NOTE	Compte-rendu de la journée thématique du 20 septembre 2018 Pôle 2 Société Sûre et inclusive
Date	18/10/2018
Auteur(s)	Eric Foucher (CPU), Jérôme Huon de Kermadec (ONERA), Ivan Meseguer (IMT), Monika Repcikova (CPU), Sophie Sergent (Ifremer), Gaël Brosseaud (CLORA)
Référence	2018/12

Présentation des aspects sécurité du pôle 2 « Société sûre et inclusive »
Mme Anabela Gago – Chef d'unité, unité innovation et industrie pour la sécurité, DG Home

La recherche dans le domaine de la sécurité s'inscrit dans le cadre de la réponse globale de l'UE aux différents types de menaces pesant sur nos sociétés, qu'il s'agisse de la menace terroriste dont le niveau est toujours élevé, ou de catastrophes naturelles, souvent liées à des phénomènes climatiques extrêmes, et qui continuent de causer trop de victimes à travers le monde.

L'Eurobaromètre de l'automne 2017 a montré que la menace terroriste est l'un des principaux sujets de préoccupation des citoyens européens (38 %), mais également la criminalité (10 %).
L'ampleur, la complexité et le caractère transfrontalier de ces menaces et de ces phénomènes exigent une réponse concertée à plusieurs niveaux.
Comme il est clairement défini dans le programme européen en matière de sécurité de 2015, l'Union soutient des actions menées en matière de sécurité via les formations, le financement et la promotion de la recherche et de l'innovation dans ce domaine.
Nous pouvons sans aucun doute affirmer qu'au cours des dernières années, l'UE a contribué à construire une communauté à l'échelle de l'UE pour la R&I en matière de sécurité.

Mise en contexte :

La recherche financée par l'UE en général représente entre 8 et 10 % du financement public total de la recherche. La situation est très différente **dans le domaine de la recherche en matière de sécurité civile, où la recherche financée par l'UE représente 50 % du financement public global dans l'UE.** La France a été, dans le cadre des programmes-cadres FP7 et H2020 un grand bénéficiaire en matière de recherche en sécurité car elle est bien représentée dans tous les domaines d'activité de cette recherche. La France fait aussi partie d'une minorité de 8 États membres disposant de son propre programme national de recherche sur la sécurité.

Toutefois, en dépit de la force du secteur européen de la sécurité, de la pertinence de l'aide financière de l'UE et de la collaboration continue avec les différents États membres, le secteur se heurte à des difficultés pour s'assurer que les résultats de la recherche sont couronnés de succès. **Un certain nombre de défis et d'obstacles contribuent à creuser l'écart entre la recherche et le marché, ce qui limite la capacité de l'UE à lutter efficacement contre les menaces en matière de sécurité. Il s'agit, entre autres : d'un marché très fragmenté et essentiellement institutionnel ; des contraintes liées aux régimes de financement existants ; du décalage entre l'offre et la demande.**

Afin de relever ces défis et d'autres, la Commission s'oriente vers une approche qui combine soutien à la recherche et soutien au développement de capacités, en grande partie d'un processus déjà consolidé dans le domaine de la défense. Le premier paradigme relatif à cette approche se base sur le fait que dans le domaine de la sécurité, compte tenu des particularités du paysage dans lequel les pouvoirs publics sont les principaux acheteurs, la recherche ne saurait être un processus autonome. La recherche est un catalyseur stratégique d'un processus plus large mené par les décideurs politiques et dans lequel les utilisateurs finaux — et l'industrie — jouent un rôle décisif.

La recherche devrait être effectuée afin de combler un déficit de capacités qui soit reconnu et validé par une autorité compétente au niveau national ou, lorsqu'il s'agit de la recherche financée par l'UE, une autorité

compétente au niveau européen. Ce déficit peut dans certains cas avoir trait à des technologies essentielles à l'autonomie stratégique de l'UE.
Cette façon de procéder est la seule qui peut assurer que la recherche servira une finalité concrète et que les résultats, lorsqu'ils sont positifs, conduiront ultérieurement à une solution que les pouvoirs publics seront alors prêts à acquérir.

