Sous la présidence de Corinne Erhel,
députée des Côtes-d'Armor,
et Laure de La Raudière, députée d'Eure-et-Loir

Sous le parrainage
de Jean-Yves Le Drian,
Ministre de la Défense

Sous le parrainage
de Bruno Le Roux,
Ministre de l'Intérieur

4èmes Assises de la Souveraineté Numérique

"Souveraineté numérique et cybersécurité"

SYNTHÈSE
Auteur : Nicolas Brizé

Mercredi 29 Mars 2017
9h00 / 13h00
Maison de la Chimie
28, rue Saint-Dominique
75007 PARIS

Au moment où nous nous apprêtions à publier cette synthèse, nous avons eu la tristesse d'apprendre le décès de Madame la députée Corinne Erhel, co-présidente des Assises de la Souveraineté Numérique.
Nous tenions ici à rendre hommage à celle qui, depuis quatre années, a accompagné nos travaux avec assiduité et gentillesse et a permis, non seulement à ces Assises de devenir le grand rendez-vous institutionnel de la souveraineté numérique mais encore de contribuer à en faire émerger les enjeux pour l'avenir de notre pays.
C'est naturellement à elle que nous dédions ce document.

L'équipe organisatrice

Édito

Le destin de la France dépend désormais de sa capacité numérique !

Depuis des temps immémoriaux, le prix de la sécurité et de la paix pour un Etat était souvent celui d'une limitation de ses libertés et de son indépendance. Une perte de souveraineté néanmoins considérée comme acceptable au regard des bénéfices ainsi procurés par des alliances avec des Etats amis ou la protection d'un Etat plus puissant et mieux armé.

Animé par la volonté de ne pas soumettre la défense de la France, ni de confier sa destinée à son grand allié américain, le général de Gaulle1 a, en décidant le retrait de notre pays de l'OTAN en août 1967, rompu ce paradigme et introduit une nouvelle stratégie, celle de la réponse du « faible au fort », rendue possible par notre maîtrise des technologies nucléaires et la constitution de notre propre arsenal de dissuasion.

La transformation numérique aujourd'hui à l'œuvre dans tous les domaines introduit aujourd'hui une nouvelle donne dans la stratégie de défense des Etats dont les manifestations sont désormais de plus en plus visibles sans être, néanmoins et à ce stade, spectaculaires : Blocages de sites internet, désinformation, attaques DDoS, manipulation de données sensibles, … jusqu'aux récentes accusations d'ingérences russes dans l'élection présidentielle américaine de 2016 qui ont fait l'objet des représailles diplomatiques2 les plus importantes depuis la guerre froide. Mais il est clair que cette réponse conventionnelle à des attaques qui ne le sont plus, ne pourra être efficace, parce qu'inappropriée.

Aujourd'hui, et à l'heure du « tout numérique » la destabilisation d'une entreprise, d'une organisation ou même d'un Etat peut être le fait d'un simple « hackeur » doté de moyens modestes en comparaison des armes conventionnelles. Plus besoin d'aviation pour paralyser des voies de communication, anéantir des moyens de production ou provoquer de graves troubles dans l'organisation d'une société numérisée. L'objectif de l'assaillant n'est ainsi plus de mettre la main sur un territoire ou une richesse, mais de prendre la main sur le système qui les gouverne.

La dissuasion consistait à prévenir un acte en persuadant celui qui l'envisageait que les coûts qui en résulteraient inéluctablement en excèderaient les bénéfices attendus3. Mais ici l'acte peut-être banal et le fait d'un individu isolé. Et la réponse d'autant plus problématique.

Dans ce contexte, la protection semble le seul recours. Une protection qui requiert un haut niveau technologique et en permanence challengée. Aussi, s'il semble naturel de choisir les meilleures technologies pour l'assurer, la question se pose, différemment mais une nouvelle fois, de la souveraineté sur ces technologies. Car, et c'est là le paradoxe, nous voilà revenu à un cadre conventionnel où la protection est assurée par le fort. Technologiquement cette fois-ci. Et c'est bien ce qui est en train de se produire avec la perte de nos champions technologiques ou leur fuite vers des contrées plus propices à leur expansion. Mais aussi avec la pénétration de nos organisations et entreprises par des solutions informatiques sur lesquelles nous ne sommes plus en mesure d'exercer la moindre autorité et le pillage en règle de nos données par des entreprises hégémoniques.

Il est clair qu'aujourd'hui, notre souveraineté, c'est à dire notre capacité à choisir le monde dans lequel nous voulons vivre aujourd'hui et dans lequel nous voulons que nos enfants vivent demain, passe la maîtrise des technologies numériques.

A l'ère de l'internet des objets et de la blockchain, la vision naïve ou romantique d'un numérique libertaire est devenu dangereuse et il est grand temps que la France se dote d'une véritable et ambitieuse politique de souveraineté numérique.

Jacques Marceau
Président d'Aromates
Fondateur des Assises de la Souveraineté Numérique

1. Charles de Gaulle, Discours et Messages – Tome 5, page 201 - Plon
2. Missy Ryan, Ellen Nakashima et Karen DeYoung, « Obama administration announces measures to punish Russia for 2016 election interference », The Washington Post, 29 décembre 2016
3. Bruno Tertrais, « La logique de dissuasion est-elle universelle ? » [archive], sur Ministère de la Défense Site de référence [archive]


NOKIA
Accroître les possibilités humaines d'un monde connecté
nokia.com

FORMER, INNOVER, CRÉER
AU SERVICE DU DÉVELOPPEMENT ÉCONOMIQUE

Au cœur des transitions **numériques, industrielles, énergétiques**

Servir l'innovation grâce à la recherche académique et partenariale

Plus de 2 700 enseignants-chercheurs, chercheurs, ingénieurs de recherche et doctorants

Près de 80 start-ups créées chaque année

2 labels Carnot

www.imt.fr

Former pour concevoir l'avenir

Le premier groupe français de grandes écoles

13 400 étudiants ingénieurs, managers et docteurs

25 MOOC, 316 000 apprenants dans le monde

Institut Mines-Télécom

Eurecom
IMT Atlantique
IMT Lille Douai
Mines Albi-Carmaux
Mines Alès
Mines Nancy
Mines ParisTech
Mines Saint-Étienne
Télécom École de Management
Télécom ParisTech
Télécom SudParis

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

Programme

8h00 / 9h00 Petit déjeuner networking

9h00Accueil

Corinne ERHEL, *députée des Côtes-d'Armor*

9h10Allocution d'ouverture

Général Jean-Marc LATAPY,
Général de division, directeur central adjoint de la DIRISI

9h20Keynote

Vice-amiral Arnaud COUSTILLIERE,
Officier Général Cyberdéfense, Etat-major des armées

9h30Table ronde 1 : « Quelles technologies et quelle stratégie industrielle pour une cybersécurité souveraine ? »

Introduction et modération : Louis NAUGÈS, CEO, *Dhasel Innovation*

Intervenants :

- Henri d'AGRAIN, *délégué général du CIGREF, membre du conseil scientifique de l'Institut de la Souveraineté Numérique*
- Alain BOUILLÉ, *président, CESIN*
- Marc CHARRIERE, *directeur des relations institutionnelles, Nokia*
- Philippe GAILLARD, *président, CyberD SAS*

10h30 Table ronde 2 : « Quel enseignement supérieur et quelles formations au service d'une cybersécurité souveraine ? »

Introduction et modération : Cathie-Rosalie JOLY, *Université de Montpellier*

Intervenants :

- Christian HARBULOT, *directeur de l'Ecole de Guerre Economique*
- Francis JUTAND, *directeur général adjoint de l'Institut Mines Télécom, membre du conseil scientifique de l'Institut de la Souveraineté Numérique*
- Didier RENARD, *président de l'Institut de la Souveraineté Numérique*
- Muriel TOUATY, *directrice générale, Technion France*

11h30 La géopolitique de l'internet et ses impacts sur la cybersécurité des entreprises

Julien NOCETTI, *chercheur au Centre Russie/NEI de l'Ifri*

11h50 Table ronde 3 : « Vers une politique publique de « cybersécurité » ?

Introduction : Bernard BENHAMOU, *secrétaire général de l'Institut de la Souveraineté Numérique*

Modération : Thibault VERBIEST, *avocat associé, de Gaulle Fleurance & Associés*

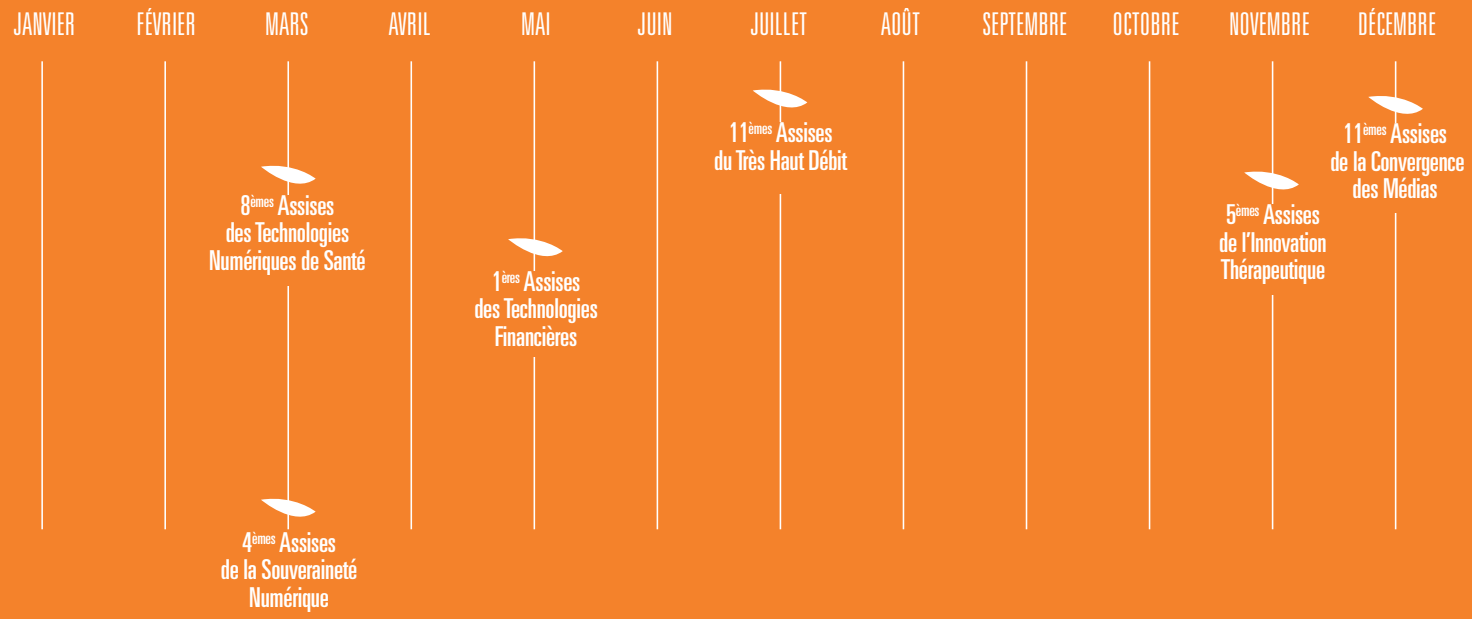
Intervenants :

- Bernard BENHAMOU, *secrétaire général de l'Institut de la Souveraineté Numérique*
- Philippe DEWOST, *directeur adjoint, Mission Programme d'Investissements d'Avenir, Caisse des Dépôts*
- Guy Philippe GOLDSTEIN, *Senior Analyst, Cyberdesk Wikistrat*
- Lionel TARDY, *député de la Haute-Savoie*

13h00 Conclusion

Laure de LA RAUDIÈRE, députée d'Eure-et-Loir

Calendrier des événements 2017



Aromates Rencontres et Débats en chiffres :

- 11 années
- 75 colloques
- 225 débats
- 11000 participants
- 1400 intervenants

Contact :
Laurent Tordjman, responsable des événements et partenariats
ltordjman@aromates.fr / 01 46 99 10 86

Aromates
RENCONTRES & DÉBATS

169, rue d'Aguesseau - 92100 Boulogne
TEL : +33 (0)1 46 99 10 80
www.aromates.fr

Avertissement : Copyright

Aromates
169, RUE D’AGUESSEAU
92100 BOULOGNE-BILLANCOURT - FRANCE

Sommaire détaillé

1. Le destin de la France dépend de sa capacité numérique !

Jacques MARCEAU, président d'Aromates

Nous avons créé l'Institut de la souveraineté numérique et ces Assises il y a un peu plus de 4 ans. Dans le meilleur des cas, on a été considéré comme des fantaisistes, et dans le pire, comme de dangereux réactionnaires.

1.1 Les failles de souveraineté

Appliquée au monde du numérique, la souveraineté n'est pas vraiment un oxymore en ces temps troublés par les révélations d'Edouard Snowden, les attentats terroristes ou le rançonnage numérique, et demain peut-être le rançonnage de nos objets connectés, de nos véhicules, et le pillage de nos données personnelles à grande échelle, sur des plateformes dont les utilisateurs auraient aimé qu'elles restent bien étanches !

La liste est longue de ce que l'on peut dorénavant appeler des « failles de souveraineté ». Elles mettent en péril non seulement la vie privée des citoyens, mais aussi le secret des affaires et la sécurité de notre pays.

Au-delà d'une salutaire prise de conscience que nous appelions de nos vœux il y a encore quelques mois, tous ces événements ont déclenché un torrent de déclarations, propositions, mesures et textes. La souveraineté est devenue un enjeu majeur de politique. C'est du destin de la France dont il est question.

1.2 Les entreprises dans l'œil du cyclone

Aujourd'hui, la déstabilisation d'une entreprise, d'une organisation ou même d'un Etat, peut être le fait d'un simple et seul « hacker » doté de moyens modestes en comparaison avec les armes conventionnelles. Plus besoin d'aviation, de bombes ou autres systèmes d'armes sophistiqués pour paralyser des voies de communication, anéantir des moyens de production ou provoquer de graves troubles dans l'organisation d'une société numérisée. L'objectif de l'assaillant n'est plus de mettre la main sur un territoire ou une richesse, mais de prendre la main sur le système qui les gouverne.

Le numérique irrigant le fonctionnement de tous les rouages de notre société, sa protection dépend désormais de son maillon faible. Nos entreprises, y compris de nombreuses PME, sont devenues de nouveaux facteurs de vulnérabilité.

Cette intrication entre l'économie et la sécurité nationale n'est pas nouvelle. Elle est même historique. Mais à l'heure du « tout numérique », elle prend une dimension nouvelle et inédite. Dans cette planète digitale qui est la nôtre, l'entreprise la plus petite devient un facteur de vulnérabilité, et les plus grandes – les géants du numérique – un facteur de risque, leur volonté hégémonique ne faisant plus de doute pour personne, et leurs moyens technologiques et financiers dépassant de loin celui de certains États. La récente nomination au Danemark d'un ambassadeur auprès des GAFA en est une expression frappante.

Je remarque que notre assistance est composée de représentants du gouvernement, de parlementaires, de militaires et d'entrepreneurs. Cette diversité me réjouit.

1.3 Feuille de route des Assises

Nos travaux de la matinée sont structurés autour de 3 grands enjeux, à l'image des 3 piliers de la souveraineté numérique que sont la maîtrise des technologies et des standards, la souveraineté des compétences, et enfin le droit :

1. Quelle stratégie industrielle et quels choix technologiques vont permettre à nos entreprises et à nos institutions d'assurer une cybersécurité souveraine ?

2. Quelle formation de nos ingénieurs et techniciens au service de notre cybersécurité souveraine, et j'ajouterais leur loyauté et leur maintien sur notre territoire et dans nos entreprises ?

3. Quelle politique publique de cybersécurité en France et en Europe ?

Je tiens à remercier chaleureusement Corinne Erhel, députée des Côtes-d'Armor, et Laure de La Raudière, députée d'Eure-et-Loir, pour l'intérêt qu'elles portent à ces questions, et leur fidélité à ce rendez-vous.

Je remercie également le général Jean-Marc Latapy, qui représente le ministre de la Défense, ainsi que le vice-amiral Arnaud Coustillière, officier général Cyberdéfense à l'Etat-major des armées, à la fois pour leur présence et leur participation à nos échanges.

Enfin, je salue le comité scientifique de l'Institut de la souveraineté numérique pour sa contribution à nos travaux.

2. Introduction des Assises

Corinne ERHEL, députée des Côtes-d'Armor

La cybersécurité est un thème cher au ministre de la Défense Jean-Yves Le Drian, qui a su au cours de ces années structurer et mettre en œuvre une doctrine en matière de cyberdéfense, et donner un certain nombre de perspectives et d'objectifs en matière de cybersécurité.

Avec ma collègue Laure de La Raudière, nous avons rendu récemment notre 4ème rapport d'information sur les objets connectés[1]. S'ils représentent une opportunité économique considérable, les objets connectés peuvent aussi potentiellement présenter des failles de sécurité sur lesquelles il faut une réflexion et une action beaucoup plus approfondies.

2.1 Les enjeux de la souveraineté numérique

La souveraineté numérique couvre de nombreux sujets : les réseaux, les équipements et les données. Si les données constituent un gisement de valeurs, d'opportunités et d'innovation, offrant des perspectives de croissance et de création d'emplois, la circulation des données pose des questions en matière de protection, que ce soient les données personnelles ou les données relevant du secret des affaires.

