d'attaque.
Il faut assurer la sécurité et protéger nos valeurs via deux façons :

1. Mieux travailler ensemble (l'UE dispose désormais de groupes de travail de haut niveau, et a identifié des besoins, des politiques et des législations au niveau européen. Depuis 2017, la CE identifie qui fait quoi sur la Cybersécurité, pour améliorer la coordination. Ces enjeux sont fondamentaux pour préserver la souveraineté des États membres. Avant cet événement CLORA, les États-Unis ont procédé à une attaque de Cybersécurité contre un État, l'Iran. Des synergies sont nécessaires avec les militaires. Des exercices de Cybersécurité ont lieu (dans le cadre de l'OTAN) et l'année prochaine, il y en aura de nouveaux.

2. Une législation est nécessaire. Le Cybersecurity Act[6] a permis la création du centre de Cybersécurité. L'agence ENISA (cf. cadre explicatif ci-dessous renforce la protection des États membres et des citoyens. Cet acte unique résulte d'un travail législatif d'un an grâce notamment au soutien des États membres. Les cadres de certification européens sont eux orientés vers le marché en répondant aux besoins d'infrastructure de recherche avant de parvenir au marché. C'est un domaine dans lequel l'UE est en avance. Les Japonais travaillent dans ce sens également.

Parallèlement à ces démarches, il y a un besoin de recherche, et un besoin de développement, y compris de produits, européens.

Le Centre européen de compétences industrielles, technologiques et de recherche en matière de Cybersécurité et le réseau de centres nationaux de coordination

La proposition pour créer ce centre de compétence[7] en matière de Cybersécurité a été émise en en septembre 2018. Il s'agit de mettre en réseau les centres de compétence nationaux. Et les partenaires existants (écosystèmes d'organismes de recherche…). La communauté sera coordonnée par ce centre européen qui s'appuiera sur elle pour identifier les domaines dans lesquels investir.

Un recensement des centres d'excellence en matière de Cybersécurité a été effectué. 650 centres ont été identifiés en Europe, ce qui représente une réelle valeur ajoutée.

Cependant, il y a un manque de capacités et un problème d'investissements qui restent relativement limités dans le domaine de la Cybersécurité. Il est nécessaire d'avoir une approche plus stratégique. Cela requiert une méthode différente en réunissant des experts pour identifier des méthodes pour investir. La CE a proposé de multiplier par cinq les investissements et par deux le budget de la recherche dans ce domaine. La CE et les États membres doivent décider ensemble des priorités à financer.

Ce centre européen travaillera sur les synergies entre les différents programmes. Il sera doté d'une *governing board* qui réunira les États membres et la CE et un *advisory board* qui réunira la communauté (experts du secteur privé et des organismes de recherche). Il s'agit d'un système inclusif.

La proposition doit être acceptée d'ici la fin de l'année.

La recherche

Il faut aussi promouvoir la recherche. Le domaine numérique comprend des spécificités, notamment par rapport aux compétences qu'il nous faut développer. Le projet de pilotes européens[8] a clairement enthousiasmé la communauté scientifique.

6 https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en
7 https://www.europarl.europa.eu/doceo/document/TA-8-2019-0419_FR.html
8 https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

L'acte législatif sur la Cybersécurité renforce le mandat de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information — ENISA pour la Cybersécurité, afin de mieux soutenir les États membres dans la lutte contre les menaces et les attaques en matière de Cybersécurité. L'acte établit également un cadre européen de certification de Cybersécurité, qui renforce la Cybersécurité des services en ligne et des dispositifs grand public.
Proposé en 2017, l'acte législatif sur la Cybersécurité prévoit:

- de doter l'ENISA, l'Agence de Cybersécurité de l'UE, d'un mandat permanent pour remplacer son mandat limité venant à expiration en 2020, ainsi que de ressources supplémentaires, et
- d'accorder à l'ENISA un rôle plus important en matière de coopération et de coordination au niveau de l'Union dans le nouveau cadre de certification de Cybersécurité afin d'aider les États membres à réagir efficacement aux cyberattaques.

En outre, l'ENISA contribuera à accroître les capacités en matière de Cybersécurité au niveau de l'UE. Enfin, l'ENISA constituera un centre d'expertise indépendant pour promouvoir un niveau élevé de sensibilisation des particuliers et des entreprises, tout en aidant les institutions de l'UE et les États membres à élaborer et mettre en œuvre des politiques.
L'acte législatif sur la Cybersécurité crée également un **cadre de certificats européens de Cybersécurité** pour les produits, les procédés et les services, qui seront valables dans toute l'UE. C'est la première législation relative au marché intérieur qui relève le défi de renforcer la sécurité des produits connectés, des appareils de l'internet des objets et des infrastructures critiques au moyen de ces certificats. Ce cadre vise à intégrer des éléments de sécurité dès les premières phases de conception et de développement techniques. Il permet également aux utilisateurs de déterminer le niveau d'assurance de la sécurité et garantit que les éléments de sécurité sont vérifiés de manière indépendante.