L'implication accrue des utilisateurs finaux dans l'activité de recherche et d'innovation en sécurité est fondamentale pour permettre une politique pertinente de développement de capacités et d'acquisition d'équipements et de technologie. En effet, les utilisateurs finaux (par exemple, police, gendarmerie, douane etc…), sont les mieux conscients de leurs besoins et doivent pouvoir être impliqués dans les projets. H2020 a connu une avancée notable en ce qui concerne la participation des utilisateurs finaux au cycle de R&I, ce qui a permis de changer la donne en ce qui concerne la solidité et la pertinence des résultats de la recherche face aux besoins opérationnels des autorités de maintien de l'ordre ou des premiers intervenants. La manière dont la proposition récemment adoptée concernant le nouveau règlement de l'Agence européenne de garde-frontières et de garde-côtes va dans ce sens. L'Art.66 du règlement intègre explicitement les efforts de recherche dans un processus global de développement des capacités.

Madame Gago signale l'arrivée d'une nouvelle directrice capacité chez FRONTEX[1] : Madame Aija Kalnaja. Capacity Building Division.

Le but est également de renforcer la compétitivité du secteur européen de la sécurité.
Sans la participation du secteur privé, l'engagement et l'investissement de la base industrielle et technologique de l'UE, les solutions innovantes ne seront jamais opérationnelles.
En outre, un marché européen unique et fort de la sécurité est fondamental pour renforcer la compétitivité de la base industrielle et le niveau de confiance dans la sécurité de l'approvisionnement en technologies stratégiques.
Madame Gago souligne que le Commissaire Julian King (commissaire à l'Union de la sécurité) était à Paris pendant les assises du COFIS lundi 24 septembre.
Dans ce contexte, le secteur privé et le secteur public doivent travailler main dans la main afin de développer une vision de l'écosystème de sécurité de demain. La CE s'efforce actuellement de mettre en place tous les canaux possibles pour permettre un tel dialogue permanent et structuré.

L'amélioration de la communication et de la diffusion des résultats de la recherche, reste un défi à relever :
Trop souvent, les résultats de la recherche ne sont pas communiqués et/ou diffusés auprès des communautés concernées, celles qui pourraient soit les mettre sur le marché, soit les utiliser sur le terrain.
La Commission redoublera d'efforts pour améliorer la diffusion des résultats. Notons la mise en place d'une communauté d'utilisateurs finaux (CoU)[2], qui offre une plateforme permettant le partage d'informations entre les États membres et qui regroupe les dernières évolutions en matière de politique et de recherche d'une manière qui soit facile d'accès. Notons également l'édition 2018 de l'événement de recherche sur la sécurité organisé par la Commission européenne et le ministère autrichien des transports, de l'innovation et de la technologie qui se tiendra au SQUARE à Bruxelles, les 5 et 6 décembre 2018. **« *Faire de l'Europe un endroit plus sûr : démontrer l'impact de la recherche sur la sécurité financée par l'UE* »,** SRE 2018 vise à valoriser les résultats des activités de recherche et d'innovation liées à la sécurité et à démontrer leur contribution positive au travail quotidien des milliers de praticiens de la sécurité http://risknat.org/security-research-event-sre-2018-making-europe-a-safer-place-bruxelles/

Horizon Europe :

Rappelons que le pôle 2 se trouve dans le pilier 2 «Défis mondiaux et compétitivité industrielle».
La pertinence de la recherche est confirmée dans le nouveau programme de recherche et d'innovation «Horizon Europe», qui sera le plus important programme de financement de la recherche et de l'innovation doté d'un budget de plus de 97 milliards d'euros (H2020: 77 milliards d'euros).

