

LA REVUE FORUM DU NUMÉRIQUE

Souveraineté numérique européenne :

Comment concilier coopération
et compétition ?

2025

Le Forum du Numérique

16 mai 2024, à Lille

Pour sa deuxième édition, les travaux du Forum du Numérique ont porté sur la souveraineté numérique européenne, autour d'une question centrale :

« SOUVERAINETÉ EUROPÉENNE, QUEL ÉQUILIBRE ENTRE COMPÉTITION ET COOPÉRATION ? »

Pour de multiples raisons qui touchent à la maîtrise des technologies ou à l'ingérence étrangère, le numérique est l'un des sujets centraux de la souveraineté européenne.

C'est pourquoi les travaux de la 2^{ème} édition du Forum du Numérique ont porté sur les enjeux de souveraineté numérique. Il s'agit d'un sujet dont l'importance est croissante pour l'Union européenne et ses États membres.

Pour gagner en souveraineté, l'Union européenne se doit d'agir sur les 3 fronts suivants :

- le cadre réglementaire et normatif,
- le développement rapide de ses propres capacités numériques, matérielles et immatérielles,
- s'adapter à la dimension indissociable de l'innovation et de la société.

La souveraineté suppose de pouvoir exercer un contrôle sur les technologies numériques, les données, l'infrastructure et les services numériques afin de protéger ses intérêts économiques, politiques et culturels. Cela inclut la protection des données personnelles, la sécurité des réseaux et des infrastructures critiques.

Elle impose d'investir vite et avec des fonds d'origine européenne, dans tous les champs de l'innovation technologique.

Pour autant, dans le domaine du numérique, l'autarcie européenne est impossible. Il est donc utile de réfléchir aux cadres politique et économique dans lesquels le numérique se développe et de chercher à trouver le meilleur équilibre entre la compétition, utile au progrès et à l'innovation, et la coopération, nécessaire à la solidarité.

Le 16 mai 2024, les partenaires du Forum du Numérique et les intervenants présents ont partagé leurs réflexions, leurs travaux, leur expérience et leurs bonnes pratiques (intervention de grands témoins, phases d'écoute inspirantes, face-à-face, tables rondes).

Contributeurs (28) :

Steven BOURGEOIS, Sophie CAVILLON, David COLON, Arnaud COUSTILLIÈRE, Manuel DAVY, Nicolas DEVAUX, Anne DUBOSCQ, Adrien FATIBENE, Hervé FÉVRIER, Christophe GOMART, François GORRIEZ, Léo HAMON, Céline HELLER, Anne LE HÉNANFF, Georges LOTIGIER, Alexandre MALAFAYE, Simon MARÉCHAL, Félix VON NOSTITZ, Jean-Paul PINTE, Théo PLANTIER, Jalal POSSIK, Mathias POVSE, Laura SCHAUB, Joséphine STARON, Jérôme TABARIES, Hervé TROALIC, Hugo WEBER, et Belhassen ZOUARI.

NOS INTERVENANTS

PARRAIN & MARRAINE



Alexandre Malafaye
Président Synopia



Arnaud Coustillièr
Amiral (2S),
Président du Pôle Excellence Cyber



Anne Le Hénanff
Députée du Morbihan, Membre de
la commission de la Défense



Mathias Poyse
Directeur régional,
EDF Hauts-de-France



François Gorriez
Avocat, Cabinet Mathias Avocats,
auteur de l'ouvrage «Le droit de la
cybersécurité»



Nicolas Devaux
Adjoint au directeur en charge de la
RSE et de la préparation de l'avenir,
Hauts-de-France Nord-Pas de Calais,
ENEDIS



Patrick Scaufaire
Président-Recteur,
Université Catholique de Lille



Jalal Possik
Directeur, Ecole du Numérique,
Université Catholique de Lille



Adrien Fatibene
Responsable Partenariats et
Développement, Campus Cyber
Hauts-de-France



Hugo Weber
VP, Corporate Affairs & Impact
M irak l



Joséphine Staron
Directrice des Etudes et des
Relations Internationales, Synopia



Jean-Paul Pinte
Docteur en sciences de
l'information et de la communication,
maître de conférences,
Université Catholique de Lille



Judith Mehl
Co-fondatrice, Ethik IA



David Colon
Enseignant-chercheur,
Sciences Po



Léo Hamon
Responsable des affaires publiques,
IBM



Patrick Zimmermann
Amiral (2S),
Délégué adjoint, Synopia



Manuel Davy
CEO & Founder Vekia,
Président de la Cité de l'IA



Steven Bourgeois
Director Governments,
Public Sector, European Affairs,
EuraTechnologies