Les nouvelles règles permettront aux utilisateurs de choisir des produits, tels que les dispositifs de l'internet des objets, qui répondent aux exigences de Cybersécurité. Le cadre de certification constituera un guichet unique pour la certification en matière de Cybersécurité. En outre, les entreprises sont encouragées à investir dans la Cybersécurité de leurs produits et d'en faire un avantage compétitif.

Les réponses à apporter doivent se faire sans militariser notre paysage de la Cybersécurité. L'approche militaire stricte n'est pas adaptée. Il s'agit en effet également de protéger les particuliers, contre le piratage de leur compte bancaire par exemple. La recherche représente une partie de la solution, et la souveraineté numérique passe par les connaissances, nos connaissances, et leur partage.

L'intelligence artificielle a un effet majeur sur la Cybersécurité (réaction à la crise) et peut contribuer à identifier les menaces. Cependant elle peut être piratée elle aussi tout aussi facilement.

Cela nécessite également d'aligner la recherche et le développement. Beaucoup d'argent a été dépensé dans la recherche, mais certains produits ont été exploités dans des pays tiers et d'excellents chercheurs sont partis. C'est pourquoi il faut développer des solutions utiles à l'UE et les synergies doivent devenir significatives pour renforcer le plan stratégique.

Échanges avec la salle
Combien coûtera la Cybersécurité, comment convaincre les citoyens ?

Henri Verdier regrette qu'il y a 20 ans les citoyens semblaient plus informés des enjeux de Cybersécurité qu'actuellement.

En 1996 un ouvrage[9] est paru, recensant déjà à l'époque les menaces du cyberespace auxquels nous faisons face actuellement : *Guerres dans le Cyberespace*. *Services secrets et Internet*. Entre temps des solutions pour faciliter la vie des usagers sont parvenues sur le marché : smart phone, Facebook, etc. Il faut donc travailler sur la prise de conscience des citoyens. Ils reçoivent des informations très ciblées pour attirer leur attention et fournissent des données stratégiques. Ce n'est pas uniquement un enjeu d'éducation mais aussi de citoyenneté pour sauvegarder notre liberté.

[9] https://www.monde-diplomatique.fr/1996/01/HEBERT/5185

Mme **Despina Spanou** rappelle que des attaques massives sont possibles. Les données sont de plus en plus connectées (une maison connectée peut faire l'objet d'une attaque). Il faut sans doute poursuivre les campagnes de sensibilisation. Le co-législateur a demandé d'inclure plus d'informations sur les produits, ce qui permet d'éclairer les consommateurs également. L'exemple de la sécurité alimentaire peut représenter un exemple à suivre. Par exemple, suite à la crise de la vache folle, des tests, une traçabilité, ont étés mises en place. C'est la crise qui a déclenché une réponse qui peut aujourd'hui être considérée comme un succès. La traçabilité est un modèle à reprendre et dans lequel l'Europe a du retard.

Pour **Christian Mrugalla**, il faut convaincre le public, qui met du temps à réagir. Le fatalisme, les réponses « je n'ai rien à cacher » illustrent le travail à faire. Les autorités publiques ont également mis du temps à réagir. D'un autre côté, si on se protège trop, on n'innove pas. C'est pourquoi le renforcement de la sécurité des produits lors de leur mise sur le marché est une priorité.

Coordination des centres

Mme Despina Spanou

Le centre européen qui coordonnera les centres de coordination nationaux, peut avoir pour mission l'organisation de recherche ou peut mettre en place des programmes d'éducation notamment dans le *digital programme*. Certains acteurs européens travaillent sur le même projet, d'autres n'ont pas assez de moyens. La Commission Européenne met en place une nouvelle gouvernance et continuera à financer des projets (exemple dans la cryptographie). Le fossé des compétences reste important alors qu'elles ne sont pas l'objectif à ce stade. C'est le *governing board* du centre européen qui décidera des orientations. Les organismes de recherche seront consultés (advisory board). Une souveraineté numérique européenne doit émerger. On ne peut pas copier le système américain ou chinois. Dès lors comment être stratégiquement pertinent, comment dépenser l'argent sur des programmes permettant la souveraineté. On doit trouver une voie innovante et assurer un retour aux centres.

Pour **Christian Mrugalla**, il faut une valeur ajoutée et changer les méthodes de travail (les financements ne doivent pas être utilisés dans les pays tiers. Les solutions seront communes et aucun État ne peut agir de son côté seul.