[1] Agence européenne de garde-frontières et de garde-côtes (FRONTEX)
[2] "Community of Users on Safe, Secure and Resilient Societies"

Par ailleurs, le prochain cadre financier pluriannuel (CFP/MFF) prévoit un renforcement considérable des activités liées à la sécurité (par exemple, en matière de gestion des frontières).
La proposition du CFP reflète la vision du Président Juncker de créer une *Europe qui protège*, une *Europe qui* donne les moyens *d'agir*, une *Europe qui défend*.

Sous Horizon Europe, **une approche plus globale et systématique est adoptée. La Commission espère que cela aura le plus d'impact possible et créera davantage de flexibilité et de synergies.**

Outre le volet dédié à une société inclusive, les aspects sécurité du pôle 2 répondent aux défis posés par les menaces qui pèsent actuellement sur la sécurité, dans toute leur diversité.
Toutefois, les préoccupations relatives à la recherche en matière de sécurité civile ne se limitent pas à ce qui se trouve dans le pôle 2, mais peuvent être considérées comme un point d'intersection avec d'autres thèmes, comme celui par exemple de l'intelligence artificielle.
Horizon Europe sera beaucoup plus axé sur l'impact que le programme «Horizon 2020» et l'ensemble du pilier 2 - «Défis mondiaux et compétitivité industrielle» - aura pour objectif de répondre à des besoins précis définis par les décideurs politiques et les utilisateurs finaux.
Il s'agit d'une sorte d'«officialisation» et d'une promotion de la façon dont la recherche en matière de sécurité a été pilotée et conduite dans le cadre d'Horizon 2020, en s'appuyant notamment sur la participation des utilisateurs finaux à des projets de recherche.
Horizon Europe encouragera les activités à mener au-delà des projets et assurera une meilleure diffusion et une meilleure exploitation des résultats au moyen de mécanismes spécifiques.
Horizon Europe prévoira également une souplesse accrue notamment pour faire face à l'évolution du paysage de la sécurité.
Une plus grande attention sera accordée à la création de synergies entre les différents programmes de l'UE, tels que le Fonds pour la gestion intégrée des frontières, le Fonds pour la sécurité intérieure et le programme «Digital Europe» (en ce qui concerne la cyber sécurité).
Des synergies seront également recherchées avec le financement de la recherche en matière de défense, évitant les doublons.

La partie «recherche dans le domaine de la sécurité» du Pôle 2 maintient une forte continuité avec l'architecture actuelle du programme «Sociétés sûres » d'Horizon 2020, comprenant deux dimensions, la dimension numérique (cyber sécurité) et la dimension « physique ».

Il importe également de mentionner que la proposition «Horizon Europe» comporte une disposition relative à la sécurité (art.16 de la proposition) qui renforce notamment l'importance de la protection des informations classifiées ; C'est la première fois qu'une disposition autonome sur la sécurité figure dans la proposition de programme cadre.

Les domaines d'intervention (1) les sociétés résilientes aux catastrophes; (2) protection et sécurité; et (3) cyber sécurité.

(1) **Sociétés résilientes :** sont considérées aussi bien les catastrophes naturelles que celles causées par l'homme. Il s'agit de la recherche destinée à soutenir les efforts de prévention, détection, préparation et réponse. La recherche abordera les phénomènes climatiques extrêmes (« mega-feux », les inondations, les phénomènes géologiques, etc.) mais aussi les attaques terroristes ou accidents industriels.
La recherche visera à : prévenir et réduire les pertes en vies humaines, les dommages pour la santé et l'environnement, les dommages économiques et matériels causés par des catastrophes; améliorer la compréhension et la réduction des risques de catastrophes et de l'apprentissage en milieu de catastrophe.

(2) **Protection et Sécurité**: sont considérées les menaces terroristes et la criminalité. Il s'agit de protéger les personnes, les espaces publics et les infrastructures critiques, aussi bien contre des agressions physiques, que des cyberattaques ; la recherche, sous ce volet, soutient donc la lutte contre le terrorisme, la radicalisation et la criminalité, y compris la cybercriminalité.
Est également considérée la gestion des frontières de l'UE — terrestres, maritimes, aériennes. La recherche, sous ce volet, vise aussi bien le contrôle des mouvements de personnes que celui des biens. La recherche

devrait soutenir le travail des garde- frontières, et de l'agence européenne des frontières, ainsi que les douanes.