Georges Lotigier
CEO, Founder et board member
Hornetsecurity Vade



Felix von Nostitz
Maître de conférences en science
politique, co-responsable master
Digital Politics and Governance,
ESPOL



Christophe Gomart
Général (2S), ancien Directeur du
renseignement militaire



Théo Plantier
CEO, OVERSOC



Simon Maréchal
Responsable régional
Hauts-de-France, association
Emmaüs Connect



Anne Duboscq
Directrice des affaires publiques,
OVHCloud



Hervé Troalic
Directeur général,
imineti by Niji



Céline Heller
Directrice commerciale Europe -
Souveraineté Numérique,
Google Cloud



Belhassen Zouari
Professeur en informatique,
spécialiste en cybersécurité,
Ecole du Numérique,
Université Catholique de Lille



Hervé Fevrier
Président,
Landelles Consulting



Jérôme Tabaries
Chef d'Escadron,
Responsable des relations
internationales et des partenariats,
Centre national de formation à la
cybersécurité



Sophie Cavillon
Doyen délégué, Faculté de gestion
économie & sciences,
Université Catholique de Lille

ORGANISATEURS ET PARTENAIRES

ACADÉMIQUES



UNIVERSITÉ
CATHOLIQUE
DE LILLE 1875



FACULTÉ DE
GESTION,
ÉCONOMIE
& SCIENCES



ETHICS
EA 7446

ESPΩL

GRANDS PARTENAIRES



Cigref
RÉUSSIR
LE NUMÉRIQUE

ENEDIS



HAUTS-
DE-FRANCE



LA QUINCAILLERIE



SOUTIENS DU FORUM



EURATECHNOLOGIES
EUROPE'S STARTUP BUILDER



PARTENAIRES ÉVÉNEMENTIELS

& MÉDIAS



SOMMAIRE

POURQUOI CE FORUM DU NUMÉRIQUE ?

par **Alexandre MALAFAYE**, Président, Synopia

LES GRANDS ENSEIGNEMENTS

par **Joséphine STARON**, Directrice des études et des relations internationales, Synopia

PRÉSENTATION DU FORUM DU NUMÉRIQUE 2024

par **Laura SCHAUB**, Directrice de projets, Synopia, en charge du Forum du Numérique

GRANDS TÉMOINS :

- **Anne LE HÉNANFF**, Députée, Morbihan
- **Arnaud COUSTILLIÈRE**, Amiral (2S), Président, Pôle d'Excellence Cyber
- **Christophe GOMART**, Général (2S), ancien Directeur du renseignement militaire

INFRASTRUCTURES NUMÉRIQUES EUROPÉENNES : UN DÉVELOPPEMENT EN COOPÉRATION

- **Nicolas DEVAUX**, Adjoint au directeur en charge de la RSE et de la préparation de l'avenir, ENEDIS Nord Pas-de-Calais
- **Adrien FATIBENE**, Responsable Partenariats et Développement, Campus Cyber Hauts-de-France
- **Hervé FÉVRIER**, Président, Landelles Consulting
- **Céline HELLER**, Directrice commerciale Europe – Souveraineté numérique, Google Cloud

INNOVATION : LA MAÎTRISE DU DESTIN NUMÉRIQUE EUROPÉEN

- **Steven BOURGEOIS**, Director Governments, Public Sector, European Affairs, EuraTechnologies
- **Anne DUBOSCQ**, Directrice des affaires publiques, OVHCloud
- **Léo HAMON**, Responsable des affaires publiques, IBM
- **Simon MARÉCHAL**, Responsable régional Hauts-de-France, association Emmaüs Connect
- **Hugo WEBER**, VP, Corporate Affairs & Impact, Mirakl

COGNITIF : LA PROTECTION DE NOS DÉMOCRATIES FACE À LA DÉSINFORMATION

- **David COLON**, Enseignant et chercheur à Sciences Po, auteur de *La Guerre de l'information. Les États à la conquête de nos esprits* (Tallandier, 2023)
- **Manuel DAVY**, CEO & Founder Vekia et Président de la Cité de l'IA
- **Jean-Paul PINTE**, Docteur en sciences de l'information et de la communication, et Maître de conférences, Université Catholique de Lille
- **Felix VON NOSTITZ**, Maître de conférences en science politique, co-responsable du master Digital Politics and Governance, Université Catholique de Lille, ESPOL