La souveraineté numérique réinvente le concept de souveraineté en lui donnant une dimension plus vaste à l'heure du numérique. Ce concept exige une réflexion à tous les niveaux de notre société, individus, acteurs économiques, État, pouvoirs publics, collectivités, et à l'échelle supranationale, notamment au niveau européen.

Il faut :

- garantir que le déploiement des réseaux fixes et mobiles, en particulier dans leurs parties actives ou cœur de réseau, ne génèrent pas de nouvelles vulnérabilités.

- engager une vraie réflexion industrielle en termes d'équipements télécoms, en France et a minima à l'échelle européenne. L'Europe n'a pas été suffisamment vigilante au cours de ces dernières années.

- intégrer la notion de souveraineté individuelle à la réflexion. Le citoyen ou l'entreprise doit pouvoir maîtriser ses données, avoir la pleine conscience de leurs valeurs, des enjeux, et également assurer une diffusion qui peut être consentie et réversible.

2.2 Les cyberattaques se multiplient

Le rapport annuel de Symantec[2] place la France dans le top 10 des pays où la cybercriminalité est la plus active, avec :

- 400 000 attaques via des ransomwares[3],

- 300 000 arnaques sur les réseaux sociaux,

- 43% des entreprises œuvrant dans l'énergie touchées au moins une fois par une cyberattaque, et 47% des entreprises du secteur industriel dans son ensemble.

---

[1] Rapport d'information sur les objets connectés, Commissions des affaires économiques, Corinne ERHEL et Laure de

[2] Internet Security Threat Report 2016 (ISTR) de Symantec. https://resource.elq.symantec.com/LP=2899?inid=symc_threat-report_istr_to_leadgen_form_LP-2899_ISTR21-report-main

[3] Les ransomwares sont des logiciels qui bloquent vos données en échange d'une rançon.

Cette multiplication des attaques contre les individus ou les infrastructures critiques est une préoccupation majeure pour les pouvoirs publics.

2.3 Pour une industrie européenne de la cybersécurité

Je rejoins la position qui a été prise par le directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) lors des Assises de la sécurité et des systèmes d'information. Une nouvelle fois, il a insisté sur la nécessité d'une action collective au niveau national et d'une collaboration renforcée au niveau européen.

Dans un contexte géopolitique instable, les cybermenaces vont continuer à croître. En plus d'accompagner les opérateurs d'importance vitale, civils ou militaires, dans leurs processus de sécurisation, l'ANSSI a pour objectif de créer une industrie de la cybersécurité à l'échelle européenne.

L'harmonisation de la législation européenne est importante. Ces démarches s'inscrivent dans le cadre de la **Directive européenne NIS** (*Network and Information Security*)[4].

2.4 Une priorité nationale

Tout le tissu économique doit être en capacité de se protéger contre les attaques informatiques, des TPE jusqu'aux grands groupes.

- En France, les pertes financières liées à la cybercriminalité sont estimées à 1,8 milliard d'euros pour l'année 2016. (Source : Symantec)

Le renforcement de la sécurité des espaces numériques a été officiellement présenté comme une priorité nationale, avec la signature du Pacte Défense Cyber en février 2014[5].

2.5 Développer l'offre de formation

Dans ce contexte, l'offre de formation s'est rapidement développée ces dernières années dans les domaines de la cybersécurité et la cyberdéfense. Les établissements d'enseignement supérieur se structurent pour offrir des formations qui répondent aux besoins exprimés. La recherche de personnels qualifiés en la matière devient de plus en plus prégnante. Nous avons une carence de l'offre de formation et de personnes suffisamment formées sur ces questions.

- **Un premier pôle d'excellence Cyber a été créé en Bretagne**. Il marque une étape importante dans la structuration de l'offre de formation en matière de cybersécurité.

Pour faire face à cette situation, un bon nombre d'entreprises cherchent à former rapidement leurs personnels aux questions de sécurité informatique. Ils se tournent vers les établissements qui ont mis en place une offre de formation continue.

L'objectif, dans une première étape, est de sensibiliser les salariés à la vigilance. En parallèle, nous avons besoin de cursus longs qui formeront les experts de demain. Les entreprises ont besoin de personnes cœur de métier, avec une vision globale des enjeux. La cybersécurité fait appel à des compétences de base en matière technologique et technique, mais aussi en sciences humaines, management et éthique.

Le pôle Cyber en Bretagne soutient également les Sciences Humaines et Sociales. Inclure les SHS dans le domaine des recherches nous permettra de mieux sonder et d'adapter nos actions auprès des acteurs économiques.

2.6 L'écosystème Cyber

Basé à Rennes, le pôle d'excellence Cyber a une vocation nationale. Il a réussi à agréger les experts les plus compétents et un certain nombre de grands groupes, et surtout il a posé les bases d'un écosystème à développer en matière de cybersécurité.

---

[4] Directive sur la sécurité des réseaux et des systèmes d'information adoptée le 6 juillet 2016 par le Parlement européen et le Conseil de l'Union européenne (UE). http://eur-lex.europa.eu/legal-content/FR/AUTO/?uri=uriserv:OJ.L_.2016.194.01.0001.01.FRA&toc=OJ:L:2016:194:TOC

[5] http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber

En France, nous avons un différentiel à faire valoir. Beaucoup d'actions méritent d'être développées. La demande est extrêmement forte en France. La valorisation et l'accompagnement des écosystèmes autour de la cybersécurité sont fondamentales.

Préserver sa souveraineté ne doit pas signifier un repli sur soi, derrière des barrières ou des frontières. Dans un monde digital, ces frontières ont perdu leur sens. La souveraineté doit être synonyme d'une pleine maîtrise des enjeux, permettant l'ouverture aux autres. C'est vital dans un contexte d'innovation permanente si l'on veut profiter des opportunités offertes par le numérique.

Je tiens à saluer le travail qui a été fait par le ministre de la Défense. Il a su établir une doctrine en matière de cyberdéfense et impulser une vraie structuration des politiques autour de la cybersécurité au bénéfice de l'ensemble des acteurs et de la France. Sur ces questions, cette réflexion doit toujours être à l'échelle européenne.

J'espère que cette matinée vous permettra de porter un regard prospectif sur cette question complexe, et de faire émerger des propositions différentes et innovantes.

3. Allocution d'ouverture – **Un enjeu majeur pour la Défense**

Général Jean-Marc LATAPY, général de division, directeur central adjoint de la DIRISI[6]

« La cyberdéfense est devenue un enjeu essentiel de la souveraineté. Il faut que demain pour la France, la cyberdéfense soit considérée comme un atout essentiel de notre protection commune. »

Jean-Yves Le Drian, ministre de la Défense,
9ème Forum International de la Cybersécurité, janvier 2017

La thématique Souveraineté numérique et cybersécurité est particulièrement d'actualité et un enjeu majeur pour la défense. Le Livre blanc sur la défense et la sécurité nationale de 2013[7] a été le premier à apporter une place significative à ce domaine. Depuis, l'organisation et les moyens de la cyberdéfense ont fait l'objet d'avancées significatives au sein du ministère de la défense pour répondre aux nouvelles menaces.

Le numérique est présent partout : dans notre vie personnelle, dans la vie économique et dans les services que nous utilisons quotidiennement. Son périmètre est difficile à cerner tant l'imbrication est importante entre toutes ces déclinaisons.

3.1 La DIRISI

Au sein du ministère de la défense, la DIRISI soutient plus de 250 000 terminaux informatiques, avec plusieurs niveaux de confidentialité, sur de multiples réseaux de communication, du câble au satellite.

Elle maintient plusieurs centaines de systèmes d'information qui sont maintenant rationalisés au sein de grands datacenters.

Tous ces équipements contribuent à la fois au fonctionnement des opérations et du ministère.

Le numérique est présent au sein de l'ensemble de nos systèmes d'armes, dans toutes les plateformes de combat, que ce soit les avions de combat Rafale, les avions de transport A400M, les bâtiments de la Marine nationale et les nouveaux véhicules de l'Armée de terre du programme Scorpion pour ne citer qu'eux.

L'ensemble de ces moyens permet de mener des opérations interarmées, partout où nous opérons, au plus bas niveau tactique, au sein d'un véritable intranet tactique qui se rapproche de l'internet des objets.

La maîtrise de cette dimension numérique est complexe. Elle contribue à l'autonomie et à l'action de nos forces, et par là, à leur souveraineté.

---

[6] DIRISI : Direction interarmées des réseaux d'infrastructure et des systèmes d'informations de la défense.

[7] www.livreblancdefenseetsecurite.gouv.fr

3.2 De multiples facteurs de vulnérabilité

Les armées, elles aussi, sont exposées de manière accrue à des vulnérabilités nouvelles, en raison :

- des progrès techniques,

- de notre dépendance au numérique et aux évolutions d'internet,

- de la diversité des adversaires : activistes, Etats, groupes terroristes,

- de la multiplicité des scénarios possibles d'attaques : de l'attaque rudimentaire à l'attaque organisée à grande échelle.

Ces cybermenaces, aux réalités profondément asymétriques, peuvent avoir des effets analogues à ceux d'actions plus conventionnelles, particulièrement si les cibles touchent des infrastructures critiques ou des cibles militaires. Dans ce contexte, nous nous trouvons au sein du cyberespace dans un véritable espace de bataille.

3.3 Le Pacte Défense Cyber

Face à ces menaces, le ministère de la Défense est engagé résolument dans la mise en place d'une cyberdéfense, instrument d'une souveraineté. Elle regroupe l'ensemble des actions conduites par des moyens militaires dans le cyberespace pour garantir à la fois le bon fonctionnement du ministère et l'efficacité de l'action des forces armées.

Suite au Livre blanc sur la défense et la sécurité nationale de 2013, des mesures ont été définies dans le cadre du Pacte Défense Cyber de février 2014 en vue d'accroître la mobilisation du ministère de la défense en matière de cybersécurité.

Ces mesures visent notamment :

- à durcir le niveau de sécurité de nos systèmes d'information et des moyens de défense et d'intervention du ministère,

- à renforcer les ressources humaines dédiées à la cyberdéfense,

- à favoriser l'émergence d'une communauté nationale de cyberdéfense en s'appuyant sur un cercle de partenaires et les réseaux de la réserve,

- à préparer l'avenir en intensifiant l'effort de recherche.

Toutes ces mesures ont été mises en œuvre. Plus de 2 milliards d'euros ont été investis depuis le lancement du Pacte Défense Cyber. Elles se traduisent concrètement par la mise en place d'une organisation de la cyberdéfense, la définition de ses missions, des moyens humains et des investissements en technologies et équipements.

Ces différents points ont été présentés par le ministre de la Défense à la Direction générale de l'armement - Maîtrise de l'information en décembre 2016[8].

3.4 La doctrine de cyberdéfense

Il est indispensable de continuer à développer une doctrine de stratégie cyber de défense et d'intégrer l'ensemble des volets cyber dans notre pensée militaire.

Cette doctrine doit s'intégrer dans une stratégie d'ensemble et un champ plus large, interministériel et gouvernemental, notamment pour ce qui concerne la protection de nos infrastructures critiques.

Cette nouvelle doctrine intégrera aussi une dimension de coopération internationale et son corollaire, une définition précise de la souveraineté appliquée à ce domaine.

---

[8] Discours de Jean-Yves Le Drian à la DGA-MI, Bruz, 12/12/2016. http://www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/cyberdefense-discours-de-jean-yves-le-drian-lundi-12-decembre-2016

Ambition majeure de cette doctrine, la nouvelle organisation de cyberdéfense consacrera au sein du ministère de la Défense la création d'un commandement cyber. Placé sous la responsabilité directe du chef d'Etat-major des armées, il assistera le ministre en matière de cyberdéfense.

Les missions de la cyberdéfense peuvent être classées en 3 catégories dans un cadre juridique qui doit être clairement défini :

1ère mission : le renseignement et l'investigation pour identifier, détecter et caractériser la menace.

2ème mission : une posture permanente de protection de défense, avec des notions de défense en profondeur et de défense de l'avant. L'objectif est de couvrir :

- l'ensemble de nos systèmes, en métropole comme en opération extérieure,

- les opérateurs d'infrastructures vitales, en coordination avec l'ANSSI, auprès duquel nous pouvons intervenir lorsque la situation le requiert, via des groupes d'intervention rapides.

3ème mission : la riposte et la neutralisation, la lutte informatique offensive, afin d'agir ou de répliquer contre un ennemi cherchant à nuire nos intérêts de sécurité et de défense.

3.5 Formation : un challenge

Les moyens humains constituent l'une des conditions de succès de ces 3 missions. Au terme de la montée en puissance prévue par l'actualisation de la loi de programmation militaire[9] :

- **3 200 personnes** devraient pour la défense participer à la mission Cyber, soit plus du double des effectifs de 2012, avec en particulier un effort sur le personnel de réserve pour la cyberdéfense.

Cela nécessite des investissements importants en termes de recrutement, de formation et d'entretien des compétences. Exemple : la mise en place du pôle d'excellence Cyber inauguré à Rennes en décembre 2016.

La formation, le recrutement et la fidélisation sont de véritables challenges.

3.6 Technologies et équipements

Les investissements en technologies et équipements ont été multipliés par 3 au cours de la loi de programmation militaire actuelle. Ils permettent d'intégrer le volet cyber :

- aux travaux de conception des futurs programmes d'armement, navires, systèmes de défense aérienne,

- à l'évolution de programmes : hélicoptère de combat Tigre ou le programme Scorpion de véhicules terrestres.

- au développement de produits souverains de détection en matière de protection : sondes réseau ou produits de chiffrement (par exemple avec la mise en service de nouveaux chiffreurs aptes à protéger des informations au plus haut niveau).

3.7 Les prochains défis

Les efforts actuels ne sont qu'une étape. Ils doivent permettre de stabiliser la base de l'organisation de la cyberdéfense et de ses moyens en mesure de répondre aux menaces actuelles.

Cette cyberdéfense devra être en perpétuelle évolution pour s'adapter au contexte mouvant des agressions cyber et aussi, selon J-Y. Le Drian :

- *« Répondre au prochain défi de la cyberdéfense : non plus uniquement détecter les attaques informatiques, mais pouvoir continuer à mener nos opérations militaires en étant sous le coup d'une agression cyber et en utilisant l'espace cyber pour conduire nos propres opérations. Nous devons engager une nouvelle accélération de l'effort national afin que la France puisse faire prévaloir ses*

[9] Actualisation de la LPM 2014-2019 – Dossier thématique. www.defense.gouv.fr/fre/content/download/475995/7627327/Plaquette_d_Actualisation_de_la_LPM_2014-2019.pdf

intérêts dans ce nouveau champ de confrontation. »

4. Keynote – **Retour d'expérience du commandement de cyberdéfense**

Vice-amiral Arnaud COUSTILLIERE, officier général cyberdéfense, Etat-major des armées

La sécurisation de l'espace numérique ne fait que commencer. Face à nous, nos ennemis, nos adversaires, nos concurrents, font preuve d'innovations technologiques et techniques, en avançant totalement masqués.

4.1 La France renforce ses moyens humains

J'ai commencé à travailler dans la cyberdéfense au moment du Livre blanc de 2008. Lorsque j'ai été nommé officier général cyberdéfense en 2011, nous étions alors une centaine de personnes sur l'ensemble du ministère à traiter de manière pointue le cœur de ce sujet.

• En 6 ans, l'effectif global du ministère, mobilisable sous les ordres du commandement de cyberdéfense qui a été mis en place est passé **de 100 à 2 000 personnes** (hors personnel de la DIRISI en charge de la sécurisation au niveau de l'opérateur).

• **D'ici à 2019, 3 000 personnes** au sein du ministère traiteront de façon précise, opérationnelle et technologique, le cœur de ce sujet.

4.2 Le périmètre de la cyberdéfense

- **La transformation numérique :** le terme cyber est trop vague. Je préfère parler de numérique. Même s'il a ses caractéristiques propres, on peut y retrouver les mêmes références que dans d'autres espaces. Le numérique nous inscrit clairement dans la transformation numérique et dans la lutte des « nocifs » de tous types qui en font partie.

- **L'espace de combat :** c'est comme de naviguer dans la mer, on ne maîtrise pas tout dans l'espace numérique. On ignore ce qui se passe dans les profondeurs. En cas de tempête, on se sent tout petit. Et là, je m'adresse aux RSSI et DSI : l'espace numérique évolue à son rythme. C'est une rupture par rapport à l'informatique où un processus numérisé est maîtrisé. La nouveauté dans cet espace numérique, c'est qu'on ne maîtrise pas tout et que ça va très très vite. Les usages invitent à modifier les modes de relations entre tous les organismes, et ils dépassent les frontières. Qui aurait prévu que les GAFA deviendraient des partenaires importants dans la lutte contre le terrorisme ? Nos relations ne sont pas forcément celles que nous entretenons dans les autres espaces da façon asses formalisée.

- **L'autre :** dans cet espace, l'autre est face à nous. Un ami, un ennemi déclaré, un concurrent, un adversaire, ou un nocif. L'autre a des usages. Il va faire preuve d'innovation tactique dans l'emploi de ces usages. Il connaît bien la technologie et innove au plan technologique. C'est la « guerre hybride », les pseudo réputées attaques russophones en sont un exemple, et surtout, l'utilisation de l'espace numérique par tous les terroristes, en premier lieu par Daesh, qui a réussi à utiliser cet espace : à faire des GAFA et de certaines zones son sanctuaire numérique. Nous avons beaucoup de mal à les toucher par les voies classiques. Les usages s'imposent.