(3) **Cyber sécurité :** ce volet vise à améliorer la capacité de l'UE à se prémunir contre les cyber menaces. Dans un monde numérisé, il est de la plus haute importance de veiller à ce que nos infrastructures digitales soient protégées contre les cyberattaques. Ce volet porte ainsi sur la résilience des systèmes.

Conclusion :
Il n'y a pas de changements de fond prévus en ce qui concerne les thématiques de recherche. Il y a surtout des changements de procédure et qui vont dans le sens de ce qui a été promu dans le cadre d'H2020 : approche par missions, soutien aux utilisateurs finaux, recherche comme un élément de la chaîne de valeur suivi de déploiement des capacités.

Questions / réponses :

Certains éléments potentiellement pertinents pour la proposition ne peuvent y être intégrés car ils sont sensibles (confidentiels, par exemple, surtout dans les domaines sécurité) envisagez-vous d'améliorer ce point ?
Réponse vague de la Commission européenne, faisant référence notamment au nouvel article 16 sur la sécurité.

Présentation des aspects SHS du pôle 2 « Société sûre et inclusive »

Mme Maria Kayamanidou – Chef d'unité adjoint, unité société ouverte et inclusive, DG R&I

Le Cluster 2 représente une approche thématique pour apporter des réponses concrètes, notamment aux crises. Trois grands objectifs le structurent :

- Renforcer la base des connaissances de l'UE ;
- Donner une dynamique pour une industrie créative orientée vers l'emploi ;
- Répondre à des problèmes de société.

Ce cluster est doté d'un budget 2,8 Mds€ et, à ce stade, on ne connait pas la répartition intra cluster.

La sécurité est de nature complémentaire avec la partie dévolue plus spécifiquement aux SHS : ces deux parties se nourrissent l'une l'autre.

La partie SHS s'inscrit dans la continuité du défi 6 du programme Horizon 2020.

Les domaines d'intervention :

(1) **Démocratie dans toutes ses expressions et résolution des crises des modèles démocratiques européens**. Cette partie intègre les différents niveaux de démocratie ainsi que ses différentes formes (aspects numériques, effets des réseaux sociaux). Il s'agit de bien renforcer la transparence et la légitimité de la gouvernance démocratique en respectant les droits fondamentaux ainsi que de travailler sur des stratégies par rapport aux « ennemis » de la démocratie (radicalisation, terrorisme, les fake news….) qui séduisent les citoyens marginalisés. L'objectif est également de mieux comprendre le rôle des standards journalistiques dans une société hyper connectée. Le rôle de la citoyenneté multiculturelle et l'identité en relation avec la citoyenneté démocratique sont également des enjeux, de même que l'impact des avancées technologiques (big data, IA ...) Outre les notions de démocratie participative, l'impact des inégalités sur les démocraties sera pris en compte : combattre les inégalités revient à renforcer les démocraties.

(2) **Patrimoine culturel** : 12 Millions d'emplois sont concernés. Ce volet comprend les aspects technologiques, vers davantage d'innovation, les approches matérielles et immatérielles du patrimoine culturel. Il s'agit de renforcer également les interactions entre le patrimoine culturel et le secteur créatif émergent et de renforcer les liens entre l'innovation (technologies numériques, méthodes de restauration) et l'influence des traditions, la perception des valeurs et le sens de l'appartenance

Transformations socioéconomiques : comment réduire les inégalités qui fragilisent la gouvernance démocratique. L'accès à la formation et aux compétences, la productivité, la mobilité et l'innovation sociale permettront pour la Commission de réduire les inégalités et créer des emplois.
Les indicateurs, au-delà du PIB, seront un autre objet de travail et ouvrent en cela la réflexion sur d'autres objectifs sociétaux à prendre en considération, comme le bien-être, le développement durable, etc. Les statistiques permettront également de mieux comprendre l'innovation et la croissance. Il sera possible de travailler sur les nouveaux types d'emplois, les évolutions du marché du travail et leur impact sur l'inclusion sociale