Henri Verdier

Nous avons peut-être perdu la bataille de l'Internet, mais pas la guerre. Une nouvelle chance se présente et il faut renforcer les entreprises européennes. L'Europe doit aussi défendre ses valeurs ; cela peut être très puissant. Nous pouvons déjà observer que de nombreux pays ont suivi ou s'inspirent de l'Europe dans la mise en place du GDPR. De son côté la Chine va également devoir faire face à des défis, ne l'oublions pas.

Mme **Despina Spanou**

L'Europe possède un fort potentiel de puissance sur ces questions mais malheureusement, ses actions ne sont pas coordonnées. L'approche choisit doit contenir des objectifs durables et stratégiques.

Fonctionnement du Centre Européen de Compétences en Cybersécurité :

- Instauration d'un Conseil de Gouvernance pour plus de coordination. Il sera composé des États membres et de la Commission.
- Un Conseil Consultatif devrait être créé et composé de chercheurs, d'industriels et d'autres membres de l'écosystème.
- Sur les questions de mise en œuvre : la DG CONNECT souhaite trouver un accord d'ici la fin de l'année.

La Souveraineté européenne et la Souveraineté européenne en matière de numérique :

Pour **Mr Christian Mrugalla, représentant allemand du Ministère de l'intérieur**, il est essentiel de se questionner sur la façon de retrouver d'une part une souveraineté en Europe et d'autre part de regagner une souveraineté sur les questions numériques. Il convient également de s'interroger sur l'application de l'intelligence artificielle et les questions de sécurité qui en découlent. Pour ce faire, il faudrait renforcer la sécurité en s'assurant d'un développement et d'un financement européen. Ralentir le processus d'entrée en fonctions de ces applications est un des moyens à disposition.

Pour Henri Verdier, la prochaine étape dont nous aurions besoin est un véritable marché européen du risque comme le NASDAQ aux États-Unis. L'Europe souhaite défendre une approche plus humaine de la Cybersécurité avec le RGPD qui a d'ailleurs été repris en Inde, au Japon et en Californie.

Session Q&R avec le public

Les maisons connectées : il n'est pas nécessaire d'avoir une maison totalement connectée et dans le cas contraire, il faut être conscient des responsabilités et des risques qui sont encourus.

L'accès à l'information : une étude a montré que si l'on rendait une information trop accessible aux individus, ceux-ci ne font pas l'effort d'y accéder.

Le Réseau des Centres Nationaux : il est important de coordonner le travail des organisations de chercheurs. L'UE n'est pas les États-Unis, et nous avons besoin d'une stratégie mais comment combiner les règles du programme avec la Cybersécurité, domaine dans lequel, nous manquons à l'heure actuelle de compétences ? Pour y répondre, l'UE a besoin de synergies avec des réponses communes et une volonté de travailler ensemble. En parallèle, elle a aussi besoin de projets concrets de financement, à titre d'exemple, la cryptographie**.**

Un des piliers de **développement des compétences** dans le cadre d'Horizon Europe sera **le programme Digital Europe.**

Concernant la **venue d'étudiants étrangers**, des questions se posent. En Australie, certains étudiants étrangers (Chinois) viennent y étudier pour retourner dans leur pays d'origine et mettre à profit les compétences qu'ils ont acquises.

Comment pouvons-nous **rapprocher la Communauté ?** À travers une approche flexible, gratuite et de soutien qui lie la recherche et le développement **par des objectifs européens présents au sein des stratégies nationales**.

La question de l'ECSO et de son avenir :
L'avenir de ce Partenariat Public-Privé (cPPP) a été soulevé durant la réunion. Un des enjeux est de savoir comment celui-ci s'articulera dans le paysage de la Cybersécurité européenne. Basé sur un programme de recherche, il aura pour objectifs de soutenir la Recherche et l'Innovation des premiers projets. Les projets actuellement européens ne vont pas se transformer à l'avenir en projet nationaux via Horizon Europe. Aujourd'hui l'ECSO a un résultat à vendre, c'est par le biais des fonds européens qu'il va ainsi soutenir une meilleure organisation du niveau national. L'ESCO continuera à exister sous le programme Horizon Europe, en tant qu'association représentante des acteurs de la recherche et de l'innovation.

L'ENISA : La présence de mécanismes est essentielle notamment après la crise de la 5G, toujours en cours, qui devrait interroger l'Union européenne. La délivrance de certificats est ainsi le seul moyen de pouvoir avoir de véritables discussions avec la Chine. La 5G devrait d'ailleurs être l'une des premières crises du Cyberespace. Cependant, il ne faut pas surestimer l'approche des certificats.

Les centres de compétences

En sachant que nous avons besoin d'une multiplicité d'approches, il est attendu des centres de compétences, qu'ils montrent le chemin.