CYBER ET SÉCURITÉ : LE RENFORCEMENT DE LA SÉCURITÉ NUMÉRIQUE DANS L'ÉTAT DE DROIT

- **François GORRIEZ**, Avocat, cabinet Mathias Avocats et auteur de l'ouvrage *Le droit de la cybersécurité* (Nuvis, 2020)
- **Georges LOTIGIER**, Founder et board member, groupe Hornetsecurity-Vade
- **Théo PLANTIER**, CEO, OVERSOC
- **Mathias POVSE**, Directeur régional (2017 – 2025), EDF Hauts-de-France
- **Jérôme TABARIES**, Chef d'escadron, Responsable des relations internationales et des partenariats, Centre national de formation à la cybersécurité, Gendarmerie nationale
- **Hervé TROALIC**, Directeur général, Imineti by Niji
- **Belhassen ZOUARI**, Professeur en informatique, spécialiste en cybersécurité, École du Numérique, Université Catholique de Lille

REMERCIEMENTS :

par **Sophie Cavillon**, Doyen, Faculté Gestion Économie et Sciences, UCL

par **Laura SCHAUB**, Directrice de projets, Synopia, en charge du Forum du Numérique

FORUM DU NUMÉRIQUE 2024



ALEXANDRE MALAFAYE

PRÉSIDENT,
SYNOPIA



À quelques semaines des élections européennes, la seconde édition du Forum du Numérique a permis d'aborder en profondeur des enjeux stratégiques majeurs pour l'Europe : cybersécurité, souveraineté numérique, transformation digitale ou encore coopération transatlantique. À travers des interventions de haut niveau, ce rendez-vous a confirmé la nécessité d'une réflexion partagée et exigeante pour penser l'avenir du numérique européen.

Le thème de cette année – "La souveraineté numérique européenne : quel équilibre entre compétition et coopération ?" – incarne à lui seul les tensions et défis auxquels l'Europe est confrontée. Le mot "souveraineté" résonne particulièrement dans un contexte où l'Union peine encore à parler d'une seule voix. Entre partisans de l'autonomie stratégique et défenseurs du marché ouvert, les divisions persistent.

Cybersécurité et souveraineté numérique sont deux priorités majeures pour l'Europe. Face à la multiplication des cybermenaces, une réponse coordonnée s'impose, fondée sur des normes renforcées, des investissements en recherche et une culture partagée de la sécurité. En parallèle, l'Europe doit reconquérir son autonomie technologique dans des secteurs stratégiques comme le cloud, l'IA ou les semi-conducteurs, en développant des alternatives compétitives et en protégeant ses infrastructures critiques.

Mais cette transformation numérique ne peut être purement technologique. Elle est aussi **sociale, éthique et environnementale**. L'inclusion numérique, la protection des droits fondamentaux, la lutte contre la désinformation ou encore la réduction de l'empreinte carbone doivent guider les politiques publiques.

Le Forum a mis en évidence un impératif majeur : **la coopération est incontournable**. Face à la vitesse des ruptures technologiques, à la complexité des enjeux, aux manipulations, aux ingérences et à la compétition croissante avec des acteurs sans foi ni loi, aucun acteur – ni État, ni entreprise – ne peut agir seul. Une coopération renforcée entre Européens est la seule voie qui permettra de construire un espace numérique plus sûr, plus souverain et plus équitable.

Enfin, pour relever ces défis, l'Europe devra agir sur plusieurs fronts : politique industrielle ambitieuse, harmonisation réglementaire, montée en compétence de son capital humain et coordination stratégique face aux ingérences extérieures. Plus qu'un constat, ce forum a été un appel à l'action : **coopérer, innover, sécuriser**. C'est à ce prix que l'Europe pourra affirmer sa place dans le siècle numérique qui s'ouvre.



LES GRANDS ENSEIGNEMENTS DU FORUM DU NUMÉRIQUE 2024

Dans un contexte mondial marqué par l'intensification des cybermenaces, la dépendance croissante aux technologies extra-européennes et l'urgence d'une transition numérique inclusive et durable, l'Union européenne se voit contrainte de repenser ses politiques, ses infrastructures et ses capacités d'innovation afin d'assurer sa résilience, sa compétitivité et son autonomie stratégique.