Les impôts, taxes, système de sécurité sociale devraient permettre également d'aborder la cohésion sociale, et de réduire les inégalités. Ce sujet sera complété par une réflexion sur la modernisation des autorités publiques qui devront mieux répondre aux demandes des citoyens, en termes de transparence et d'accessibilité.
L'efficacité du système judiciaire et un accès amélioré à ses services devraient également rapprocher les citoyens de leurs institutions et amoindrir leur défiance. Enfin au sujet des migrations, la CE financera des projets ayant pour but de faciliter l'intégration des migrants au sein des sociétés européennes.

Il s'agit de renforcer les liens entre ces recherches et les décideurs politiques. Les sujets SHS de ce cluster portent sur deux axes prioritaires : le rapprochement des citoyens et des institutions publiques, et la question des inégalités économiques et sociales qui représente une force centrifuge sur toute la construction européenne.

Echanges
Si la démocratie est une partie importante des objectifs du Cluster 2, certains s'interrogent sur les contradictions entre ces priorités de recherche et l'incapacité de l'UE à régir aux coups de butoir d'Etats membres contre la démocratie, notamment en Hongrie. Pour Maria Kayamanidou, il n'y a pas d'incompatibilité entre le financement de la recherche et la poursuite de l'action politique.

Retours et propositions des sciences sociales françaises pour une société sûre et inclusive

M. Olivier Bouin – Fondation RFIEA / Alliance Athéna

L'alliance thématique nationale des sciences humaines et sociales (Athéna) est présidée alternativement par la Conférence des présidents d'université (CPU) et le Centre national de la recherche scientifique (CNRS). Créée en juin 2010, l'alliance Athéna regroupe les acteurs clés de la recherche française en sciences humaines et sociales. Ses missions : renforcer les dynamiques du système de recherche SHS et bâtir une réflexion prospective de long terme.

L'alliance Athéna a publié son rapport d'activité 2017. Elle a également fondé la plateforme FUNDIT et l'Observatoire des SHS.

L'alliance a produit également un **annuaire et une cartographie des structures de recherche en SHS en France** qui a permis de dégager des grandes tendances sur l'emploi scientifique SHS en France :

- 15 000 chercheurs dans la recherche publique et 4 000 à 5 000 chercheurs dans le secteur privé (ne sont pas comptabilisés les doctorants) ;
- Potentiel important et diversifié en termes de disciplines ;
- Très faible taux de dépôt de projets SHS aux appels nationaux et européens mais un très bon taux de succès.

L'alliance Athéna souhaite **accroître la réponse française** aux appels à projets européens et **augmenter la part des financements obtenus par les équipes françaises** en Europe : préparation de la programmation des SHS dans Horizon Europe et en particulier dans le Cluster 2. Elle encourage la mobilisation et le réseautage des experts, des équipes de recherche pour qu'ils aient une vraie place dans le processus d'élaboration des programmations européennes.

L'Alliance Athéna coordonne les positions des organismes de SHS sur les questions liées aux financements européens de la recherche et de l'innovation.

Concernant le programme Horizon Europe :

Quatre principes

1. Nécessité d'un grand « cluster » thématique fortement centré sur les questions humaines et sociétales telles qu'abordées aujourd'hui par les sciences sociales et les humanités (questions relatives à la démocratie, aux mutations sociétales et technologiques, aux héritages culturels).

2. Nécessité de disposer d'**une mission centrée sur une recherche appliquée impliquant au premier chef les communautés en sciences sociales et des humanités** (p. ex: éducation, inégalités et prévention des risques).