4.3 Les vulnérabilités

- **S'adapter, vite** ! Dans cet espace, nos ennemis font preuve d'innovation. Quand on est responsable d'un gros organisme, c'est compliqué de faire preuve d'innovation, surtout quand on est embourbé dans la technique et que l'on n'a qu'une vision technique.

- **Le maillon faible.** L'objectif de l'adversaire est de nous faire mal. Pour cela, il va faire de l'action indirecte, attaquer le maillon faible. Si je veux faire tomber une entreprise, je vais plutôt couper son réseau électrique ou sa climatisation plutôt que de m'attaquer à son système d'information. Et donc je dois trouver le maillon faible. Dans une organisation, c'est surtout l'humain. Il est au premier rang de la ligne de défense. En même temps que les processus techniques, l'éducation des personnes est donc la première chose à travailler. Il faut éviter que des individus puissent être les relais des attaques (consentants ou non consentants). L'évaluation des risques d'une attaque informatique commence donc par le volet social : on s'intéresse d'abord à tous ceux qui font l'interface de l'entreprise avec l'extérieur, puis à tous les autres. Il est plus facile d'attaquer une secrétaire ou un moniteur de sport – qui eux aussi ont accès au réseau de l'entreprise –, pour

ensuite remonter vers les administrateurs. Aujourd'hui, dans une entreprise ou un réseau, un administrateur a des pouvoirs exorbitants, même si on les considère comme des acteurs techniques de bas niveau.

- **L'attaque.** C'est donc une action combinée, qui se caractérise par une approche des individus et des administrateurs, une approche technique, ou des rumeurs (hoax). On attaque la réputation pour fragiliser la confiance en faisant courir des rumeurs. Le groupe Vinci a chuté en Bourse en quelques heures à cause d'une rumeur très bien organisée qui a circulé sur les réseaux sociaux.

- **La géostratégie des câbles.** Cet espace commence par les câbles. Il y a une géopolitique, une géostratégie des câbles sous-marins, des datacenters. Si les Russes placent des datacenters dans les zones extrêmement froides du nord de la Russie, c'est aussi pour se rapprocher des clients du continent américain, de façon à répondre très rapidement aux puissances de calcul. Cette implémentation n'est pas laissée au hasard. Face aux DDoS (attaque par déni de service), il faut de la puissance de calcul. Un certain nombre de GAFA détiennent cette puissance de calcul. Dans quelques années, ce seront aussi de grands acteurs de la sécurité.

- **La réputation.** Les réseaux sociaux jouent un rôle très important. Le numérique ne se réduit pas à l'informatique. L'attaque de la réputation, le sabotage, la prise en otage informatique marchent aussi très bien. Peu de plaintes sortent au grand jour. Mais l'innovation technique et la tactique sont permanentes. Les attaquants ont au moins une longueur d'avance. Pour leur répondre, il faut prévoir des défenses en profondeur, retarder leur attaque, disposer de systèmes de défense mobiles et mouvants.

4.4 Les 3 cercles de souveraineté

Quels sens faut-il donner à la souveraineté ? La donnée est au cœur de l'espace numérique. Il faut la protéger. Les espaces de souveraineté sont différents :

1. Souveraineté individuelle : qu'est ce que l'on accepte de donner ? A l'Etat ? Aux acteurs commerciaux ? Qu'est-ce qu'on n'a pas envie de donner : protection de nos vies privées, de nos mouvements, etc. Il faut réinventer la souveraineté.

2. Souveraineté de l'entreprise : la donnée est tout ce qui fait sa richesse. L'échange des données à travers le monde fait la richesse du commerce.

3. Souveraineté de l'Etat, la nôtre. Il faut absolument la protéger.

4.5 Le retour des attaques réseau par saturation

On assiste à un retour très fort et très rapide des attaques par saturation. Il est possible de faire tomber des plaques complètes du Net.

- Le malware Mirai a montré qu'un certain nombre d'acteurs – étatiques ou non – peuvent mettre à mal la résilience du Net.

- On a vu des plaques complètes du Net s'effondrer pendant quelques heures au niveau du Vietnam, et plus clairement du Liberia.

- Dans cette géopolitique des câbles et des flux, il y a aussi des actions aux approches des câbles transatlantiques. Isoler l'Europe et les États-Unis peut faire partie des grandes hypothèses de tension entre les grandes nations.

_ Jacques MARCEAU : Le facteur humain est essentiel. Confiance, information… nous sommes dans la société de l'information. La cyberdéfense concerne les particuliers et les entreprises, le secret des affaires. Pour que la cybersécurité reste souveraine, quelles seront les technologies, les acteurs, les contrôles ? Comment l'entreprise peut-elle se défendre quand la guerre économique se déplace vers le cyberespace ? Avec quels acteurs ? Avec quels moyens technologiques ? Si effectivement gagner en cybersécurité fait perdre en souveraineté, c'est une vraie question. Enfin, quelle est l'économie qui la sous-tend ?

5. Table ronde 1 – **Quelles technologies et quelle stratégie industrielle pour une cybersécurité souveraine ?**

Introduction et modération : Louis NAUGÈS, CEO, Dhasel Innovation

Dans mon métier, qui est d'accélérer la transformation numérique dans des entreprises publique ou privées, on se heurte à ces phénomènes de cyberdéfense et de sécurité. Si la demande de cybersécurité est universelle, il y a toujours un challenge entre la réflexion et l'action. L'Europe est le bon échelon face aux GAFA américains et asiatiques Tencent, Xiaomi et autres Alibaba, qui investissent des milliards de dollars dans le cloud et les outils numériques.

5.1 Pour une industrie souveraine du composant électronique

Henri d'AGRAIN, délégué général du CIGREF, membre du conseil scientifique de l'Institut de la souveraineté numérique

La cybersécurité conditionne la confiance des citoyens et des entreprises dans la transformation numérique de la société. Elle garantit nos libertés démocratiques et notre prospérité économique. C'est un facteur clé de la souveraineté, pour la France et pour l'Europe, dans cet espace stratégique que constitue aujourd'hui le cyberespace.

Depuis plusieurs années, cette capacité des grands États à agir dans le cyberespace pour y protéger leurs propres intérêts, éventuellement en dénier l'accès ou l'usage à leurs adversaires ou concurrents, connaît une croissance exponentielle. Les États-Unis, la Chine, la Russie, et dans une moindre mesure le Royaume-Uni, la France, l'Allemagne ou l'Iran, ont pris conscience de ce phénomène et de sa géopolitique. Leurs efforts budgétaires et humains sont significatifs pour maîtriser leur sécurité dans le cyberespace, la protection numérique de la population et la défense de leurs intérêts économiques.

En France, les moyens et effectifs de l'ANSSI se sont renforcés dans ce domaine. La stratégie nationale pour la sécurité du numérique est un progrès considérable. Est-ce suffisant ? Je ne pense pas.

Le composant électronique est trop rarement abordé lorsqu'on parle de cybersécurité. Pourtant l'autonomie stratégique en matière de composants électroniques est l'une des conditions d'une cybersécurité effective. Cette autonomie est absente aujourd'hui en France et en Europe.

Sans une industrie souveraine du composant électronique, il n'est pas possible de garantir dans le temps la sûreté de fonctionnement des infrastructures sensibles. Les États-Unis, la Chine et la Russie l'ont bien compris, les deux derniers développent actuellement les moyens de leur autonomie en la matière avec des approches différentes.

Quand on utilise un microprocesseur, notamment d'origine américaine, nous sommes incapables d'avoir une garantie sur ce qu'il fait effectivement et de savoir ce qu'il n'est pas sensé faire. C'est un sujet très prégnant.

La France et l'Union européenne ont-ils les moyens de leur indépendance dans ce domaine des microprocesseurs ? Dans les conditions actuelles, il semble que non.

- **En Chine, 150 milliards de dollars sur 10 ans** sont mis en œuvre dans un programme destiné à construire une industrie du microprocesseur maîtrisée et auditable par les Chinois.

- **Aux États-Unis,** la consolidation dans l'industrie du microprocesseur a fait l'objet de fusions-acquisitions d'environ **145 milliards de dollars**. Le président Obama, quelques mois avant de quitter ses fonctions, a réuni un comité d'experts composé de pdg de l'industrie du semi-conducteur afin d'assurer la capacité de leadership des États-Unis sur ce domaine dans la durée.

Les politiques menées dans ce domaine en France et en Europe sont très loin du compte.

- **En France, entre 1 milliard et 1,5 milliard d'euros** sont mis en oeuvre pluriannuellement pour conforter cette filière, qui existe encore. Fragile, elle se concentre essentiellement sur des sujets de niche.

Il est temps d'envisager une vraie politique européenne sur la durée pour reconstruire l'autonomie stratégique de la France et de l'Europe dans le domaine des microprocesseurs.

_ Louis NAUGÈS : Un microprocesseur compte actuellement entre 5 et 10 milliards de transistors. A-t-on les compétences pour tout connaître de son fonctionnement ? Il est probablement impossible de mesurer des points d'entrée masqués…

_ Henri d'AGRAIN : C'est comme un programme. Si on n'a pas le code source du microprocesseur, on ne sait pas ce qu'il fait.

5.2 Souveraineté des données : le partenariat allemand avec Microsoft

Alain BOUILLÉ, président du CESIN[10], RSSI du Groupe CDC

La souveraineté est devenue un sujet de préoccupation pour les entreprises et les administrations. La transformation numérique est en route. Elle se traduit par le recours à des technologies cloud, en particulier des solutions de type SaaS, beaucoup plus agiles et faciles à implémenter, plus collaboratives et innovantes.

Cependant, le choix est restreint : Microsoft ou Google, sinon vous êtes ringard !

C'est vers la puissance américaine que nous livrons, sur des plateaux d'argent, nos données de bureautique et de messagerie. Elles représentent parfois un gros tiers du patrimoine informationnel d'une entreprise. Dans ces mails, powerpoint, word et autres fichiers excel, il y a tout le patrimoine de l'entreprise.

Les révélations de Snowden datent de 2011, sur des actes perpétrés quelques années avant. En 2017, la CIA ne s'est pas endormie sur ses lauriers. Pas plus tard qu'hier, WikiLeaks a encore dévoilé de nouveaux forfaits grâce à un malware introduit sur les iPhones et les Mac qui résiste à la réinstallation du système d'exploitation. La CIA peut exploiter les données des possesseurs de ces appareils.

Évidemment, toutes les entreprises n'ont pas le même niveau de contraintes. Mais toutes celles qui sont concernés par une souveraineté absolue de leurs données sont condamnés aujourd'hui à la ringardise. Une circulaire émise en avril 2016 demandait aux collectivités locales de ne pas recourir au cloud public parce que leurs productions étaient considérées comme du trésor national…

Vis-à-vis de la criminalité ordinaire, Microsoft offre des niveaux de sécurité très supérieurs à ce que les trois quarts des entreprises sont capables de produire.

En Allemagne, sous une forte pression gouvernementale, Deutsche Telekom s'est associé avec Microsoft pour opérer comme « data trustee ». La solution proposée aux clients allemands consiste à utiliser les outils de Microsoft comme si vous étiez dans leur cloud, mais au moment où vous écrivez les données, elles vont s'inscrire dans des datacenters placés sous la responsabilité juridique de Deutsche Telekom, à l'abri de la curiosité directe de la CIA, en tout cas des injonctions du Patriot Act.

Microsoft annonce que 85% du CAC 40 lui a déjà confié ses données. 15% ne l'ont pas fait. Comme moi, ils sont concernés par ces problématiques de souveraineté : les collectivités locales, l'ensemble de l'Etat et des ministères. En France, on peut imaginer un copié-collé de cette solution allemande, étant entendu qu'il est plus approprié de parler d'une souveraineté européenne.

_ Louis NAUGÈS : Effectivement, les entreprises ont le choix entre Google et Microsoft. Et il faut bien choisir entre les deux. Le grand danger serait de créer une ligne Maginot numérique, comme cela a été fait il y a quelques années dans le domaine militaire.

_ Christophe DUBOIS-DAMIEN, administrateur Forum Athéna : Cet exemple de protection des données dans un cloud paraît presque trop beau. Quelle est la fiabilité de Microsoft sur un sujet aussi sensible ?

_ Alain BOUILLÉ : Gardons-nous d'être trop naïf. Quand Microsoft vous dit : « dormez tranquille en France, nous allons ouvrir les datacenters et le problème sera réglé »… Non, il ne sera pas réglé. Peut-être sur le temps de réponse et de disponibilité des données, mais pas d'un point de vue juridique. Si ce datacenter reste sous la responsabilité juridique de Microsoft, il est bien évident que le Patriot Act et tout ce qui s'ensuit s'appliqueront.

La réponse allemande me semble intéressante. Le sujet n'est pas la localisation des données. Il s'agit de

[10] Le Club des experts de la sécurité de l'information et du numérique (CESIN) coordonne les RSSI des grandes organisations françaises (300 membres).

savoir qui peut avoir accès aux données sur une injonction étatique. En Allemagne, ce sera le gouvernement allemand. En cas de bug, Microsoft devra pouvoir intervenir, sous le contrôle de Deutsche Telekom. Ce qui est différent de leurs datacenters où Microsoft est libre de faire ce qu'il veut.

5.3 Réseaux télécoms : raisonner de bout en bout, en écosystèmes

Marc CHARRIERE, directeur des relations institutionnelles, Nokia

Depuis sa fusion avec Alcatel-Lucent, Nokia est fournisseur de réseaux de bout en bout. Dans les Bell Labs et nos centres de R&D, 40 000 ingénieurs R&D sont particulièrement concernés par ce sujet. La cybersécurité doit être une préoccupation dès la conception des réseaux télécoms. Dans les prochaines années, les fonctions les plus critiques des réseaux (notamment leur pilotage mais pas uniquement…) vont être transférées vers les plateformes numériques. Avec les dizaines de milliards d'objets connectés en 2025, les plateformes numériques vont constituer un nœud critique en matière de cybersécurité.

5.3.1 La virtualisation des réseaux

Demain, la connexion de tout, partout, tout le temps, va exiger une flexibilité de nos réseaux qui vont devoir tout savoir faire. La virtualisation des réseaux va permettre de découpler les équipements des logiciels.

Pour l'instant, les réseaux publics ont des équipements réseau hardware et software, dans la nature, dans les rues, sous les antennes mobiles. Demain, les logiciels présents dans ces réseaux vont remonter vers des plateformes de cloud qui vont servir à la gestion du réseau, voire des plateformes de réseaux elles-mêmes, en dessous des plateformes qui servent aux usagers (stockage des data et applis).

C'est un gain en flexibilité : en cas de saturation des réseaux, un réseau virtualisé va permettre à l'opérateur de déplacer sa puissance à tel endroit, à tel moment.

Les applications auront des besoins extrêmement différents. L'opérateur sera obligé d'adapter en temps réel le réseau de façon à assurer :

- une sécurité maximale pour un mouvement bancaire,

- une latence minimale pour un jeu vidéo ou une vidéo 3D regardée avec un masque de virtualisation (nécessitant des débit de m'ordre du gigabits/secondes)

- le slicing, à travers la mise en place technique de classes de services informatiques à l'intérieur de ces grosses artères IP .

5.3.2 Vers une économie de flux

Nous allons passer d'une économie numérique de stockage (data–applis) vers une économie de flux. Avec ces réseaux virtuels, les applications seront de plus en plus imbriquées. Nous aurons de plus en plus de difficultés à savoir, techniquement, où sont placées les données.

Nokia est présent sur toutes ces parties du réseau, d'un point à l'autre, derrière les opérateurs. En Europe, nous sommes les seuls. Il le faut pour assurer la sécurité et la fiabilité des réseaux de bout en bout.

5.3.3 L'écosystème Nokia

En France, nous agissons étroitement avec les autorités.

- Nous assurons la vice-présidence européenne du Pôle d'Excellence Cyber (PEC).

- Au plan industriel, nous pilotons les actions du plan « Souveraineté télécoms » avec des acteurs publics et privés, l'ANSSI, Orange, SFR, Thalès, etc.

- Nous mettons en place des plateformes d'expérimentation en écosystème ouvert afin d'expérimenter ces réseaux en avance de phase et étudier les conditions de la mise en place de programmes 5G ou IoT (Internet des objets).

- Sur le site Nokia de Paris-Saclay, nous avons installé toutes les différentes configurations du réseau. Les acteurs, petits et grands, sont invités à venir tester leurs équipements IoT.

- À Lannion, nous développons une plateforme de cybersécurité en partenariat avec des acteurs institutionnels. Nous participons à toutes sortes d'écosystèmes, centres de formation, etc.

La France n'est pas un territoire suffisant pour développer ces solutions. Il faudra beaucoup de collaboration en Europe pour commencer à travailler.

5.4 Logiciels et internet

Philippe GAILLARD, président, CyberD SAS

Nous accompagnons et investissons dans des sociétés cyber françaises depuis 7 ans, et peut-être à moyen terme dans des sociétés européennes.

Pour construire une souveraineté, on doit s'appuyer sur des produits de confiance et sur un internet de confiance.