La cybersécurité constitue le premier défi de cette ère numérique. Les institutions, les entreprises, les services publics, mais également les citoyens, sont désormais exposés à des attaques informatiques de plus en plus sophistiquées. Ces menaces, souvent transnationales, mettent à l'épreuve les capacités de coordination des États membres, la solidité des infrastructures numériques, mais aussi la souveraineté des données. Face à cette réalité, **l'Europe doit impérativement renforcer son arsenal normatif, investir massivement dans la recherche en cybersécurité, et consolider une culture commune de la sécurité numérique.**

Parallèlement, la question de la souveraineté numérique est devenue cruciale dans un monde dominé par quelques géants technologiques, principalement américains et chinois. **L'Europe, souvent réduite au rôle de consommatrice de technologies, doit retrouver sa maîtrise dans des domaines stratégiques tels que le cloud, les semi-conducteur et l'intelligence artificielle.** La dépendance à des solutions extra-européennes pour l'hébergement de données sensibles ou le fonctionnement de services publics expose les États membres à des risques d'ingérence, de surveillance ou de rupture d'accès. Il devient dès lors urgent de **bâtir des alternatives crédibles, interopérables et compétitives.**

Toutefois, **les initiatives européennes doivent s'accompagner d'un soutien fort à l'écosystème technologique européen**, notamment aux start-up, aux laboratoires de recherche et aux industriels stratégiques.

La transformation digitale, quant à elle, représente à la fois une opportunité économique sans précédent et un défi social et éthique majeur. La numérisation des services publics, de l'éducation, de la santé, de la justice ou de l'administration ouvre la voie à une plus grande efficacité, une meilleure accessibilité et une simplification des démarches. Sur le plan économique, **la digitalisation des chaînes de valeur et l'exploitation intelligente des données peuvent renforcer la compétitivité des entreprises européennes, stimuler l'innovation et favoriser l'émergence de nouveaux modèles économiques.**

Néanmoins, cette transition doit être pensée de manière inclusive et durable. Elle ne saurait se faire au détriment de la protection des droits fondamentaux, de l'équité sociale ainsi que de la préservation de l'environnement.

La fracture numérique, la protection des données personnelles, la lutte contre la désinformation ou encore l'impact environnemental des infrastructures numériques sont autant de dimensions qu'il convient d'intégrer dans une vision globale de la transformation digitale.

Pour renforcer sa position, l'Europe devra s'appuyer sur plusieurs axes stratégiques essentiels :

- Consolider son autonomie technologique par une politique industrielle ambitieuse, soutenue par des investissements publics et privés à la hauteur des enjeux.
- Approfondir l'harmonisation réglementaire entre les États membres afin de créer un véritable marché numérique intégré, capable de rivaliser avec les grandes puissances technologiques.
- Développer les compétences numériques, la formation continue et la recherche universitaire pour favoriser l'émergence d'un capital humain capable de porter l'innovation européenne.
- En matière cyber, mettre en place des stratégies de détection des ingérences étrangères et être capable d'y répondre, dans le cadre de l'état de droit.

Renforcer la position de l'Europe dans le domaine numérique dépendra de sa capacité à conjuguer sécurité, souveraineté et innovation. Comme les différents intervenants l'ont rappelé, face aux défis posés par la révolution numérique, seule une approche volontariste, coordonnée et résolument tournée vers l'avenir permettra à l'Europe de préserver ses valeurs, de défendre ses intérêts et d'affirmer sa place sur la scène mondiale.



PRÉSENTATION DU FORUM DU NUMÉRIQUE 2024

Lancé en 2023, le projet du Forum du Numérique repose sur le partage d'une conviction commune : les décideurs, et tous ceux qui ont en charge des équipes ou des populations, sont confrontés dans leurs organisations aux enjeux des transformations numériques, auxquels **il est souvent difficile d'apporter seul des solutions**. Pour répondre à ce besoin, Synopia a créé son Forum et se propose de mobiliser un panel pluridisciplinaire de décideurs publics, privés, associatifs, et académiques, afin de les faire travailler ensemble. Dans les mois qui précèdent le Forum, Synopia interroge ses partenaires au travers d'interviews et d'ateliers d'intelligence collective, pour réfléchir en amont aux enjeux du numérique et aux impacts en termes de cohésion. Le jour du Forum, différents formats ont été proposés afin de permettre aux participants de partager leurs expériences des enjeux de cohésion et leurs bonnes pratiques.

Notre objectif : bâtir et consolider une souveraineté numérique européenne. Tout au long de la journée, des experts et des grands témoins éclaireront le sujet sous différents angles. Le Forum du numérique a aussi pour ambition d'**établir des ponts nouveaux** entre le secteur public, le monde de l'entreprise, le monde académique, le secteur associatif, la recherche et l'innovation, et entre le national, le régional, et le local. La cohésion passe par là.