3. Intégration d'acteurs représentatifs des sciences sociales et des humanités aux trois étapes principales de la préparation et de l'exécution du FP9 :
- architecture du programme et définition des grandes orientations
- formulation des « grappes » thématiques et des appels à projets
- évaluation des consortia de recherche en réponse aux appels

4. Importance d'un financement adéquat et proportionnel à l'importance de la place des SHS dans les problématiques sociétales **actuelles**, dans les grands enjeux qui caractérisent l'avenir de l'Europe mais également au regard de la forte mobilisation des communautés SHS. Il est important que les appels à projets nationaux, européens, internationaux reconnaissent la place prépondérante des SHS.

L'alliance Athéna propose d'adopter une approche opérationnelle dans la préparation des projets SHS, à savoir la préparation en amont, en créant des groupes de travail pluri institutionnels et pluridisciplinaires qui définiront les thèmes futurs de la recherche européenne.
Pour atteindre cet objectif, il est nécessaire d'identifier les équipes de travail ex ante et pas ex post, d'où l'idée de la cartographie.

L'objectif est double :

- Pour les domaines dans lesquels les SHS sont plus présentes : adopter une approche innovante pour que les acteurs des SHS français puissent coopérer et pour qu'ils soient prêts à répondre aux appels à propositions ;
- Explorer de nouveaux sujets – p. ex. le littoral, le changement climatique, les inégalités, etc.

Position ATHENA sur Démocratie, Transformations socio-économiques et mutations scientifico-techniques, Patrimoine et Sécurité : voir Présentation PPT de *Olivier Bouin.*

Pour en savoir plus : http://www.alliance-athena.fr/

Le Pôle d'excellence cyber
M. Patrick Erard – Délégué général adjoint - Pôle d'excellence cyber

Créé en 2014 par le ministère des armées et la Région Bretagne, Le Pôle d'excellence cyber est une association qui fédère au niveau national des acteurs de la recherche, de la formation et de l'industrie pour contribuer à développer la filière cybersécurité (Cyber) française et la promouvoir à l'international.

Ce pôle regroupe désormais un nombre important d'acteurs majeurs, incontournables de la formation, de la recherche, du développement économique, du ministère des armées et plus d'une douzaine de grands industriels : douze grands groupes (Airbus Cyber Security, Atos-Bull, Bertin IT, Capgemini, DCI, EDF, La Poste,

Naval Group, Nokia, Orange, Sopra Steria, Thales), des PME et plus d'une quinzaine de laboratoires, d'universités et d'écoles d'ingénieurs.

Parmi les industriels, nombreux sont ceux qui sont à vocation européenne et capitaux Européens.

La Cybersécurité est présente dans le cluster 2 du futur programme-cadre, mais elle est dans les faits désormais présente partout ou presque, par exemple elle a toute sa place dans le cluster 4 également, entre autre…
La Cybersécurité est transverse, et les problématiques qui sont les siennes sont illustrées quotidiennement – Ex : de nombreux constructeurs de solutions et matériels informatiques se font prendre à mettre sur le marché des solutions comportant des portes dérobées (backdoors).On peut citer les exemples de matériels HP et Dell, marques connues du grand public, qui se sont avérés comporter des éléments de type keylogger ou tracking qui posent un problème grave de sécurité.
Plusieurs pays revendiquent même d'installer de telles backdoors dans leurs produits.

Contrairement à ce que la légende urbaine se plaît à raconter, à l'origine, le hacker est quelqu'un de bien, qui cherche des choses que personne d'autre que lui n'aurait l'idée de chercher. Et surtout le hacker trouve, ce qui lui permet d'aider, de nous aider, à disposer d'une meilleure sécurité. Dans ce cas, on les nomme « les white hat ».
Il y a bien sûr d'autres types de hackers, moins bien intentionnés.

L'enjeu au niveau Européen, c'est qu'il faut que nos matériels soient certifiés en termes de Cybersécurité. C'est entre autres pour cette raison que la région Bretagne est membre du Board de l'ECSO[3], le partenariat Public Privé qui s'est constitué à l'initiative de la Commission européenne dans les domaines de la Cybersécurité et qui travaille sur ces questions.