5.4.1 Créer des produits de confiance

En cyberterrorisme, nous collaborons avec tous les pays occidentaux. En cyberintelligence, nous sommes plutôt ennemis. Les informations que nous recevons dans le domaine du cyberterrorisme proviennent parfois du domaine de la cyberintelligence. Cela démontre que tous les produits américains, israéliens et anglais sont backdoorés et monitorés par nos amis américains. Ils le font de façon très officielle entre eux. Mais les Russes et les Chinois ont la même activité. Malheureusement, on ne peut pas considérer que ce soit des produits de confiance pour la France et l'Europe.

C'est pourquoi il nous semble très important de se focaliser sur des produits de confiance pour nos entreprises et nos gouvernements. Nous avons accompagné une quinzaine d'entreprises en France et l'on prévoit une trentaine supplémentaire dans les 5 prochaines années en France et dans les pays voisins.

Un produit de confiance, c'est un produit auditable dont on a compris la conception.

Nous prônons un open source de confiance, avec des personnes, des façons de développer et de mettre à disposition des produits qui soient auditables.

> • **Attention, l'open source est dans la ligne de mire des hackers.** Depuis 4 à 5 ans, certains hackers ont eu l'idée de se greffer sur les produits open source, notamment CRM, probablement avec l'aide de certains Etats. En contribuant au développement open source, ils en ont profité pour glisser tout ce qui leur est nécessaire pour exfiltrer, le moment venu, des données qui pourraient leur servir.

5.4.2 Créer un internet européen de confiance

Plus critique est la capacité à maintenir un internet actif européen, même si d'autres parties de l'internet dans le monde tombent.

Aujourd'hui le fonctionnement de notre internet est complètement dépendant des Etats-Unis. Si vous n'avez pas internet, vous n'êtes même pas capable d'envoyer un mail à votre voisin de bureau !

La cyberattaque en octobre 2016 contre Dyn[11] a fait tomber tous les serveurs de la côte Est. Et pourtant, Dyn est un prestataire composé de spécialistes. Il faut savoir que cette attaque n'a pas été poussée jusqu'au bout. Elle aurait pu aller beaucoup plus loin. Nous pensons que c'était un test.

Parallèlement, en août 2016, la Chine s'est coupée de l'internet mondial pendant une dizaine de minutes, alors qu'internet continuait à fonctionner en interne. À ma connaissance, la Chine est le seul pays capable de le faire dans le monde.

Quand vous corrélez la capacité à se couper de l'internet mondial et la possibilité de faire tomber, de façon peu coûteuse, toute la côte Est des États-Unis, on comprend qu'il est urgent de s'organiser pour être capable de continuer à fonctionner au cas où des services de ce type-là seraient attaqués.

[11] L'exemple de la cyberattaque DDoS contre le prestataire DNS américain Dyn est également cité par Julien Nocetti (ch.6) Bernard Benhamou (7.1) et Philippe Dewost (7.2).

• Pour le dire plus trivialement, **en cas de cyberguerre entre les États-Unis et la Chine, c'est l'Europe qui va morfler le plus !**

Ce sujet, extrêmement sensible, ne peut être traité qu'au niveau européen.

5.5 Discussion avec la salle

5.5.1 L'internet européen pris en tenaille entre la Chine et les États-Unis

_ Jacques MARCEAU : En 1966, la France a décidé de sortir de l'OTAN pour ne pas être prise en tenaille dans un conflit entre Soviétiques et Américains qui n'était pas le sien. Mais cette décision du général de Gaulle était sous-tendue par une capacité technologique : la possession de l'arme nucléaire à l'époque.

Aujourd'hui, nous sommes au milieu d'un terrain de jeu malsain entre la Chine et les Etats-Unis, dont nous risquons d'être les victimes collatérales, mais sans avoir véritablement de capacités technologiques à ce jour. Après avoir entendu le général Latapy et le vice-amiral Coustilliere, on voit bien que c'est une préoccupation majeure des états-majors français, qui impacte aussi le monde économique.

5.5.2 Les produits de sécurité : un problème

_ Louis NAUGÈS : No Network, no work ! On a vu que le maillon faible sera attaqué en priorité : réseau, microprocesseur, données, ou les serveurs qui les hébergent. Une vision globale de cette protection doit donc être mise en œuvre. Messieurs, reste-t-il encore un niveau à protéger ?

_ Henri d'AGRAIN : Tout ce qui est applicatif, étant entendu qu'il faudra protéger les trois couches : physique, logique et sémantique. Il semble que notre cybersécurité soit moins engagée sur la couche très physique.

_ Alain BOUILLÉ : On peut aussi s'interroger sur la cyberprotection en entreprise et les produits de sécurité qu'on achète. Ils sont majoritairement de provenance américaine et israélienne, parfois russe. Rarement de provenance européenne. C'est un problème.

Par rapport à la souveraineté des données, le chiffrement ne fait plus peur aux puissances étatiques. Pire, si on décide de tout chiffrer, Microsoft va vous expliquer gentiment que ses outils d'indexation et tous ses outils qui font la richesse de ses produits ne vont plus très bien fonctionner.

5.5.3 Protection des données personnelles et Privacy Shield : jusqu'où peut-on aller ?

_ Sabine MARCELIN, juriste en droit du numérique, membre de la réserve citoyenne de cyberdéfense : quelle est la place de la protection des données personnelles dans la souveraineté numérique ?

_ Henri d'AGRAIN : C'est un domaine qui évolue en France, en Europe, et dans leurs relations avec le reste du monde. Le nouveau règlement européen sur la protection des données personnelles s'appliquera à partir du 25 mai 2018[12]. Il permet de créer en Europe une législation unique pour chaque pays. Créé par les Cnil, ce référentiel unique vise un marché domestique pour l'ensemble des entreprises. Reste à savoir ce que donnera la transposition en droit français ?

Second point d'interrogation : les relations avec les États-Unis. Depuis le 1er août 2016, le Privacy Shield[13] a remplacé le Safe Harbor pour transférer des données personnelles vers les États-Unis. Les entreprises américaines doivent respecter les obligations et les garanties prévues par le Privacy Shield. Mais le 25 janvier 2017, l'administration Trump a signé un *executive order* dans le domaine de la lutte contre l'immigration illégale, qui peut remettre en cause l'applicabilité du Privacy Shield. Le G29, qui regroupe les Cnil européennes, a adressé un courrier à l'administration américaine. On attend encore la réponse. De quelle sécurité juridique pourront se prévaloir les données personnelles des ressortissants européens ?

---

[12] Règlement européen sur la protection des données : ce qui change pour les professionnels. Cnil, juin 2016. https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

[13] https://www.cnil.fr/fr/le-privacy-shield

_ Marc CHARRIERE : Je peux répondre au nom de la Commission Numérique de la Fieec[14] que je préside. Si notre continent va trop loin dans la protection des données, nous aurons un problème d'innovation par rapport à d'autres comme les Etats-Unis. Le marché intérieur étant très fort aux Etats-Unis, l'innovation numérique sera facilitée, et l'on va simplement utiliser ce qui aura été développé. L'innovation risque de se faire ailleurs, le savoir-faire risque de se faire ailleurs, et donc la protection technique des données risque d'être moins bonne.

5.5.4 Les réseaux dans les territoires

_ Michel LEBON, consultant en aménagement numérique territorial : la loi pour une République numérique[15] a fait l'objet d'une approbation consensuelle en octobre 2016. L'article 69, qui installe la notion de stratégie de développement des usages et services, appelle au recours à la médiation numérique dans les territoires. Cette médiation peut être un outil formidable d'acculturation par le bas des populations et de la société pour accompagner la transition numérique. Les collectivités doivent s'en saisir.

_ Marc CHARRIERE : À l'heure de la virtualisation des réseaux, nous aurons besoin de réseaux Ultra Haut Débit partout pour mettre en place les nouveaux services (e-santé, etc.). La fracture numérique ira au-delà du seul téléchargement.

5.5.5 Le cloud souverain face à l'intelligentsia numérique

_ Jacques MARCEAU : Sur les couches basses comme sur les couches plus hautes, la France est en perte de souveraineté. Je regrette que la belle idée de cloud computing souverain ait été descendue en flammes par de nombreux acteurs de l'écosystème du numérique en France qui se demandaient ce que l'État venait faire là. Cette idée a été reprise. Aujourd'hui il manque aux collectivités territoriales un support souverain pour stocker et traiter les données de nos citoyens.

5.5.6 Le travail de normalisation

_ Amal TALEB, directrice adjointe des affaires publiques chez SAP, membre du comité scientifique de l'Institut de la souveraineté numérique et du Conseil national du numérique : En matière de stratégie industrielle pour une cybersécurité, la question de la norme et du standard présente une véritable difficulté au niveau européen. La plupart de nos standards sont faibles au regard des standards américains dominants. Sur toutes ces couches que vous avez évoquées, quel est le bon degré de détermination de ce standard ou de cette norme technique qui nous permettrait enfin de créer une différence industrielle forte et de l'attractivité de nos standards au niveau mondial ? Cela vous paraît-il possible à mettre en œuvre ?

_ Henri d'AGRAIN : En France, travailler sur les normes et standards n'a jamais été une activité porteuse. C'est très dommage, et même assez catastrophique dans certains domaines. Aujourd'hui nous n'en sommes que les consommateurs. Sans négliger le travail qui est fait dans les entreprises françaises et dans certains ministères, notamment à la Défense, ce travail aujourd'hui n'est pas reconnu, il est peu visible, et il n'y a pas de mise en cohérence de l'ensemble des actions de normalisation et de standardisation en France et en Europe. Je crois que sans une véritable impulsion des États européens, il n'y aura pas de solution pour créer les structures et les conditions qui permettront une présence forte, renforcée, cohérente, de l'Europe.

C'est un vrai sujet de politique publique qui permettrait d'assurer une certaine forme de souveraineté, soit pour bien connaître les standards, soit pour faire en sorte que les standards ne soient pas eux-mêmes *backdoorés* au profit d'autres utilisateurs, et enfin, pourquoi pas pour imposer des standards auxquels nous pourrions tenir.

5.5.7 L'effort de formation

_ James GOLDBERG : Des formations sont-elles prévues pour accompagner la population dans tous les secteurs : éducation, santé, protection sociale, etc ?

---

[14] La Fédération des industries électriques, électroniques et de communication rassemble 22 syndicats professionnels.

[15] Loi du 7 octobre 2016 pour une République numérique. https://www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829&type=general&legislature=14

_ Henri d'AGRAIN : L'effort de formation à ces enjeux de transformation numérique et aux risques induits doit être porté sur les élites et les décideurs, chez qui le déficit est criant, notamment dans l'administration, la haute administration, le personnel politique, les directions de grandes entreprises, les administrateurs de société.

_ Alain BOUILLÉ : Au CESIN, on y travaille. Un tiers de notre action dans les entreprises vise à sensibiliser les utilisateurs au risque numérique, ainsi que les dirigeants pour qu'ils nous donnent davantage de moyens pour lutter contre la cybercrimininalité.

Tout le monde est concerné. Un utilisateur nous confiait récemment que la lecture *in extenso* des conditions générales d'utilisation d'un réseau social bien connu lui avait pris 9h00. On la signe instantanément. L'éducation nationale doit introduire cette problématique de sécurité, dès le plus jeune âge. Quand c'est gratuit, c'est vous le produit. Tout ce qu'ils vont poster va appartenir au réseau social.

Concernant les spécialistes en cybersécurité, ils sont très recherchés sur le marché de l'emploi. Il faut former des spécialistes, organiser la reconversion. La transformation numérique impacte les métiers dans l'informatique. Beaucoup de programmeurs devoir se convertir, pourquoi pas dans la sécurité ?

6. Table ronde 2 – **Quel enseignement supérieur et quelles formations au service d'une cybersécurité souveraine ?**

6.1 Introduction et modération

Cathie-Rosalie JOLY, avocat associé (Paris-Bruxelles), cabinet Bird & Bird, docteur en droit, chargée d'enseignement en cybersécurité (Montpellier I)

La formation et la sensibilisation sont des enjeux majeurs de cybersécurité en Europe. C'est d'autant plus compliqué dans un univers de plus en plus interconnecté, sans frontières, international, où il n'est plus possible de sécuriser un périmètre géographique donné.

Les technologies évoluent très vite. En 15 ans, on est passé des premières régulations informatiques à l'intelligence artificielle et au droit des robots. Comprendre ces technologies, leurs enjeux et les formations qu'il faut mettre en place, devient fondamental.

Au regard de l'accroissement des risques encourus et des opportunités fournies par toutes ces évolutions, un cadre réglementaire de plus en plus complexe trouve à s'appliquer : règlement européen sur la protection des données personnelles ; loi relative à la lutte contre le terrorisme ; loi de programmation militaire ; Directive européenne *Network and Information Security* (NIS) sur la cybersécurité, auxquels s'ajoutent des projets de réglementation en cours de résolution sur l'intelligence artificielle et le droit des robots.

J'ai eu la chance de bénéficier d'une petite formation technique et informatique qui était à l'époque un peu réservée à des juristes *geek*. On se rend compte aujourd'hui à quel point c'est vital d'avoir une vision transversale de la cybersécurité et de pouvoir tous se comprendre.

Quel sont les besoins en matière d'enseignement et de formation pour une cybersécurité souveraine ? Les domaines d'expertise nécessaires à un enseignement sont pluridisciplinaires, techniques, juridiques, et font appel à l'intelligence économique, la gestion des risques, la gestion de crise.

6.2 Quelle politique de puissance ?

Christian HARBULOT, directeur de l'Ecole de guerre économique [16]

6.2.1 La France n'a pas de politique de puissance

Plusieurs types d'enseignements sont nécessaires. Mais avant tout, il faut une grille de lecture. Au-delà des États-Unis et de la Chine, d'autres pays ont adopté une politique de puissance et de protection des données. À l'Ecole de guerre économique (EGE), nous discutons avec nos partenaires allemands de l'université militaire de Munich. Malgré la langue de bois, certaines subtilités sont intéressantes à capter. L'Allemagne a

[16] Auteur de « Manuel d'intelligence économique », PUF 2015 et « Fabricants d'intox : la guerre mondialisée des propagandes », Lemieux éd. 2016.

une démarche affichée, dans un cadre européen, beaucoup plus subtile que la France.

Certains pays ont une vraie politique de puissance, d'autres n'en ont pas. La France, malgré les efforts des militaires, de certains hauts fonctionnaires et du secteur privé, n'a pas de politique de puissance dans ce domaine.

6.2.2 La sensibilisation des élites

Chez nos élites administratives, politiques ou économiques, il y a un déficit de lecture sur les enjeux de conquête du monde immatériel. L'EGE mène actuellement un exercice de sensibilisation auprès de l'ensemble des candidats à l'élection présidentielle. Même si l'on trouve plusieurs approches qui ont déjà été évoquées – sur les différentes couches, des approches techniques ou liées aux données personnelles – aucun programme présidentiel ne propose une grille de lecture sur les enjeux de puissance.

Il y a quelques années, le conseiller du ministre de l'éducation nationale M. Peillon avouait à nos étudiants qu'il se sentait bien seul par rapport au monde administratif. Et du côté des entreprises, les RSSI de grandes entreprises m'avouaient lors d'un colloque qu'il avait fallu l'affaire Snowden pour que des comités exécutifs de grands groupes fassent machine arrière sur des décisions en matière de numérique. Loin d'une stratégie, ou même d'une prise en compte d'une finalité des enjeux du numérique dans l'activité de l'entreprise, ils avaient peur d'être ridicules !

L'EGE va lancer l'an prochain un MBA exécutif sur cette question. Il consistera à montrer les enjeux dans une logique transversale.

_ Cathie-Rosalie JOLY : En France, l'enseignement est-il adapté aux différents besoins des opérateurs d'importance vitale (OIV), du secteur public ou privé ?

6.3 Recherche : cap sur les entreprises

Francis JUTAND, directeur général adjoint de l'Institut Mines Télécoms, membre du conseil scientifique de l'Institut de la souveraineté numérique

Il faut prendre en compte la force du phénomène de métamorphose numérique. La transformation profonde de la société apporte des espaces de liberté et de progrès, et en même temps, une nouvelle jungle. Il s'agit d'apprendre et de trouver les règles dans cette jungle.

6.3.1 Les chaires Cybersécurité à l'Institut Mines Télécoms

La cybersécurité n'est pas un thème nouveau. En France, il existe des laboratoires de recherche puissants, dont certains sont en connexion avec le monde militaire et d'autres mondes. À l'Institut Mines Télécoms, 160 chercheurs travaillent au cœur de la cybersécurité.

Au fur et à mesure que le numérique se diffuse, la cybersécurité prend elle aussi un aspect « diffusant », qui constitue un problème. Nos chaires sur la cybersécurité portent actuellement sur :

- « Cybersécurité des infrastructures critiques »,
- « Cybersécurité et voiture connectée et autonome »,
- « Valeurs et politiques sur les informations personnelles ».

En France, nous avons un noyau solide, mais pas assez nombreux de chercheurs sur la cybersécurité.

6.3.2 Un nouvel enjeu : les plateformes de données industrielles

La sécurité en elle-même comprend deux dimensions : cybersécurité et sûreté.