Lors de cette deuxième édition, Synopia a posé la question suivante :

« Souveraineté européenne : quel équilibre entre compétition et coopération ? »

Les chiffres clés du Forum du Numérique 2024 :

4 TABLES RONDES proposées au cours de la journée, avec des témoignages inspirants et des vrais partages d'expérience :

- Infrastructures numériques européennes : un développement en coopération
- Innovation : la maîtrise du destin numérique européen
- Cognitif : la protection de nos démocraties face à la désinformation
- Cyber et sécurité : le renforcement de la sécurité numérique dans l'état de droit

3 GRANDS TÉMOINS :

- Anne Le Hénanff, Députée, Morbihan,
- Arnaud Coustillière, Amiral (2S), Président, Pôle d'Excellence Cyber.
- Christophe GOMART, Général (2S), ancien Directeur du renseignement militaire

30 INTERVENANTS et experts de grande qualité.

+ DE 100 PARTICIPANTS en présentiel tout au long de la journée.

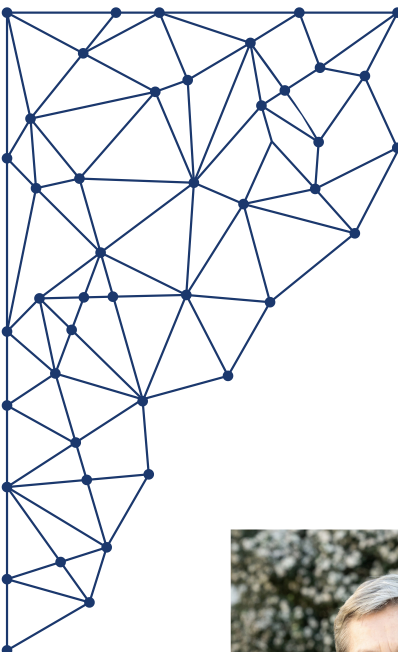
1 SOUTIEN et ENGAGEMENT déterminants de nos GRANDS PARTENAIRES : l'Université Catholique de Lille, avec la Faculté de Gestion, Économie & Sciences, l'École du Numérique, ETHICS Labs, ESPOL et de toutes leurs équipes, et EDF. Ainsi que les 28 autres PARTENAIRES entreprises, institutionnels, associatifs et académiques.

1 EXCELLENT ANIMATEUR, Thierry Fouquet, et le soutien sans faille de M la Constellation.

4 LABS mis à disposition pour faire découvrir les travaux, recherches et innovations des enseignants-chercheurs de l'École du Numérique.

1 ÉQUIPE au top avec l'appui de la Faculté de Gestion, Économie & Sciences et l'École du Numérique





GRANDS TÉMOINS



ANNE LE HÉNANFF

DÉPUTÉE,
MORBIHAN



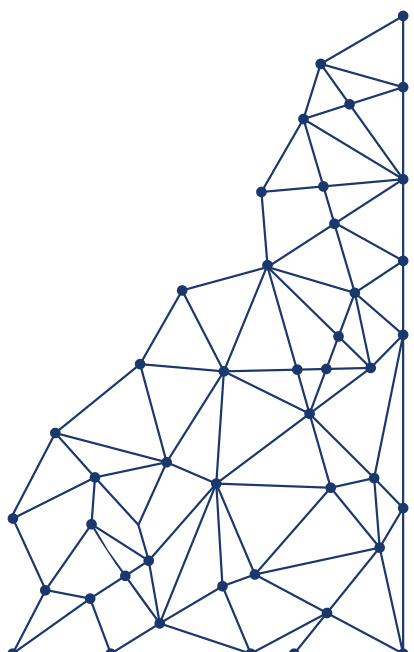
ARNAUD COUSTILLIÈRE

AMIRAL (2S)
PRÉSIDENT,
PÔLE D'EXCELLENCE CYBER



CHRISTOPHE GOMART

GÉNÉRAL (2S)
ANCIEN DIRECTEUR,
RENSEIGNEMENT MILITAIRE



FORUM DU NUMÉRIQUE 2024



ANNE LE HENANFF

DÉPUTÉE,
MORBIHAN



Thierry Fouquet (TF) : *La loi SREN est vraiment très intéressante pour l'avenir. Pourriez-vous nous en dire quelques mots ?*

Anne Le Hénanff (ALH) : À l'origine, la loi « Sécuriser et Réguler l'Espace numérique » (SREN) adapte plusieurs règlements européens, en particulier le *Data Act* qui porte sur la régulation, le contrôle des grands opérateurs du numérique et la façon qu'ils ont d'aborder le marché du *cloud*.