Concernant le matériel informatique, un autre exemple : pour ce qui est des routeurs nous avons souvent (pour schématiser) le choix entre ceux de la marque CISCO et ceux de la marque HUAWEI. En fait, les deux sont risqués en termes de Cybersécurité.

Il nous faut donc promouvoir une industrie Européenne dans ce secteur.

Le pôle Cyber stimule le développement de la recherche académique Cyber, l'offre de formation cyber (initiale, continue, supérieure), et la base industrielle et technologique de cybersécurité, avec une attention particulière portée aux PME-PMI innovantes, y compris à l'international.

3 dimensions culturelles fortes :
- Civile et militaire
- Publique et privée
- Recherche et Industrie

Le Pôle d'excellence cyber répond ainsi à trois enjeux majeurs, au profit de la communauté nationale de cyberdéfense et de cybersécurité :

- Disposer des compétences nécessaires pour répondre aux besoins de développement de la filière,
- Disposer d'une offre de recherche en adéquation avec les besoins du ministère et des industriels,
- Disposer de produits et de services de confiance.

Les actions concrètes et les résultats du Pôle, ce sont par exemple quatre chaires industrielles concernant la cyberdéfense, la cyber navale, l'analyse de la menace et les systèmes industriels critiques, plus de 20 nouvelles formations dont le mastère spécialisé conduite des opérations et gestion de crises en cyberdéfense, 12 M€ sur

[3] L'ECSO est une association dont l'objectif est de promouvoir le marché de la cybersécurité en Europe et de stimuler les efforts de recherche appliquée dans ce domaine.

6 ans investis en thèses, post doc et séminaires scientifiques et 6,3 M€ en plates-formes de recherche et de formation.

Le pôle Cyber forme entre 2000 et 2800 étudiants par an. Notre catalogue de formations est fort de 100 offres distinctes, dont 22 sont de nouvelles formations civiles et militaires. A également été créé le laboratoire de haute sécurité de l'INRIA à Rennes.

Bien sûr pour compléter cette offre, le pôle travaille à la fois sur les compétences initiales et les compétences à développer dans la durée, de façon, à former aussi bien les techniciens de très haut niveau que les décideurs.

Le pôle a en outre mis en place des plateformes de simulation, avec des exercices d'équipes et la simulation d'infrastructures en situations réelles. Et c'est pour toutes ces raisons combinées que le pôle est l'organisateur du grand évènement de Hacking Européen.

Exemple : 3ème édition du challenge étudiant d'attaque/défense lors de l'European Cyber Week 2018
https://www.pole-excellence-cyber.org/evenement/3eme-edition-du-challenge-etudiant-dattaque-defense-lors-de-leuropean-cyber-week-2018/

Au-delà des problématiques de la recherche, de la formation et des grandes industries, il faut être prêt à protéger nos startups et PME. C'est un aspect beaucoup trop souvent oublié et négligé.

Pour plus d'informations : https://www.pole-excellence-cyber.org/recherche/

Table ronde : le contrat social numérique du 21ème siècle
Mme Fabrizia Benini– Chef d'unité Economie et compétences numériques, DG Connect

M. Mark Hunyadi – Professeur de philosophie sociale, morale et politique à l'Université catholique de Louvain (UCL): blog : https://markhunyadi.wordpress.com/
Publications : https://markhunyadi.wordpress.com/articles/

M. Claude Kirchner – Directeur de recherche émérite à l'INRIA, président du COERLE de l'INRIA.
Publications : https://dblp.org/pers/hd/k/Kirchner:Claude

Modérateur : M. Gaël Brosseaud - Chargé de mission, CLORA

Pourquoi un contrat social numérique ?