Comment une usine numérisée va-t-elle résister à des attaques ou à des dysfonctionnements ? Des problèmes de résilience se posent, de vie privée…

Nous avons perdu la bataille sur les plateformes de données grand public. Mais aujourd'hui, un nouvel enjeu s'annonce sur les plateformes de données industrielles. Si l'on perd cette bataille-là aussi, on ouvrira des

portes béantes et simples d'accès à nos données.

6.3.3 Le manque d'attractivité des entreprises

En collaboration avec une grande entreprise franco-allemande dans le domaine de la sécurité, l'Institut Mines Télécoms a organisé des formations spécialisées pour attirer les étudiants vers cette entreprise. On n'a pas obtenu le succès escompté. Cela dénote un problème d'attractivité du secteur vis-à-vis des étudiants.

La sécurité est un secteur nouveau qui touche tous les secteurs d'activité. Il faut s'organiser pour fournir une approche à la fois systémique, technique, technologique, scientifique, d'usage. On sait le faire dans les écoles d'ingénieurs. L'enseignement se développe et il suit les évolutions. Les entreprises doivent également faire cet effort pour attirer vers ce domaine les chercheurs, les ingénieurs et les techniciens supérieurs.

Un travail d'analyse est à faire. Les acteurs se connaissent. Il existe déjà des actions structurantes dans la recherche. L'Agence Nationale de la Recherche propose des thématiques spécialisées. Des mesures assez urgentes doivent être prises pour aider la formation.

_ Cathie-Rosalie JOLY : Didier Renard, vous êtes VP Strategy d'Orange Cloud for Business après avoir été président de Cloudwatt. En tant que président de l'Institut de la souveraineté numérique, pensez-vous que la prise de conscience et les budgets soient suffisants pour aborder ce domaine dans toutes ses implications régaliennes : armée, police, justice, sphères publique et privée…?

6.4 La formation des élus

Didier RENARD, président de l'Institut de la souveraineté numérique

6.4.1 Un vivier d'emplois

On peut aussi s'interroger sur les métiers qui vont disparaître, ne serait-ce que pour bien orienter nos enfants. Faire le choix des métiers du numérique et de la cybersécurité est un bon choix. C'est également vrai en termes de reconversion pour beaucoup de gens aujourd'hui qui sont employés ou en recherche d'emploi.

La cybersécurité constitue un vivier d'emplois, et pourtant, il y a un vrai déficit entre l'offre et la demande de formation, en particulier sur les offres de formation professionnelle, de formation continue, les cours du soir, etc. C'est un gros marché à prendre.

6.4.2 Les axes de travail de l'Institut de la souveraineté numérique

L'Institut de la souveraineté numérique y travaille, sur plusieurs axes :

- **la formation des élus, des législateurs**, et tous ceux qui les conseillent, think tanks, philosophes et sociologues en cyberdéfense. Cette démarche doit être prospective. Avec la virtualisation des réseaux et le passage d'une logique de stock à une logique de flux, les flux de données vont circuler entre le cloud, le réseau, le device de type smartphone, voire l'humain. Elon Musk vient d'annoncer la création de Neuralink, une start-up dont l'objectif est de connecter le cerveau humain à une puissance de calcul artificielle.

- **la révision du cadre juridique.** Avec le vol, la destruction ou l'altération de la donnée, on quitte le terrain mercantile pour un actif plus essentiel qu'est la pensée ou un réseau de voitures autonomes. Ces cas de figures dans un futur très proche vont changer totalement la donne en termes de gravité.

- **les normes :** la maîtrise des normes et des standards est une arme au niveau français et européen. Malheureusement, cette arme est aujourd'hui entre les mains quasi exclusives des États-Unis. Toutes les associations, consortium de gestion de l'internet et des réseaux mondiaux sont de droit américain.

6.5 L'écosystème du Technion

Muriel TOUATY, directrice générale, Technion France

Israël est un petit pays qui depuis sa création il y a 70 ans est confronté à la diversité par la résilience et donc à l'insécurité. La guerre, le terrorisme, le cyberterrorisme... toutes ces données sont extrêmement ancrées dans la conscience collective. Il y a urgence à former des étudiants et des chercheurs, et ce depuis le lycée. L'éducation nationale a la responsabilité de former nos étudiants. Ils seront les garants de l'avenir et de la cybersécurité, contre les attaques auxquelles nous sommes confrontés à l'échelle mondiale.

6.5.1 Le financement de la cybersécurité

Le Technion en sa qualité de première école d'ingénieurs d'Israël est au fondement même de la *Start-up Nation* qui est liée intrinsèquement à l'armée et à l'industrie israélienne, avec la bénédiction du gouvernement israélien pour qui c'est une priorité d'allouer des fonds dans ce domaine.

Le centre de cybersécurité au Technion reçoit des fonds à hauteur de 125 millions de $:

- du bureau national de la cybersécurité en Israël,
- des fondations privées,
- du programme de soutien européen H2020,
- des revenus générés par les start-up, au Technion et en Israël.

6.5.2 Un enseignement pluridisciplinaire

Dès la première année, les étudiants sont propulsés dans ces problématiques de cybersécurité de façon très transverse, pluridisciplinaire, en associant la faculté électronique et la faculté de sciences informatiques (15ème position dans le ranking mondial du classement de Shanghai).

Le facteur humain est pris en compte dans cette formation. Au travers de workshops, les étudiants sont mis en situations de guerre et d'attaques terroristes. Ils les connaissent par cœur parce qu'ils ont fait l'armée : 2 ans obligatoires pour les jeunes filles, 3 ans pour les garçons.

Des projets sont menés sur ces sujets-là avec des étudiants étrangers et des équipes de sciences sociales et de sciences humaines. Cette pluridisciplinarité vise notamment à les sortir d'eux-mêmes, pour qu'ils apprennent à se mettre dans la tête de l'adversaire et mieux anticiper les attaques.

6.5.3 *Start-up Nation*

Le Technion est aussi un vivier de croissance pour le pays. Même si tous les chercheurs ne sont pas voués à devenir des entrepreneurs, l'ADN du Technion est de valoriser sa recherche pour faire du transfert technologique et créer du bien, de la valeur ajoutée par ses start-up.

- **Sur 5 000 start-up en Israël, 1 500 ont été créées en 2016, dont 65 dans le domaine de la cybersécurité qui a levé plus d'un demi-milliard de dollars.**
- **Israël a 15% du marché mondial de la cybersécurité.**

Autres sources de financement : **les brevets, les royalties des start-up développées par le Technion et les exit.** Waze / Google par exemple, ou Mobileye dans le domaine de la voiture connectée qui vient de faire un exit avec Intel pour 15 milliards de $.

Dans une économie qui circule, c'est de l'argent qui sort et qui rentre de nouveau dans le pays pour être réinvesti dans l'innovation, la création de valeur ajoutée pour les start-up, et donc dans la cybersécurité.

_ Cathie-Rosalie JOLY : Didier Renard, pour essayer d'anticiper le futur et comprendre les mécanismes du succès de la Silicon Valley, vous n'avez jamais cessé d'étudier dans votre parcours professionnel. D'abord en 2010 à Moffett Field au sein de la Singularity University, puis à Palo Alto en 2011 au Technology Venture Program de Stanford. Comment est financé Stanford ?

6.6 L'écosystème de l'université Stanford

Didier RENARD

6.6.1 Un modèle économique guidé par le marché

D'un point de vue socioculturel, le modèle économique de Stanford est avant tout guidé par le marché, y compris en matière d'éducation.

> • **l'université Stanford est une entreprise privée dont le chiffre d'affaires s'élève à 5 milliards $** (auxquels s'ajoutent, dans un cadre plus large, 4 milliards de $ issus de son activité de santé. Stanford délivre du service de santé en vendant du médecin à la journée.)
>
> • **les frais étudiants ne représentent que 11% du chiffre d'affaires.** Plus de la moitié des étudiants à Stanford ont une bourse partielle ou totale. Si la famille de l'étudiant gagne moins de 65 000 $ de revenu annuel, il est exempté de frais de scolarité et d'hébergement.
>
> • **plus du quart du financement provient de l'État fédéral,** sous la forme de programmes de recherche précis (non pas sous la forme de dotation). L'Etat est client (il n'est pas financeur du système éducatif). Ces programmes viennent du ministère de l'éducation, du département de la Défense et des agences fédérales.
>
> • **plus du quart du financement provient des commandes privées par les entreprises voisines de Stanford.** Cet écosystème se compose du milieu universitaire, des entreprises, start-up ou grandes entreprises dirigées par d'anciens élèves, et du capital risque.

6.6.2 Une conception libérale du métier d'enseignant-chercheur

Au sein d'une même promotion, on retrouve ainsi des enseignants-chercheurs, des capital-risqueurs et des entrepreneurs.

Le métier d'enseignant-chercheur à l'université n'est pas un renoncement en matière de salaire. Contrairement à la France, cette activité n'est pas incompatible avec celle de consultant. C'est même l'inverse. Dans le domaine de la cybersécurité par exemple, un secteur très dynamique, avec des cycles courts et des innovations permanentes, les enseignants-chercheurs qui sont au contact quotidien avec la réalité du terrain constituent une vraie valeur ajoutée.

Ce qui est vrai du modèle économique de Stanford l'est aussi pour les 8 autres universités de l'Ivy League (Harvard, Yale, Princeton, etc.).

6.7 Réactions

_ Cathie-Rosalie JOLY : On le voit, le financement de la formation dans la cybersécurité nécessite des investissements mais aussi de lutter contre la fuite des cerveaux.

6.7.1 Créer des task force

Christian HARBULOT

Les recettes du Technion ou de l'université Stanford nous tendent les bras. Hélas, compte tenu du système français, ce sera très difficile de les appliquer chez nous. On n'a pas cette chance d'avoir des gens sensibilisés par le service militaire comme c'est le cas dans l'Etat hébreu, ni d'avoir cette transversalité des élites comme à Stanford, qui a parfaitement compris le lien entre le marché, la sécurité et la géopolitique.

Nous sommes condamnés à essayer de construire à côté de ce qui ne bouge pas !

- Pour trouver ce lien entre le marché, la sécurité et la géopolitique, il va falloir constituer des task force, apprendre à se parler dans le monde de la formation. En particulier entre les ingénieurs et les sciences sociales, il y a un lien très important à créer.

- Des industriels vont devoir montrer l'exemple. Par rapport aux enjeux, les chaires sont insuffisantes en

termes financiers. Il faudra trouver des solutions originales. Pour l'instant, l'Etat ne me semble pas capable d'impulser un élan (à cause de son fonctionnement et de l'état de ses finances). En revanche, il peut l'appuyer.

Une nouvelle flexibilité reste à inventer entre nous. Aujourd'hui cette voie ne peut venir que sur la base du volontariat.

6.7.2 Resserrer les liens entre les entreprises et le milieu académique

Francis JUTAND

6.7.2.1 Optimiser le Crédit d'Impôt Recherche

Effectivement, notre système de financement de la formation dans l'enseignement supérieur est assez différent. Beaucoup d'anciens chercheurs sont financés à temps plein, ce qui a des avantages et des inconvénients. Le système français n'est pas orienté vers le don. Aux États-Unis, les entreprises et les personnes bénéficient de conditions de dons vers l'enseignement supérieur tout à fait exceptionnelles et méconnues en France. Quant aux budgets de l'enseignement supérieur, ils ne vont pas augmenter. Donc il faut trouver d'autres solutions.

Les chaires : est-ce suffisant pour passer à l'échelle ? Les chaires représentent 2 à 3 millions d'euros qui viennent en soutien à la recherche et à la formation.

Beaucoup d'efforts sont faits entre les entreprises et le milieu académique. Il faut regarder les manques et les outils à utiliser.

On peut optimiser le Crédit d'Impôt Recherche :

- en créant un **Crédit d'Impôt Recherche Cybersécurité** pour inciter les entreprises à aller dans ce domaine. Lorsqu'une entreprise a atteint le plafond de dépense de recherche en Crédit d'impôt Recherche, elle bénéficie d'un Crédit d'impôt Recherche supplémentaire spécialisé dans la cybersécurité[17].

- en réfléchissant à un **Crédit d'impôt Formation et Recherche,** puisque l'effort de formation est très important.

6.7.2.2 Rassembler toutes les parties prenantes

Ces outils doivent s'accompagner de conditions attractives et dynamiques autour de projets et de programmes de réflexion qui réunissent l'Etat, l'enseignement supérieur et les entreprises – si possible sans créer de nouvelles structures –, autour d'un Institut par exemple. Ce serait probablement plus efficace que la sensibilisation nécessaire des décideurs.

On ne fait pas assez de prospective en France, parce que l'on a peur des résultats. Une telle initiative nous obligerait à regarder en face les vérités, élaborer des scénarios et prendre des positions. Tout l'écosystème se développera.

6.7.2.3 Faire l'effort d'une économie puissante

Les grandes entreprises qui travaillent dans ce domaine sont connues en France. Des start-up se créent. D'autres sont plus ou moins discrètes. Mais cela ne suffit pas. Nous sommes trop sur la défensive. La souveraineté ne peut marcher que si l'on fait cet effort de puissance, et donc un développement économique à la hauteur. D'autre pays dans le monde souhaitent éviter d'avoir à choisir entre les États-Unis ou la Chine. On doit être capable de leur apporter des solutions. Ce n'est qu'au prix d'une économie puissante que l'osmose Enseignement supérieur - Recherche - Entreprises pourra fonctionner.

6.7.3 Mise en garde

Philippe DEWOST, directeur adjoint, Mission Programme d'Investissements d'Avenir, Caisse des Dépôts et Président d'Honneur du CHECy (Centre des Hautes Etudes du Cyberespace)

[17] Le taux du crédit d'impôt recherche est de 30 % pour les dépenses de recherche jusqu'à 100 millions d'euros (ou 50 % dans les départements d'outre-mer), 5 % au-delà.

6.7.3.1 Sur le Crédit d'Impôt Recherche : il faut être attentifs au rapport qualité-prix exceptionnel de nos ingénieurs R&D, que le CIR ne fait qu'amplifier. C'est sans doute une des raisons qui attirent les géants étrangers lorsqu'ils implantent, acueillis à bras ouverts par les pouvoirs publics, des centres de R&D dans notre pays. Ces dispositifs, qui (ne) créent (que) quelques centaines d'emplois, sont sans doute un outil de détection de hauts potentiel très efficace qui leur permet de détecter in situ les meilleurs. Les propositions qu'ils font ensuite à ces ingénieurs R&D pour les accueillir à l'étranger sont de celles qui ne se refusent pas, non seulement en termes financiers, mais aussi parce qu'ils promettent à ces chercheurs deux choses essentielles pour eux : pouvoir s'entourer de la dizaine de pointures dont ils ont besoin, et définir leur agenda de recherche, et ce en toute liberté.

6.7.3.2 Sur le danger de l'exit : c'est formidable d'investir autant dans nos start-up. Je suis engagé dans environ 2,5 milliards d'euros d'investissement à travers les différents fonds qui ont été déployés dans le cadre du Programme d'Investissements d'Avenir. Ceux-ci couvrent toute la chaîne de financement, de l'amorçage au capital développement ;a vraie question demeure cependant celle de l'exit. Si nous n'avons pas en effet, d'ici 2 à 3 ans, de marché de cotation, ni de mobilisation de nos grands groupes pour l'acquisition (à des valorisations correctes) et l'intégration de ces start-ups, une part importante de l'argent public qui aura été injecté aux côtés des investisseurs privés dans ces dispositifs depuis 2011 permettra alors à des groupes non européens de faire des achats de technologies et de compétences très développées à très bon prix.

6.8 Comment empêcher la fuite des cerveaux ?

_ Cathie-Rosalie JOLY : Comment a-t-on valorisé la filière cyber en Israël pour attirer les talents et les retenir ?

6.8.1 Retour d'expérience du Technion

Muriel TOUATY, directrice générale, Technion France

6.8.1.1 La culture de l'innovation

L'écosystème coule de source en Israël. Tout est question de culture. En Israël, rien n'est acquis. Ce pays a été façonné par l'adversité. Tout son écosystème en découle. On est obligé, parfois malgré soi, d'être dans cette dynamique, cet élan vital de formation et de création. Dans un contexte géopolitique complexe, la notion de patriotisme est très importante au regard de l'armée. Israël n'a ni père ni mère. Nous sommes un collectif, une patrie qui œuvre dans le même sens pour garantir la pérennité du pays, y compris au plan économique. Il n'y a pas de ressources naturelles. Par contre, nous avons des cerveaux.

- Le gouvernement israélien alloue 4,8% de ses dépenses en R&D en part du PIB.
- En France, la part du PIB consacré à la recherche et développement est de 2,24%. [18]

6.8.1.2 L'interdisciplinarité a un rôle moteur

Les universités israéliennes sont toutes excellentes, et quoique très différentes, elles se parlent entre elles. La notion d'interdisciplinarité est majeure, notamment dans les formations de cybersécurité qui sont associées aux sciences cognitives et aux sciences humaines et sociales. On se frotte à des cultures d'innovation, des raisonnements différents.

6.8.1.3 Industrie et Académie sont profondément liées

Israël construit, façonne, invente un terrain propice à l'innovation par la création de la valeur, les incubateurs et les écosystèmes entrepreneuriaux dont disposent toutes les universités israéliennes, en particulier Technion, première école d'ingénieurs.