J'ai été rapporteure du Titre III du *Data Act* qui portait spécifiquement sur le *cloud*, notamment sur la régulation des grands opérateurs y compris des *clouders* français, dont il a été établi que certains avaient des pratiques dites « anticoncurrentielles ». Nous souhaitons mettre fin à toutes ces pratiques anticoncurrentielles dont l'auto-préférence qui est une pratique assez courante et également un outil commercial. Elle permet par le biais de crédit *cloud* de capter certains acteurs, notamment les *start-ups*. Cependant, nous avons bien conscience que ce crédit *cloud*, qui est un avantage, une gratuité, proposé à une *start-up*, constitue un vrai atout pour le modèle économique de celle-ci.

Dans le titre III, nous avons également imposé aux *clouders* une obligation de transparence sur la juridiction dans laquelle les services sont sauvegardés : est-ce que c'est sur un territoire français, européen ? Est-ce que c'est extraterritorial ? Les *clouders* sont dorénavant obligés d'indiquer où sont sauvegardées les données et à quelles juridictions leurs services sont soumis.

Nous avons aussi souhaité réguler les frais de transfert. En effet, ces derniers sont parfois si élevés qu'ils peuvent dissuader certaines entreprises de changer d'hébergeur. La loi SREN limite et encadre désormais les frais de transfert d'un opérateur *cloud* vers un autre opérateur *cloud*. C'est-à-dire que dorénavant, quand on veut passer d'un *clouder* vers un autre, tous les aspects techniques de portabilité, d'interopérabilité sont plus faciles à réaliser.

Je salue l'Autorité de Régulation des Communications Électroniques, des Postes et de la distribution de la Presse (Arcep) qui effectue déjà un travail approfondi de protection des données des consommateurs. Avec la loi SREN, qui donne davantage de pouvoir à l'Arcep avec l'ajout d'une compétence supplémentaire, l'ARCEP veillera à ce que les *clouders* soient en conformité avec les dispositions du titre III de la loi SREN.

TF : *Pouvez-vous nous donner votre opinion à propos de la protection de la donnée de santé en France ?*

ALH : La volonté des Français de protéger leurs données médicales est tout à fait légitime, ce sont les données qu'ils souhaitent le plus protéger. En tant que législateur, nous sommes là

pour écouter les Français et modifier la loi si nécessaire en fonction de leurs attentes, surtout lorsque celles-ci sont légitimes.

Les hôpitaux et plus largement les établissements de santé sont de plus en plus des cibles de cyberattaques, ce qui est préoccupant. Ces attaques peuvent bloquer un hôpital durant plusieurs mois et le risque de fuite de données est très grand, pouvant entraîner un risque de chantage ou d'espionnage. Il faut donc y porter une attention toute particulière. Globalement, en France, nous avons un niveau de protection des données de santé assez sécurisé. J'estime que le ministère de la Santé a vraiment une longueur d'avance sur la prise en compte des risques numériques dans leur activité. Cela s'est notamment traduit par un niveau de cybersécurité (nouveau référentiel HDS) imposé aux *clouders* qui est largement supérieur à d'autres ministères qui sauvegardent des données sensibles.

Cependant, nous devons œuvrer à ce que l'ensemble des ministères et des administrations de l'État soient également exemplaires dans la protection et la sauvegarde des données qu'ils produisent, détiennent et exploitent.

Il faut souligner le rôle de l'ANSSI qui travaille à mettre en place une stratégie, des outils et un accompagnement pour mettre en œuvre au plus vite la protection de nos données de santé. Cependant, je pense que sur les données de santé, il faudra aller encore plus loin sur la protection notamment avec une volonté de s'assurer que toutes les données sont sauvegardées sur des *clouds* souverains, français ou européen, en plus d'avoir un niveau de cybersécurité élevé.

TF : *Un certain nombre de textes législatifs sont des transpositions de règlements et de directives européennes. Quelle est la position de la France dans cet univers normatif ?*

ALH : En Europe, les positions sont assez hétérogènes. Cela s'explique notamment par des raisons géographiques et géopolitiques. En France, nous avons une position plus protectrice vis-à-vis des usagers, et donc « plus disant » que beaucoup de nos voisins. La difficulté que nous rencontrons aujourd'hui est de convaincre qu'il faut monter notre niveau de protection.

Mais sur ce sujet, nous n'y arriverons pas tout seuls. Pour réguler l'espace numérique et assumer un haut niveau de cybersécurité, il nous faut travailler avec nos partenaires européens.