Il ne sert à rien de diaboliser le numérique, introduit Mark Hunyadi. Au contraire, ce serait contre-productif : le numérique augmente et simplifie l'activité humaine. Promouvoir le numérique, c'est garantir notre souveraineté, renchérit Claude Kirchner. La cybersécurité est capitale : au niveau individuel, les appareils que nous utilisons tous les jours – téléphones, ordinateurs - jouent un rôle majeur dans nos vies professionnelles et personnelles. Au niveau d'un état, la sécurité des systèmes d'information est un enjeu majeur pour le bien-être de toute la population.

Nous, humains, sommes aussi des systèmes d'informations qui se complètent, interagissent, collaborent et se combinent. Les systèmes numériques et l'humain sont « compatibles », en ce qu'ils sont tous deux des systèmes de traitement d'information. Aussi, comme on peut « hacker » un système numérique, on peut aussi « hacker » l'humain. Autrement dit, on peut « tromper » son système de traitement de l'information, avec quelques « inputs » judicieusement choisis. Par exemple, un humain réagit mieux au visage d'un autre humain qui lui ressemble, et ce sans raisonnement conscient. En utilisant ce type d'information, on peut « hacker », manipuler l'humain, et le numérique permet de le faire à grande échelle en délivrant des messages personnalisés à des groupes de population profilés.

C'est pour cela qu'il est nécessaire de réfléchir aux enjeux éthiques et sociétaux du numérique, tout en maintenant un bon niveau technologique. Comment, dès lors, doit-on définir le cadre éthique du numérique ?

Vers une « grande éthique » pour définir les finalités idéales de la transformation numérique.

Il s'agit alors de définir un « contrat social du numérique », c'est à dire ce que nous voulons, en tant que société, de la transformation numérique, les fins de cette transformation. Cependant, selon Mark Hunyadi, on se heurte rapidement à la logique libérale européenne, la « petite éthique ». En effet, le numérique a un principe de plaisir : il est extrêmement satisfaisant d'utiliser les outils numériques. C'est « pratique », c'est « rapide », c'est « agréable », addictif. L'individu est attiré par le numérique. La « petite éthique » libérale, individualiste, ne permet pas de créer un modèle de société, une réflexion globale sur les fins de la transformation numérique. Une telle réflexion empièterait sur la liberté de l'individu de jouir du numérique comme il le souhaite.

Pourtant, une éthique globale est bien en train de se construire, c'est celle que les géants du numérique souhaitent. L'éthique libérale individualiste laisse à ces géants le soin de décider des fins de la transformation numérique, et de la forme de la société qui en résultera. En effet, les individus, en utilisant leurs téléphones et leurs ordinateurs, en surfant sur internet, se placent dans le cadre qui a été créé pour eux, alimenté par ces géants du numérique et s'y conforment.

La solution est de construire une « grande éthique », une éthique de société, qui transcende l'individu. Un projet commun de définition de l'avenir, pour définir ce que nous voulons de la transformation numérique.

Des solutions politiques incomplètes ?

La Commission européenne est consciente des problèmes éthiques et sociaux liés à la transformation numérique, et a fait plusieurs propositions dans ce sens :

- Dans le cadre de la stratégie sur l'IA, une partie est dédiée à l'élaboration d'un cadre éthique pour l'intelligence artificielle : « nouvelles technologies ne signifie pas nouvelles valeurs ».
- Pour la protection des données personnelles, le RGPD sera complété par la directive e-privacy.
- La préparation aux transformations du marché du travail est également un enjeu majeur pour la Commission européenne : dans le cadre de digital Europe et Erasmus +, l'Union européenne devra tenter de renforcer les compétences numériques de sa population (aujourd'hui, 44% des européens n'ont pas les compétences numériques de base.)
- La nécessité de mettre en place des comités d'éthique aux niveaux nationaux et européens a également été citée. La Commission mentionne qu'elle met régulièrement en place de tels comités, par exemple le groupe de haut niveau sur l'intelligence artificielle, ou l'*advisory group* sur les dimensions éthiques de la protection des données

La salle et les panelistes conviennent de la nécessité d'initier des réflexions, à la fois globales et les thématiques, sur l'élaboration d'un contrat social numérique fondé sur les valeurs européennes.