Les start-up créent des technologies disruptives qui répondent aux besoins du marché industriel. Le chercheur ne reste pas cloisonné dans son laboratoire à faire de la recherche fondamentale. Il raisonne pour

[18] Source : MENESR, décembre 2015. http://www.enseignementsup-recherche.gouv.fr/pid25351/chiffres-cles-de-la-recherche.html

répondre aux besoins du marché, non pas pour gagner de l'argent, mais pour générer de la croissance qui sera réinvestie dans d'autres innovations au sein même du pays.

Les fonds de dotation, les bourses, les chaires, permettent aussi à nos étudiants israéliens de partir à l'extérieur, ce qui leur donne encore plus envie de revenir en Israël, où ils pourront évoluer dans un terrain propice qui répond à leur desiderata d'entrepreneuriat, d'innovation, de création de valeur.

6.8.1.4 La prise de risque

De quoi a-t-on peur dans la création et la formation quand on vise l'excellence ?

L'audace est dans notre culture. Si on tombe, ce n'est pas grave. On analyse pourquoi on a échoué, on se relèvera et on fera. C'est la symbolique de la névrose collective. On se lève le matin, mais on ne sait pas si on va se coucher le soir.

Dans cet espace-temps, on doit viser l'excellence. On est absolument obligé de créer, sans doute aussi pour légitimer sa condition et son être.

_ Cathie-Rosalie JOLY : l'accueil des étrangers, le mélange des origines et des cultures sont-ils un risque ou une opportunité pour la formation cyber en France ? Comment empêcher la fuite des cerveaux ?

_ Francis JUTAND : C'est évidemment une opportunité, même s'il faut prendre quelques précautions.

6.8.2 La diversité des cultures est une opportunité

Francis JUTAND

Les États-Unis attirent, le *brain drain* est efficace. Il faut former, se brasser.

En France, on se demande toujours pourquoi on utilise l'argent de l'État pour former des étudiants étrangers. Soit on est dans un repli, soit on est dans une dynamique.

- nos entreprises ont besoin de travailler à l'international. De plus en plus nos étudiants ont besoin de deux formations, deux cultures, des doubles diplômes.

- ces étudiants restent beaucoup plus en France qu'on ne le prétend. Des études ont montré que beaucoup d'étudiants chinois restaient en France.

- cela dépend de l'attractivité. Il ne faut surtout pas se fermer dans la formation. Il faut attirer les meilleurs, les former, armer nos entreprises qui vont travailler à l'international. Elles ont besoin de s'appuyer sur des étudiants français et étrangers qui sont formés.

- nous avons environ 36% d'étudiants étrangers dans nos écoles. Les entreprises sont très contentes de les trouver quand elles se développent.

Par contre, au niveau des doctorants, plus de 55% sont étrangers. Le financement des doctorants en France est tel que nos ingénieurs ont tendance à partir directement en entreprise. Je fais confiance à nos services pour avoir une vision dynamique. Un pays n'est jamais figé. Un pays considéré comme un ennemi aujourd'hui peut être amené à évoluer. C'est pourquoi il faut avoir une approche ouverte. De toute façon, on n'empêchera jamais les gens de circuler. Autant attirer les bons chez nous que de les laisser aller se former ailleurs.

_ Didier RENARD : Quand j'ai voulu embaucher un alternant en master 2 de nationalité camerounaise, on lui a refusé son visa de travail. Et pourtant, on l'avait formé à nos frais !

6.9 Discussion avec la salle

6.9.1 Cyberdéfense passive : de la primaire aux formations bac +2

_ Cathie-Rosalie JOLY : Si de grands chantiers sont nécessaires pour revaloriser les formations cyber, il faut également mettre en place une cyberdéfense passive, en apprenant aux jeunes à avoir les bons réflexes cyberdéfense, puisqu'ils naissent avec des outils connectés. La cybersécurité dépasse le cadre de

la formation des experts. Elle nous concerne tous, dès le plus jeune âge.

_ Didier RENARD : L'Institut de la souveraineté numérique travaille sur un programme de formation des élus des collectivités territoriales qui vise à les former à former, aussi bien les enfants que l'ensemble des citoyens, aux réflexes de la sécurité informatique. Cela commence par des gestes simples.

D'autre part, la cybersécurité a besoin de BTS. Au niveau européen, la normalisation LMD (licence, master, doctorat) a dévalorisé les bac +2, en particulier les BTS. À l'intérieur d'un centre de sécurité opérationnelle, en particulier sur l'*ethical hacking*, on a besoin de ces diplômes. Aujourd'hui il y en a très peu.

L'école spéciale militaire de Saint-Cyr ouvre un BTS en cyberdéfense à la rentrée prochaine, et l'ANSSI a développé un référentiel de labellisation des formations initiales en cybersécurité de l'enseignement supérieur « SecNumedu », qui commence à la licence. Je pense qu'il devrait s'élargir au bac +2.

6.9.2 100 000 postes à pourvoir

_ Un représentant de l'ISEP (Institut supérieur d'électronique de Paris) : au Forum international de la cybersécurité, l'ANSSI a labellisé 26 formations à partir de la licence. Notre école d'ingénieurs va lancer cette année un master spécialisé Architecture cybersécurité et intégration labellisé par l'ANSSI.

Le rôle de l'ANSSI est important pour regrouper les différents secteurs. On a peu parlé de l'employabilité. 100 000 postes seraient à pourvoir aujourd'hui en France, dont 24 000 sur la partie Syntec numérique qui couvre les entreprises ESN (entreprises de services du numérique ex-SSII), auxquelles s'ajoutent la banque-assurance, les industriels et les institutionnels. La capacité d'enseignement et de formation est de 1 500 postes par an. Il faut nous aider à former de futurs experts en cybersécurité.

La Commission nationale de la certification professionnelle (CNCP) peut délivrer des pass pour permettre à des OPCA, FONGECIF et organismes paritaires de prendre en charge une partie de ces formations.

6.9.3 Les valeurs de loyauté

_ Christian HARBULOT : Les professeurs jouent un rôle essentiel dans l'éducation nationale. Des efforts de sensibilisation sont faits dans la protection antiterroriste. Mais on ne sait pas définir un plan stratégique pour que l'éducation nationale, au collège et au lycée, aborde ces questions de cybersécurité. En France, c'est difficile d'atteindre le corps enseignant sur cette question. Il y a un problème de culture générale, un manque de vision globale qui se limite à la navigation sur internet.

_ Francis JUTAND : On a besoin de l'éducation civique régalienne à l'école, mais ce n'est pas un canal prioritaire. Les jeunes savent discuter, échanger, partager sur les réseaux sociaux pour peu qu'ils aient accès à de bonnes informations.

L'esprit du renoncement est plus à craindre, celui qui consiste à penser qu'après Snowden, de toute façon, on est écouté et observé. Ce point de vue est dangereux. Il faut travailler sur les valeurs, en particulier sur la loyauté. Plutôt que de livrer 50 pages de conditions générales d'utilisation incompréhensibles, s'engager à dire ce que l'on fait des données et faire ce que l'on dit. C'est beaucoup plus impactant.

On pourrait réfléchir à une Convention de Genève autorisant l'accès aux données pour des raisons de sécurité, mais pas pour de la veille économique.

_ Cathie-Rosalie JOLY : Des réglementations existent déjà. La convention de La Haye, des lois anti-discovery assez anciennes, méconnues dans les entreprises, permettent de lutter contre le « fishing expedition » d'informations et contre l'intelligence économique. Il reste à les parfaire.

6.9.4 La formation en ligne

_ Luc RUBIELLO, fondateur d'innooo : Innooo est un moteur de recherche et réseau social français, une initiative volontaire de la société civile destinée à créer une alternative à Google. Notre ambition est de créer un wikipedia français. Nous avons lancé une pétition pour la souveraineté internet de la France qui a recueilli 20 000 signatures (Pacte numérique pour l'Indépendance et la Sécurité Internet de la France). Quid des formations en ligne pour s'informer, se former ?

_ Francis JUTAND : Le contenu numérique est déjà utilisé dans le cadre de la formation continue pour les

entreprises. Nous réfléchissons à la création de MOOC totalement ouverts pour faire ce travail de sensibilisation au niveau des politiques de sécurité. L'un des écueils est le caractère évolutif du contenu. Chaque jour la sécurité déplie de nouveaux impacts.

6.9.5 La fuite des cerveaux

_ Gérald DELPLACE, vice-président de Fortinet : Comment retenir nos talents ? Pourquoi nos talents s'en vont-ils ? À cause du marché. Au bout du compte, ce qui leur importe, c'est ce qu'ils ont dans leur portefeuille à la fin du mois. 90% des outils utilisés aujourd'hui dans les entreprises pour faire de la sécurité sont américains ou israéliens. Comment changer cette donne ? Cela commence à l'école.

_ Francis JUTAND : Non, l'appât du gain n'est pas le seul moteur de nos cerveaux brillants. Dans les services de défense, les gens qui travaillent pour leur pays ne sont pas payés au même niveau que les entreprises américaines. Les valeurs sont fondamentales. On l'a vu avec l'exemple israélien.

Si la centaine de start-up créées par l'Institut Mines Télécoms n'arrive pas à croître, c'est pour des raisons culturelles. Il faut que les gens circulent et reviennent pour créer des environnements propices à la création d'entreprises en France.

La France est la 5ème ou 6ème force dans le monde. Nous sommes puissants dans certains secteurs. On essaie de combler notre retard dans le numérique de deux manières : par la création de start-up, et par association et hybridation avec de grandes entreprises françaises qui savent créer des choses. Ce qu'il nous manque, c'est une prise de conscience réelle des menaces et des enjeux économiques. Ce n'est pas en décidant de créer un Google français qu'on y arrivera, mais plutôt en misant sur nos forces économiques !

_ Didier RENARD : Quel projet de vie veut-on donner à nos enfants ? C'est la première fois depuis des siècles que nous disons à nos enfants que leur niveau de vie sera inférieur au nôtre. Quels doivent être nos combats technologiques ? Il ne faut pas se tromper de débat, avoir les ordres de grandeur à l'esprit. Tout à l'heure, Henri d'Agrain a dit qu'une industrie du microprocesseur coûtait 150 milliards. La France n'y est pas. C'est comme ça, on ne peut pas se l'offrir, il faut l'oublier.

En revanche, il y a d'autres combats à mener. Par exemple :

- sur les moteurs de recherche : en France, Google a un taux de pénétration de 97%. A l'instar de nombreux petits pays, des initiatives permettraient à d'autres moteurs de recherche de réduire ce taux de pénétration unique au monde.

- sur l'algorithmie et l'intelligence artificielle : la France a l'une des meilleures écoles de mathématiques au monde. Nous devrions être les champions du monde de l'algorithmie et de l'intelligence artificielle. Ce n'est pas le cas.

6.9.6 Cybermanipulation

_ Tariq KRIM, vice-président du Conseil national du numérique : La Cybermanipulation n'est pas que technologique. C'est aussi la PsyOps *(Psychological Operations*). L'ENA ou Sciences Po réfléchissent-elles à des formations sur ces nouvelles formes de menaces pour les personnels politiques actuels et futurs ?

_ Christian HARBULOT : C'est justement l'objet de la formation que l'EGE va lancer. Nous travaillons depuis 20 ans sur les questions d'affrontement informationnel. Nous voulons mailler le contenant et le contenu en favorisant la transversalité disciplinaire. Notre objectif est d'aller sur ces enjeux-là. Les ordres de grandeur sont très démonstratifs, dans le cadre politique, mais également dans le monde de l'entreprise.

_ Jacques MARCEAU : On assiste en effet à une nouvelle source de déstabilisation des entreprises et des États, jusque dans les processus électoraux. Se repose de nouveau les antagonismes entre Américains, Russes… et Chinois. Julien Nocetti va nous en parler.

7. La géopolitique de l'internet et ses impacts sur la cybersécurité des entreprises

Julien NOCETTI, chercheur à l'Institut français des relations internationales (Ifri)

Les événements de 2016 ont replacé les problématiques numériques et cyber sur la scène politique internationale. Les soupçons d'ingérence russe dans les élections américaines, piratages massifs (Dyn,

Yahoo…) et plus globalement la course au cyberarmement, traduisent une politique internationale très volatile, profondément bouleversée par la dissémination globale de ces moyens numériques et cyber.

Au-delà de la « cyberguerre », un terme quelque peu galvaudé ces dernières années, quelle est la réalité et quels sont les enjeux ? La transition numérique et cyber a de multiples impacts sur les politiques étrangères.

7.1 Stratégie

Au plan stratégique, la transition numérique se traduit par une rivalité entre puissances, en particulier entre Chinois et Américains, et par l'apparition de nombreux acteurs non institutionnels qui peuvent parfois disposer d'une influence globale.

Depuis le premier mandat de Barak Obama, l'industrie numérique américaine est devenue à la fois la priorité du redéploiement économique centré autour de ces acteurs de l'industrie du Net et la priorité de la stratégie de sécurité américaine. Comme Ben Laden avant lui, Snowden a contribué à refaçonner l'appareil de sécurité des États-Unis autour d'une surveillance électronique planétaire par la NSA et de cyberopérations qui se substituent à des interventions extérieures beaucoup plus coûteuses et risquées.

Du point de vue américain, Internet participe de la stratégie d'endiguement de la Chine, d'isolement de la Russie, grâce au contrôle des réseaux, à la définition des normes et standards internationaux, aux mesures protectionnistes, en particulier contre les équipements chinois, et à la captation des données.

La gouvernance d'internet permet aux États-Unis de conserver une influence juridique sans précédent via la prééminence du droit souple (*Soft Law*) et de la langue anglaise. Contrairement à l'Europe, ces débats sur la gouvernance d'internet sont suivis au plus haut niveau à Washington, avec un très fort intérêt du Congrès.

Ce statu quo savamment entretenu permet aux Américains d'éviter toute régulation autre que technique de ce bien commun qu'est l'internet. Plus globalement, les GAFA engendrent une nouvelle forme de puissance, de pouvoir, dont il est parfois délicat de percevoir tous les contours et implications.

Début mars 2017, la valorisation cumulée des GAFA égalisait presque le PIB de la France en 2016.

7.2 Economie

Au plan économique, le passage d'une économie de consommation de masse à une économie de la consommation personnalisée fait que certains pays, comme la France, souffrent d'un déclassement économique qui affaiblit leur puissance globale.

La domination de l'économie numérique par les États-Unis et la Chine placent la souveraineté numérique et la maîtrise des données au cœur de l'autonomie stratégique des États.

Ceci sera encore plus vrai avec la convergence prochaine de l'économie des données, de la robotique, de l'intelligence artificielle et de la connectivité des objets. Cette « 4ème révolution » (dixit le Forum de Davos 2016) bouleverse non seulement la vie des sociétés, la production, mais il aura des conséquences profondes sur le système international, les rapports entre États et acteurs privés.

7.3 Diplomatie

Au plan diplomatique, le numérique accélère la diffusion de la puissance à l'ensemble des acteurs sociaux. Autrefois sacralisée, la diplomatie est aujourd'hui diluée dans une forme de *gouvernance globale*, de régulations transnationales qui se multiplient, et dont les acteurs nationaux, les États, sont parfois écartés ou marginalisés.

Un grand nombre de normes internationales et standards, dans des domaines très variés (finance, santé, alimentation, internet, etc.), sont mis en place sans passer par les canaux traditionnels de la diplomatie et des rapports inter-étatiques.

7.4 Trump

L'arrivée de Trump à la Maison Blanche fait peser des incertitudes. Si je caricature mon propos, pour Obama, il était plus important de parler aux GAFA qu'à Poutine, alors que pour Trump, il semble pour l'instant que ce soit différent.

Plus sérieusement, une inconnue majeure réside dans les décisions de Trump en matière de cybersécurité. Elles auront un impact substantiel à la fois sur la position des États-Unis et ses conséquences pour l'Europe et pour les entreprises européennes. Le candidat Trump s'était contenté de préconiser un accroissement des capacités cyberoffensives et de réformer toute l'architecture de cyberdéfense en interne, sans qu'il y ait eu de réflexion profonde de sa part sur ces thématiques.

Or depuis deux ans, les États-Unis sont confrontés à nombre croissant de cyberattaques et de cybermenaces. Il est fortement probable que Trump doive prendre des décisions d'importance vitale pour mieux protéger l'infrastructure américaine, et répliquer. Cela aura des conséquences sur nos propres politiques et sur notre sentiment de vulnérabilité.

Trump a été très critique envers la Chine pendant sa campagne électorale. Il sera inévitablement testé par Pékin en matière de cyberespionnage.

Le possible renforcement des mesures protectionnistes de la part de Washington contre les équipements chinois pourra peser dans les tensions entre les deux pays.

Sur le front européen, les membres de l'OTAN auront besoin d'être rassurés sur l'engagement des États-Unis en matière de dissuasion cyber face à la Russie qui est perçue comme agressive au double plan cyber et informationnel.

À très court terme, Trump risque de fédérer contre lui les deux courants majeurs de la puissance cyber et numérique américaine : la Silicon Valley qui fustige ce produit de la téléréalité, et le complexe militaro-numérique qui s'inquiète profondément de sa vulnérabilité.

7.5 La Russie

À l'évidence, le contexte géopolitique pèse, parfois lourdement, dans cette cyberconflictualité que nous connaissons actuellement.

La Russie conteste l'Occident sur les affaires du monde. Le numérique lui permet de déployer des opérations d'influence et de désinformation à une échelle inédite.