TF : *Pouvez-vous nous donner votre regard sur l'écosystème du cloud européen ?*

ALH : Nous sommes en train de le construire. Notre ambition est d'avoir des champions français puis européens. Nous régulons pour protéger notre filière et nos grands opérateurs internationaux. En parallèle, nous avons une politique économique très volontariste pour la filière des *clouders* français. L'idée est que nos acteurs puissent décrocher des marchés au niveau européen. La loi SREN avait aussi cette ambition. C'est-à-dire que plus nous autorisons les extraterritoriaux à faire ce qu'ils veulent sur notre territoire, plus cela affaiblit nos *clouders* français. Un *clouder* français ne sera jamais un champion européen s'il ne se limite qu'au marché français. En ce sens, le travail d'influence que fait l'ANSSI en Europe est essentiel pour le développement de nos *clouders* français.

TF : *Vous avez récemment rendu un rapport et vous évoquiez certaines pistes concernant le portage politique sur la cyberdéfense. Pouvez-vous nous parler de vos propositions ?*

ALH : Concernant les enjeux de cyberdéfense nous venons de voter la loi de programmation militaire et déjà, il est temps de penser à l'après, c'est-à-dire 2030. Il y a des enjeux essentiels comme l'intelligence artificielle, le quantique, l'espace, l'exploration des fonds marins. Nous devons les aborder en équipe avec nos partenaires européens. C'est là que nous pèserons au niveau mondial. Cependant, il n'est pas sérieux d'envisager de confier les données de Défense, sujet régalien par excellence, à un cloud autre que français.

La question de la cyberdéfense est régalienne par définition. Les Armées le font très bien : il y a différents niveaux de sauvegarde des données en fonction de leur niveau de sensibilité. Il faut que l'Europe arrive aussi à faire cela pour les données des citoyens sur une plus grande échelle.

Un autre enjeu est la question de la formation et du recrutement. Nous manquons cruellement de ressources humaines dans ces domaines et il faut passer à la vitesse supérieure. Beaucoup de choses ont été faites déjà, mais il y a seulement 10 % de femmes dans les filières d'ingénieurs, il faut changer cela ! Le numérique est une filière, il existe divers métiers, et il faut les faire connaître. Il faut pouvoir montrer dès le collège que le numérique n'est pas réservé exclusivement aux hommes et que les femmes y ont toute leur place.

Nous devons parallèlement élargir nos capacités juridiques. Nous développons des métiers du numérique, donc il faut vraiment donner plus de moyens à la Justice pour sanctionner ceux qui ne respectent pas la législation et la réglementation.

Enfin, force est de constater que le Code du marché public n'est plus adapté. Si nous ne le changeons pas, nous serons rapidement bloqués dans notre stratégie et la mise en œuvre de nos politiques. Si nous voulons atteindre une souveraineté numérique, il nous faut pouvoir acheter des produits français. Le marché public est clé dans le développement de la filière industrielle française.

TF : *Si vous aviez un message à faire passer à l'École du Numérique, quel serait-il en quelques mots ?*

ALH : Les jeunes ont leur place dans les filières numériques, ils doivent avoir confiance en eux ! En France, nous pouvons être fiers de ce que nous proposons dans les écoles qui dispensent un niveau de formation élevé. Cependant, afin de répondre aux besoins et aux nouveaux défis que posent l'actualité, il nous faut augmenter significativement le nombre de techniciens et d'ingénieurs.

FORUM DU NUMÉRIQUE 2024



**AMIRAL (2S) ARNAUD
COUSTILLIÈRE**

PRÉSIDENT,
PÔLE D'EXCELLENCE
CYBER



Synopia : Pouvez-vous nous donner votre regard, votre vision de la souveraineté en matière de numérique ?

Arnaud Coustillière (AC) : Je n'aime pas le terme de souveraineté, le terme d'autonomie stratégique m'apparaît comme un terme géopolitique intéressant. Ce terme est employé dans la dissuasion nucléaire qui est confrontée à deux immenses puissances : russe d'un côté, américaine de l'autre. Comment, dans cet environnement, pouvait-on créer une force de dissuasion nucléaire, du faible au fort, qui permettrait de retrouver une voie d'autonomie pour défendre les intérêts de la nation ? Le numérique est un peu similaire. Il s'agit d'un environnement très compliqué dans lequel nous devons retrouver une ligne directrice. Par exemple, lorsque nous donnons des données à l'État, ce n'est pas pour qu'il se permette de les partager avec des tiers hors du cadre juridique national ou européen. Le numérique est un domaine où l'on fait beaucoup d'affaires et de lobbying, où les acteurs sont nombreux et divers. Des grandes entreprises, comme Microsoft ou Google, ont quasiment la même représentation qu'un État, aussi bien à l'ONU qu'à l'Union européenne. Quelques parlementaires courageux se sont saisis de ce sujet en France avec la dernière loi « SREN », qui est plutôt encourageante. Il faut donc que chaque organisation ou entreprise définisse sa voie afin de retrouver une part d'autonomie là où cela est nécessaire ; c'est un sujet de gouvernance.