D'autre part, la Russie joue sur l'asymétrie pour transformer ses faiblesses en atouts. Piratages, fuites d'informations, *fake news*, sont perçus à Moscou comme étant complémentaires du déploiement de moyens conventionnels comme des bombardiers stratégiques, la défense anti-missiles et autres atouts traditionnels.

En matière de cyberguerre, il ne faut pas faire l'erreur de porter notre analyse sur les seules actions du Kremlin. Leurs capacités reposent sur une grande porosité entre les services de l'État et le secteur privé. Cette horizontalité peut être très dynamique.

7.6 La Chine

La Chine s'oppose directement à Washington pour la maîtrise de l'internet. Elle défend ardemment son marché tout en projetant ses champions. Ses capacités de cyberespionnage sont quasi industrialisées, tout en testant l'architecture de l'internet.

Pour rappel, déjà en 2010, la Chine avait fait la preuve de ses capacités en détournant temporairement, via China Telecom, environ 15% du trafic internet mondial. Le trafic internet mondial a été coupé pendant une vingtaine de minutes pour le faire passer à travers ses multiples mouchards. A l'heure actuelle, ce test de l'architecture internet est pratiqué de manière régulière par Pékin.

7.7 Les infrastructures vitales dans la ligne de mire

Cette cyberconflictualité cible de plus en plus les infrastructures vitales. Ces dernières années, les cyberattaques se sont multipliées dans le secteur de l'énergie.

En 2012, le piratage des systèmes informatiques de la compagnie pétrolière Saudi Aramco dans le Golfe avait été imputé à l'Iran dans un contexte de très forte tension avec l'Arabie Saoudite.

Au printemps 2014, le réseau ukrainien a été mis hors service après l'entrée des Russes.

Il y avait eu un précédent en 2010 avec Stuxnet, ce ver informatique qui avait permis à la coopération américano-israélienne de mettre hors service les centrales nucléaires mises en place par Téhéran.

Les télécommunications en sont pour leurs frais : TV5 Monde en 2015, ou l'attaque contre Dyn en octobre 2016 qui a touché plusieurs plateformes, réseaux et médias américains (CNN, New York Times, Financial Times, Guardian).

7.8 Les entreprises face au fossé générationnel et à l'explosion des données

La cybermenace se situe aux confins de cette guerre politique, de l'espionnage économique et du crime organisé. Certains États n'hésitent pas à mobiliser de larges capacités offensives à des fins de déstabilisation et de destruction, en s'abritant derrière l'incertitude de l'attribution. C'est devenu aujourd'hui un outil éminemment politique, qui fait évoluer les pratiques diplomatiques.

Cette menace diffuse et très complexe représente un défi colossal pour les entreprises. Pour faire évoluer leur approche de la sécurité, elles devront prendre en compte deux paramètres :

- Le fossé générationnel : ceux qui sont aux commandes doivent surmonter leur peur du cyber. Un gros effort d'éducation est à fournir auprès des élites et des décideurs du pays.

- L'explosion des données. Le problème est centré sur les données et non plus sur les systèmes d'information, un défi accentué par l'explosion de l'internet des objets, 20 à 50 milliards d'objets connectés à l'horizon 2020.

_ Jacques MARCEAU : Cette vision du cyberespace international pose la question d'une politique publique de cybersécurité. J'ai rappelé cette initiative publique dans le domaine du cloud qui avait été fustigée par l'intelligentsia numérique. Quelles seraient les bases d'une politique publique de cybersécurité ? Quelles interactions entre cybersécurité des Etats et cybersécurité des entreprises ? Faut-il définir de nouveaux opérateurs et industriels d'importance vitale, voire élargir à la notion de donnée vitale ? Comment l'Etat peut-il contribuer à assurer leur cybersécurité ? La France et l'Europe peuvent-elles encore imposer leurs choix ? La commande publique peut-elle être un levier ? Faudra-t-il imposer des normes de cybersécurité aux entreprises par la loi ?

8. Table ronde 3 – **Vers une politique publique de cybersécurité ?**

Modération : Thibault VERBIEST, avocat associé, De Gaulle Fleurance & Associés

8.1 L'espace européen d'une souveraineté numérique

Bernard BENHAMOU, secrétaire général de l'Institut de la souveraineté numérique

8.1.1 La fin de l'innocence

Il y a quelques années, la cybersécurité se limitait à quelques piratages de banques ou d'entreprises et ne parlait qu'à une poignée de spécialistes. Aujourd'hui elle est partagée par tous les citoyens. Nos sociétés ont pris conscience de leurs vulnérabilités. L'ensemble de nos organisations et de nos nations est concerné.

Avant la présidence Trump, les États-Unis ont montré qu'ils pouvaient remettre en cause les piliers fondamentaux de la confiance de l'internet à l'échelle mondiale, en sapant les soubassements des systèmes de sécurité utilisés partout sur la planète. Des programmes entiers de la NSA avaient pour objectif de créer des backdoors dans les systèmes de sécurité et d'affaiblir les systèmes de chiffrement. Lorsque vous créez une faille de sécurité, elle est agnostique, c'est-à-dire qu'elle est ouverte aussi bien pour vos ennemis que pour vous-même. La vulnérabilité devient systémique et elle peut se retourner contre vous.

Les preuves sont tangibles, tant au niveau industriel que de l'évolution de l'actualité.

Qui finance les systèmes de sécurité des objets connectés aux États-Unis ? La NSA. Qui s'inquiète du devenir sécuritaire de nos infrastructures informationnelles ? Les grandes agences de sécurité. Et qui est le bras droit du président Trump dans le domaine des technologies ? Peter Thiel, patron et cofondateur de PayPal et surtout de Palantir, la start-up de la CIA qui est l'outil d'analyse prédictive des données big data utilisé par la quasi totalité de l'appareil militaro-internet américain. Toutes les agences de sécurité utilisent Palantir. Sa capacité d'analyse et de suivi, voire d'influence sur les opinions, aurait paraît-il été brillamment utilisée lors de la campagne de Trump pour lui permettre de cibler voire d'influencer certains États et de

cibler certaines populations.

8.1.2 Objets connectés : un vecteur de risque avéré

Notre infrastructure informationnelle est aujourd'hui notre bien le plus précieux, avant la montée en puissance de l'internet des objets.

L'attaque du 22 octobre 2016 sur les ressources critiques de l'internet aux États-Unis, via le prestataire Dyn, a été basée sur l'utilisation d'objets connectés comme robots d'attaques. Caméras de contrôle, distributeurs de boissons, etc., tous ces objets peu sécurisés ne font jamais l'objet de mise à jour de sécurité.

Dans les temps à venir, au lieu de s'attaquer au New York Times ou aux ressources informationnelles, on s'attaquera aux humains. Le prochain enjeu de la cybersécurité sera la protection des citoyens.

Un virus dans les appareils médico-connectés ou les voitures auto-pilotées, et c'est la création d'une arme de destruction massive à coût zéro : pertes massives et blocages d'infrastructures cruciales telles que l'énergie, sans même mettre un pied sur le territoire ennemi !

8.1.3 Participer à l'édification des normes

Nous devons être là où se créent les normes et standards des technologies de sécurité et de l'internet au sens large.

Le devenir de nos sociétés est engagé (et non plus seulement les dividendes boursiers d'une poignée d'actionnaires).

Si nous ne participons pas à l'édification de ces normes, en ayant des géants européens, nous serons rayés de la carte des pays et de l'économie.

Nos homologues allemands sont très vigilants sur ces questions. Nous devons prendre conscience de notre vulnérabilité et être capables de rebondir à l'échelle européenne, une Europe peut-être recentrée.

8.1.4 Trop de divisions industrielles en Europe

En ce jour de « Brexit / Scot-in », il faudra réfléchir à la bonne échelle de l'espace européen en matière de cybersécurité.

Dès sa création, l'Institut de la souveraineté numérique a souligné sa vision européenne de la souveraineté (et non pas « souverainiste »). En cette période de campagne électorale, et de campagne numérique, le diagnostic concernant l'espace européen d'une souveraineté numérique n'a pas été correctement fait par la plupart des acteurs politiques. Notre vulnérabilité, c'est la division. Combien de divisions industrielles en Europe aujourd'hui sur ces sujets ?

En matière de cybersécurité, il n'est pas possible de réfléchir à la souveraineté d'un point de vue uniquement technique ou juridique. Nous devons avoir une présence industrielle. Or ce n'est pas le cas aujourd'hui. Aux côtés des GAFA, NATU (Netflix, Air BNB, Telsa et Uber) et BATX (Baidu, Alibaba, Tencent, Xiaomi), l'Europe n'a aucun acronyme à rajouter.

> • Dans la liste mondiale des 152 start-up valorisées à plus d'1 milliard d'euros, **il n'y a que 16 Européens, et un seul Français : BlaBlaCar.**[19]

8.1.5 Ubériser nos propres acteurs intra-européens

Les start-up fleurissent en France massivement, et elles filent grandir à l'étranger !

Certes, nos instruments de financement sont insuffisants, mais il y a aussi un obstacle psychologique majeur à penser ce mot : « ubérisation ».

Une vision défensive n'est pas souhaitable : le but n'est pas d'empêcher l'ubérisation. Il ne s'agit pas non

---

[19] Toute la liste sur le site *The Billion Dollar Startup Club*, The Wall Street Journal and Dow Jones Venture Source, http://graphics.wsj.com/billion-dollar-club

plus de permettre à de grands acteurs (CAC 40 etc.) de pouvoir ubériser des sociétés à l'international.

Nous devons ubériser nos propres acteurs. Il nous faut des acteurs intra-européens qui vont ubériser des acteurs plus anciens et montrer qu'ils sont capables de grandir, au-delà de la plateforme continentale européenne, vers des marchés internationaux. Cette dimension-là est cruciale, y compris sur la cybersécurité. Si nous ne le faisons pas, les États européens, individuellement, deviendront tous vulnérables, Allemagne et France comprises.

_ Thibault VERBIEST, avocat associé, De Gaulle Fleurance & Associés : Ce monde inquiète, mais nous ne sommes pas inactifs. Dès 2013, la France a soumis les organismes d'importance vitale à des obligations de sécurité et de notification des incidents de sécurité. La France et l'Allemagne sont les seuls pays européens à s'être dotés d'une législation très proche de la récente Directive européenne NIS.

Philippe Dewost a des choses à nous dire sur la cybersécurité, notamment en relation avec les objets connectés.

8.2 Suggestions à la Commission européenne

Philippe DEWOST, directeur adjoint, Mission Programme d'Investissements d'Avenir, Caisse des Dépôts et Président d'Honneur du CHECy (Centre des Hautes Etudes du Cyberespace)

Homo Deus[20] démontre comment le communisme, lors de sa mise en place, s'est d'abord fondé sur une compréhension du monde réel et de ses transformations industrielles, et non sur une action dogmatique.

Question à la salle : Combien d'entre nous utilisent Gmail pour leurs communications électroniques ? et un VPN pour se connecter à un réseau Wifi ouvert comme celui qui nous est proposé aujourd'hui ? Nous sommes à égalité…

8.2.1 Quatre observations

Voici quelques observations que j'ai adressées à l'attention conjointe des DG Energie et DG Connect de la Commission européenne à Rome il y a quelques jours.

1. Raisonner sur différentes échelles de temps simultanément. La jonction de l'IT (Technologies de l'Information) et de l'OT (Technologies des Objets - IoT) est un enjeu de très large échelle. L'IT va beaucoup plus vite que l'OT, parce que dans l'IT il y a du software, alors que dans l'OT il y a du hardware. Les octets se manipulent et se déplacent à des coûts bien inférieurs que pour les atomes…Les cycles de vie des objets, notamment industriels, sont beaucoup plus longs que les cycles informatiques, en raison de la combinaison des lois de Moore et de Metcalfe.

- Ceci éclaire l'attaque Dyn sur les caméras de sécurité, ou le piratage potentiel d'une vingtaine de millions de voitures Volkswagen via leur « plip » (kit d'ouverture à distance). À l'origine, le directeur des achats chez VW a du fort normalement décider qu'il ne fallait pas mettre plus de, disons 25 cents dans le module de chiffrement de la clé, ce qui était tout à fait raisonnable à l'époque. VW a simplement oublié que le cycle de vie de leurs voitures est de l'ordre de dix ans. Sur une telle période la loi de Moore vous rattrape assez rapidement….

2. La vitesse prend le pas sur la solidité des forteresses. Dans certains domaines, les membres de l'Union Européenne gagneraient à s'aligner sur les plus rapides comme l'Estonie (et non pas sur les plus puissants, que vous mesurez par le PIB, autrement dit le couple franco-allemand).

- Trois ans pour élaborer une directive me semble un peu long, même si je suis conscient que raisonner dans l'urgence de l'émotion est sujet à caution.

- Dans le même ordre d'idées, investir moins dans l'épaisseur de ses murs et plus dans la détection agile et le rebouchage des failles me semble une approche intéressante, comme l'a montré Tesla. Encore faut-il être capable d'acheter le premier les découvertes de failles « zero day » puis de redéployer à distance les correctifs réalisés dans les heures qui suivent…

[20] « Homo Deus, a brief history of tomorrow », Yuval Noah Harari, éd. Harvill/libri, 2016.

3. La technologie se décentralise. Les réseaux se sont décentralisés, les transactions sont en train de se décentraliser avec la blockchain, le développement logiciel se décentralise et se répand, ainsi que le hacking.

> • La start-up Neuralink ambitionne d'hybrider nos cerveaux et les machines. La protection des humains va bientôt concerner celle de nos cerveaux. Des failles zero-day[21] permettront de « bricker » les humains (et non plus seulement les smartphones). Des mises à jour logicielles de mauvaise qualité risquent de devenir un sujet pour l'humanité.

4. Les hackers au service des États. Jusqu'à présent, les hackers servaient la cause ou repoussaient leurs propres limites. Désormais ils peuvent se mettre au service des États. Pour le pire et pour le meilleur.

8.2.2 Cinq enjeux majeurs et suggestions

1. Le hardware et la maîtrise des couches basses

En été 2016, la Chine a présenté son nouveau super calculateur le plus rapide du monde. Sunway TaihuLight est trois fois plus rapide que son prédécesseur chinois , mais on notera surtout que la totalité de ses processeurs sont désormais chinois (LoongSon). Plus un seul processeur n'est américain et c'est sans doute un choix (géo)politique.

> • Suggestion : l'Europe ferait bien de se pencher sur des architectures ouvertes telles qu'Open RISC-V développé à Berkeley par l'Université de Californie.

2. Le développement du Bug Bounty[22]

> • Suggestion : un cadre réglementaire permettant à des *white hat* (hacker agissant dans un cadre légal) de combler des failles zero-day de l'extérieur.

3. Le travail avec les start-up

Les consultations conduites par la Commission européenne se font avec les plus grands acteurs industriels européens. Il y a me semble-t-il « un éléphant dans la pièce » : Les start-up n'y figurent pas. Pourtant elles resteront toujours plus agiles et plus compétentes que les grands groupes notamment sur ces sujets de disruption numérique.

> • Suggestion : inviter les start-up dans les consultations de la Commission européenne.

4. La traçabilité et l'auditabilité du code et des processus, pour peu que l'on assure sur la durée la maintenance de ce code. Un code open source mal maintenu peut être à l'origine de très gros problèmes comme l'a démontré l'an dernier l'accident industriel de TheDAO.

> • Suggestion : s'appuyer sur le code source.

5. L'éducation des utilisateurs et des enseignants. J'ai été effaré par l'enseignement informatique qu'ont reçu mes enfants à l'école primaire. Celui-ci consistait à décrire l'ordinateur avec des mots de vocabulaire et à en définir une taxinomie comme on le fait en biologie.

Par ailleurs, dans trop de grands groupes, l'informatique est vue comme un centre de coûts piloté par la direction des achats, ou rattaché au secrétariat général dans le meilleur des cas. Or comme le rappelle sa dénomination anglo-saxonne, il s'agit d'une science.

> • Suggestion : que les écoles informatiques françaises comme Epita / Epitech fassent partie des grandes écoles « du groupe A ».

Pour conclure : il faut se souvenir que « la sécurité est une taxe sur les honnêtes gens ». L'équilibre entre

[21] Faille zero-day : vulnérabilité informatique logicielle non publiée et pouvant être exploitée par des pirates.

[22] Bug Bounty : récompense offerte par une entreprise ou un site web aux développpeurs qui ont découvert des vulnéabilités.

la sécurité et le respect de la Privacy est très difficile à trouver. On a pu lire récemment que le FBI aux États-Unis jouait avec les données de reconnaissance faciale de dizaines de millions d'Américains sans aucun contrôle. C'est bien d'être honnête, encore faut-il ne pas être naïf.

_ Thibault VERBIEST : Au lieu de parler de souveraineté numérique, Guy-Philippe Goldstein propose le concept de souveraineté par l'influence numérique. Cette philosophie mériterait plusieurs thèses.

8.3 La recette israélienne : interdépendant et souverain

Guy-Philippe GOLDSTEIN, Senior Analyst, Cyberdesk Wikistrat

La question posée par M. Christian Harbulot est fondamentale : Quelle politique de puissance ? Cela implique de rechercher l'indépendance nationale, l'indépendance par rapport à l'influence d'autrui, et de préserver la défense de ses propres intérêts. Pour être indépendant, il faut développer sa propre capacité d'indépendance, comme ce fut le cas avec le nucléaire par de Gaulle en 1966.

Le numérique est particulier. Il se développe en réseau. L'espace numérique est un ensemble d'embranchements qui se développent de manière exponentielle. L'innovation est permanente. La valeur d'une réflexion en réseau va suivre la loi de Metcalfe (proportionnelle au carré du nombre de ses utilisateurs). Pour être plus riche, plus fort, je dois m'interconnecter avec le maximum de personnes.

Pour ne pas dupliquer ce qui est fait ailleurs, je dois trouver ma spécialisation en développant mon propre nœud dans le réseau. Cela nécessite un effort constant d'innovation.

Dans le numérique, la manière d'être le plus influent et de défendre l'indépendance de ses propres intérêts est de défendre son influence, et non pas de se recroqueviller sur une ligne Maginot numérique.

La politique industrielle de l'État d'Israël illustre cette approche. Que les raisons soient organiques, culturelles, les questions de sécurité sont omniprésentes dans tout le corps social.

8.3.1 Attirer les talents

Cela a été dit par Muriel Touaty : au départ, il y avait une absence de ressources en Israël. Au début de son histoire dans les années 90, la *Start-up Nation* n'avait pas d'argent. Plusieurs politiques industrielles ont échoué. D'abord il y a eu un afflux extraordinaire de cerveaux venus de l'extérieur et du talent.

Pour des raisons historiques et militaires, la France a également su développer une vraie politique du talent. On retrouve cet avantage compétitif dans la Silicon Valley.

8.3.2 Développer les start-up

Israël s'est développé en poussant les start-up à se développer, et non pas en cherchant à défendre de grands champions nationaux. Dès la fin de leur service militaire dans les services de renseignement (Unité 8200), les jeunes sont poussés hors de l'armée pour développer leurs propres start-up.

L'innovation se fait dans les start-up, là où l'on peut aller au plus vite dans la recherche de nouveaux nœuds dans le réseau. Cela ne peut se faire dans un cadre bureaucratique, au milieu des frictions politiques propres aux grands groupes.

8.3.3 Le capital risque hybride

En Israël, le développement de l'écosystème local s'est fait en interdépendance avec les Etats-Unis. Le gouvernement israélien (ministère des sciences, des technologies et de l'espace) a fait appel à du capital privé américain en le mêlant à des investisseurs israéliens. Le marché américain est le plus grand marché au monde. Il permet de développer plus rapidement des start-up. Mais pour ne pas être complètement dépendant des Américains, le gouvernement israélien a su générer localement une industrie de capital risque.

Dans le capital risque, le capital n'est pas uniquement de l'argent, c'est aussi le *smart money*. Dès le début, Israël s'est rendu compte qu'ils ne savaient pas développer des entreprises tech. L'entrepreneur tech, le manager tech, n'existaient pas en Israël, et donc on les a fait venir, tout en développant cette industrie locale de capital risque.

Un écosystème s'est développé. Aujourd'hui, quand une entreprise israélienne se fait racheter par une entreprise américaine, c'est un signe très positif pour l'écosystème israélien. Cela signifie que d'autres entreprises américaines sont prêtes à parier sur des équipes techniques locales, pour les faire vivre et donner des salaires à ces ingénieurs, et donc alimenter toute la filière éducative.

8.3.4 Un écosystème local souverain et interdépendant des Américains

En termes de souveraineté, cette géopolitique d'interdépendance permet d'avoir des points de contrôles sur ses partenaires. Les clients des start-up israéliennes sont des Américains. Cette bonne connaissance du marché américain crée un lien d'interdépendance. Israël est un partenaire de poids des Américains, à tel point qu'Israël est capable d'aller renégocier de très larges contrats sur l'armement et de mener une politique diplomatique qui ne va pas nécessairement dans le sens de ce que voudraient les Américains. On est fort et souverain, car on est indispensable pour les autres dans un contexte d'interdépendance pour tout le monde, imposé par la logique des réseaux. L'influence dans un monde du software et des réseaux universels se fabrique différemment que dans le monde du hardware et des territoires circonscrits.

8.4 Les priorités du prochain quinquennat

Lionel TARDY, député de la Haute-Savoie

L'État doit être capable d'assurer sa protection, sa compétitivité et son attractivité, autant de critères en matière de souveraineté numérique. Tous les acteurs doivent être impliqués : État, collectivités, entreprises, citoyens.

En cas de cyberattaque généralisée, on n'est pas capable aujourd'hui de fonctionner en mode autonome. Exemple : l'annulation par le gouvernement du vote électronique aux législatives pour les Français de l'étranger. Cela dénote un manque de préparation et la crainte d'une cyberattaque. Ce sujet mineur peut changer les règles d'une élection.

Autre exemple avec le cloud. La très grande majorité de nos données sont hébergées à l'étranger. Avec la décentralisation de l'infrastructure informatique, les entreprises perdent une part du contrôle sur leurs données.

Pour maîtriser notre souveraineté, il faut maîtriser les cœurs de réseau, les serveurs racines, la normalisation. Au niveau des équipements, nous devrons avoir une politique industrielle à l'échelle européenne.

Toute seule, la France ne sera pas capable de créer le futur Google.

8.4.1 Le couple franco-allemand

Les décideurs publics, élus ou fonctionnaires, souffrent d'un manque de compétence numérique pour comprendre les enjeux et négocier au niveau international. La souveraineté, c'est aussi savoir imposer les normes.

La Chine ou Israël ont su imposer une véritable politique publique en matière de cybersécurité.

Nous militons pour une initiative avec l'Allemagne dans ce domaine. Le couple franco-allemand pèse lourd. 150 millions d'habitants, les deux plus grandes puissances européennes en termes de PIB, une taille critique importante.

L'Europe réagit beaucoup trop lentement, sur le sujet du numérique comme sur la fiscalité. Le couple franco-allemand peut relancer les choses, et puis ensuite, qui nous aime nous suive.

8.4.2 Quatre leviers d'action

Dans le numérique, les plus gros vont manger les plus petits, et les plus agiles vont manger les plus lents.

Nous devrons :

1. Construire une filière des infrastructures européennes du numérique, du microprocesseur jusqu'au software, dans un premier temps conjointement avec l'Allemagne, puis au niveau

européen.

2. Modifier le cadre réglementaire européen. Toute activité sensible en Europe doit être supportée par des solutions hardware et software auditables et maîtrisées. C'est une priorité pour être autonome en termes de souveraineté.

3. Accepter des dérogations avec la commande publique lorsque notre autonomie stratégique et notre cybersécurité sont en jeu. Dans les choix qui sont faits, y compris par l'armée, ne faut-il pas privilégier de temps en temps un acteur français ou européen ?

4. Créer des fonds sectoriels et technologiques dans des domaines de pointe, dont la cybersécurité. L'État doit être capable d'assurer sa contribution en matière de cybersécurité au niveau des entreprises.

8.4.3 La formation des « combattants numériques »

Il faut encourager le développement des filières universitaire qui sont consacrées aux nouveaux métiers. Les lacunes sont énormes, que ce soit dans la programmation informatique, la cybersécurité, l'intelligence artificielle, la blockchain.

L'enseignement supérieur doit inscrire un module dédié aux techniques de cybersécurité dans les programmes de la plupart des disciplines.

Tous ces éléments doivent être mis en place rapidement. Pour assurer la cybersécurité, il faut agir sur quatre niveaux : l'État, les institutions, les entreprises, les citoyens.

8.5 Discussion

8.5.1 Les territoires sont démunis

_ Thibault VERBIEST : La cybersécurité ne concerne pas que les grandes entreprises. Elle est vécue aussi par des PME. Parfois des Chambres de commerce locales nous consultent, complètement affolées, parce que certains de leurs membres sont rançonnés en bitcoin pour désactiver un virus. Elles ignorent si c'est légal de payer. Il n'y a aucune information au niveau local. Quel est le service de l'État compétent ? À Paris, il existe des services spécialisés de la gendarmerie et de la police nationale. En province, ces entreprises sont totalement livrées à elles-mêmes. Ces piratages arrivent tous les jours.

8.5.2 Palantir à la DGSI

_ Un auditeur : On a évoqué Palantir dans sa genèse. L'administration française au sens large est cliente de Palantir. Honnêteté et naïveté…

_ Bernard BENHAMOU : C'est très clair. Le contrat en question a été négocié auprès de la Direction générale de la sécurité intérieure il y a plus d'un an, avant que nous ne connaissions l'étendue de l'influence réelle de Palantir au niveau mondial. Il nous faut développer nos propres expertises, même si dans un premier temps, cela nous pose des difficultés. La vassalisation des services de renseignement, qui s'ajoute à celle autour des GAFA, des NATU et bientôt des BATX, a des limites si l'on veut ne pas devenir définitivement, comme le dit l'excellente Catherine Morin-Desailly[23], une « colonie numérique » de deux autres continents.

9. Clôture – **Pour une ambition européenne de l'industrie numérique**

Laure de LA RAUDIERE, députée d'Eure-et-Loir

Avec Corinne Erhel, nous nous sommes toujours attachées à porter les enjeux du numérique à l'Assemblée nationale dans un double objectif : faire gagner la France et faire progresser nos collègues dans la compréhension des enjeux de transformation de la société par le numérique.

Une tâche difficile. À trop vouloir ajuster des problèmes de court terme en politique, on oublie de réfléchir à

[23] Sénatrice de Seine-Maritime, présidente de la commission Culture, éducation et communication.

plus long terme et de porter une vision d'avenir pour les Français.

Dans le cadre des élections présidentielles, on entend parler des start-up, ce qui est déjà bien, mais on n'entend parler que des start-up à propos du numérique. J'en suis profondément désolée.

9.1 Les briques du dynamisme entrepreneurial en France

Les start-up, c'est peut-être ce qu'on a fait de mieux en France. D'abord parce que la dynamique entrepreneuriale est forte, liée à des acteurs privés. Les jeunes diplômés français veulent d'abord créer une start-up ou travailler dans une start-up plutôt que dans un cabinet d'audit. C'est une excellente opportunité, qu'il faut appuyer.

- La création par Fleur Pellerin du **label French Tech** nous permet de porter ce dynamisme à l'étranger, d'améliorer l'image de la France à l'étranger.

- La création de la **banque publique d'investissement** et la nomination à sa tête d'une personne venant du monde de l'entreprise a permis de développer plusieurs programmes favorables au développement numérique en France, à la transformation numérique des entreprises et à la prise de conscience de la cybersécurité et de la protection des entreprises face aux attaques qu'elles subissent en permanence, piratage d'informations sans même s'en rendre compte.

- Le financement de l'innovation en France a été maintenu de façon continuelle entre les différents gouvernements, avec le maintien du **Crédit d'Impôt Recherche**, le maintien et le développement du statut de **Jeune Entreprise Innovante**, la poursuite des **Investissements d'avenir** fléchés vers le numérique. Notre écosystème de la recherche et de l'innovation est envié par les autres pays.

9.2 La 2è révolution numérique est en cours

Je regrette que le thème de la souveraineté numérique en France et en Europe soit absent du débat des élections présidentielles. La première des ambitions européennes devrait être de construire une souveraineté numérique. Aussi je tire la sonnette d'alarme :

La première phase de la révolution numérique concerne tous les nouveaux services développés depuis une vingtaine d'années sur internet : Google au départ, pour l'accès à la gigantesque base de connaissance et de service qu'est Internet, Facebook ou LinkedIn pour la connexion des individus dans le monde entier ; YouTube ou Netflix pour l'accès à l'offre culturelle films et musique ; Booking ou AirbnB pour la mise en valeur d'offres d'hébergement variées ; Amazon pour la banalisation du e-commerce. Tous ces géants de l'internet que nous utilisons majoritairement sont Américains. Tous connaissent un peu, ou beaucoup de nous-mêmes grâce aux données qu'ils collectent en permanence sur nos comportements.

La deuxième phase de la révolution numérique est celle de l'intelligence artificielle, les robots intelligents, les objets connectés qui vont prendre des décisions pour nous, et tout ce qui va avec, c'est-à-dire l'explosion de la collecte des données sur nous-mêmes et sur notre environnement.

Si cette histoire de l'internet continue, nous mettrons nos vies personnelles, nos vies collectives et celle des États dans les mains des Américains, ou alors peut-être, avec une reconfiguration, dans celles des Chinois. Nous leur donnons déjà tout volontairement ! Nul besoin de cybersécurité dans ce cas. De plus, nous ne savons pas non plus où sont hébergées nos données. Peut-être dans un ancien goulag de Sibérie, qui sait ?

9.3 Pour un espace numérique franco-allemand

La souveraineté numérique passe par la maîtrise industrielle de la production des données à l'échelle européenne : microprocesseurs, équipements réseaux, cloud et code. Je ne crois pas, je ne crois plus que nous pourrons agir d'emblée sur ce sujet à 27.

Les chefs d'État ne sont pas mûrs, les autres pays non plus pour discuter de ces sujets-là. Que l'on évoque la question des données électroniques et de l'hébergement des données, la réponse est toujours la même : « libre-échange ! »

Il ne s'agit plus d'économie. Il s'agit de protéger nos citoyens, de sécuriser nos pays, de faire appliquer nos lois. Il faut donc revisiter l'ambition européenne.

Nous ne le ferons pas seul, au risque d'handicaper nos start-up. Comme ce sont des entreprises extrêmement agiles, si les règles en France sont plus contraignantes qu'ailleurs en Europe, elles partiront s'installer dans un pays voisin. À 27, nous y passerons 10 ans. Donc je milite **pour la construction en bilatérale avec l'Allemagne d'un espace numérique homogène**, avec :

- une réglementation identique entre les deux pays,

- une vision éthique sur la vie privée, l'usage que l'on peut faire des données, des algorithmes d'intelligence artificielle,

- et finalement une réflexion de la place de l'homme dans ce cyberespace.

Il faut aussi avoir une ambition industrielle numérique pour la richesse de nos pays.

C'est dans ce cadre qu'il convient de renforcer l'industrie de la cybersécurité et de la cyberdéfense.

9.4 Un choix de société

À l'heure de la prise de décision par des algorithmes d'intelligence artificielle, nous devons définir :

- quelle sera la place des décisions humaines,

- quelles seront les règles communes de vie de notre société,

- et au premier rang, quelle sera la place de la vie privée et de la solidarité.

Ce n'est pas aux Américains de répondre à ces questions. Ce serait délaisser notre vision de la société à d'autres, un abandon complet de notre culture, de notre indépendance et de notre avenir.

9.5 Quelques idées pour une gouvernance à l'Elysée

Je ne suis pas certaine que les actuels chefs d'État européens aient conscience de ces enjeux-là, ou en tout cas, aient eu l'ambition d'y travailler. Aujourd'hui il n'y a pas de conseiller numérique à l'Elysée pour bâtir la stratégie numérique de l'État français. Il faut en discuter avec le Président, le secrétaire général de l'Elysée ou le directeur de cabinet. Et chacun sait que ce n'est pas le rôle d'un secrétaire d'État au numérique de bâtir cette stratégie, tant le numérique est transverse et touche tous les ministères.

La gouvernance dans le prochain mandat sera un point essentiel à discuter avec le futur gouvernement, le futur président de la République. Je milite pour :

- **Un conseiller en stratégie numérique à l'Elysée** de bon niveau, venant si possible du privé, qui puisse avoir l'oreille du Président, parler de ces enjeux stratégiques et construire une vision d'avenir. Le Président ne peut pas l'avoir seul. Il lui faut une vision sur l'avenir de la société, ce qui se construit, la place des robots et des algorithmes d'intelligence artificielle, pour qu'il puisse porter la pédagogie vis-à-vis des Français et en bilatérale avec les autres chefs d'État.

- **Des meetings ou des réunions mensuelles sur le numérique à l'Elysée** pour alimenter cette vision stratégique, par exemple pour se demander si c'est normal que Palantir soit le prestataire informatique de la DGSI en France.

- **Des compétences numériques pour le futur ambassadeur de France en Allemagne**. On ne construira pas une collaboration profonde avec l'Allemagne sans une diplomatie sur le numérique. Le Quai d'Orsay a besoin d'un excellent diplomate en charge du numérique, et c'est le cas aujourd'hui avec l'excellent David Martinon. Il doit être relayé avec l'ambassadeur de France en Allemagne pour cet espace numérique franco-allemand.

- **Un Secrétaire Général Modernisation de l'Action Publique / Transformation numérique** à côté du SGMAP classique, pour assurer la gestion de l'équilibre des textes de lois, la transformation numérique de tous les services de l'administration, la réflexion en matière d'évolution des formations, d'éducation à la santé, avec suffisamment de poids pour influer les décisions des ministères.

Le rôle du ministre ou du secrétaire d'État en charge du numérique sera de décliner cette politique. Il sera grandement épaulé par une telle gouvernance. Si l'on ne la met pas en place, on rediscutera des mêmes sujets l'an prochain, avec des gens initiés mais pas assez nombreux et suffisamment haut placés pour

prendre les bonnes décisions.

Partenaires

Aromates remercie Monsieur Jean-Yves Le Drian, Ministre de la Défense, Monsieur Bruno Le Roux, ex-Ministre de l'Intérieur pour leur parrainage, Madame Corinne Erhel, députée des Côtes-d'Armor et Madame Laure de La Raudière, députée d'Eure-et-Loir, ainsi que tous les intervenants pour leur participation.