Synopia : Le numérique est une technologie qui possède un aspect cognitif, et vous avez été un des acteurs de la cyberdéfense. Selon vous, quelles sont aujourd'hui les marges de manœuvre de nos démocraties pour évoluer entre la désinformation et les aspects cognitifs de la technologie ?

AC : Le numérique est un espace stratégique où la partie technique a rencontré la partie informationnelle depuis une grosse dizaine d'années. Ces attaques ne sont pas nouvelles mais elles se sont amplifiées depuis les années 2010, notamment via Al-Qaïda et Daech qui ont conceptualisé et déployé la théorie du chaos au niveau numérique. Le cognitif se propage dans la société en utilisant la propagande et en utilisant les outils numériques développés au départ par les démocraties. Pour revenir sur le mot « cybersécurité », il correspond aux opérations de sécurisation et aux opérations défensives. Néanmoins, il existe aussi le volet des opérations offensives qui consiste à rentrer dans un système ennemi pour le perturber, le neutraliser ou le détruire, ou pour faire de l'espionnage. Il existe également aujourd'hui la lutte informationnelle, c'est-à-dire l'utilisation de processus techniques, des trolls, des avatars, des blogs manipulés, des influenceurs... pour manipuler ou changer la façon dont l'ennemi, voire le concurrent vous perçoit ou est perçu. Cette lutte obéit à un certain nombre de règles. Dans une démocratie, il est hors de question d'utiliser les mêmes outils ou méthodes que ceux utilisés par les autocraties. Nous, militaires, sommes soumis au droit des conflits armés : la ruse oui, la perfidie non.

Les armées françaises ont une forte éthique. Le cadre d'action des militaires en uniforme est très clair, contrairement à celui de milices, comme le groupe russe paramilitaire Wagner. Les autocraties vont pouvoir agir en se cachant derrière des bandes de malfrats, des ONG manipulées ou des groupuscules qui sont dirigés ou téléguidés par des services de renseignement d'un État et qui vont conduire des opérations plus ou moins sophistiquées. L'ingérence russe est à l'origine de nombreux coups d'État en Afrique. Face à cela, force est de constater que les démocraties sont assez désarmées. Mais nous savons observer et caractériser pour dénoncer – c'est ce que fait aujourd'hui l'agence française VigiNum, sans pouvoir répondre ou contrer les actions. Un récent rapport du Sénat aborde d'ailleurs le sujet. Nous avons besoin de faire évoluer le cadre juridique d'emploi des forces armées en France pour être mieux à même de répondre à juste niveau. Comme mentionné dans le Livre blanc 2013 au sujet des attaques informatiques techniques contre les intérêts stratégiques, l'État français se doit de répondre avec tous les moyens à sa disposition, juridiques, politiques, diplomatiques, sans s'interdire de recourir aux moyens coercitifs des armées. L'État a su mettre en place les structures et processus ad hoc légalement encadrés ; il lui faut faire de même, à mon avis, pour les attaques informationnelles en provenance d'autres États et dûment caractérisées.

Synopia : *Selon vous, quelles sont les prochaines tendances qui apparaîtront dans ce monde de l'information ?*

AC : Difficile à dire, on voit des technologies de rupture qui se profilent mais le calendrier de leur généralisation est compliqué à prévoir. Le monde évolue vers le quantique, c'est certain. Ce sera une révolution en matière de puissance de calcul et donc de traitement des données. De nombreux domaines vont être concernés, pour le meilleur comme pour le pire, y compris et surtout en capacité de traitement de l'information, parce que le quantique permettra de traiter beaucoup plus rapidement des quantités énormes de données, challengeant au passage tous les systèmes de chiffrement classique.

Ensuite, il y aura probablement une deuxième révolution. Aujourd'hui, les *clouds* sont assez centralisés (les informations sont toutes dans de gros *data centers*) et une tendance forte pousse à mettre de l'intelligence et de la donnée dans les capteurs ou les nœuds des réseaux, c'est la tendance de l'*edge computing*, de la 5G, des SDR (*software defined radio*).

Les *fake news* vont continuer à exploser. Nous ne sommes pas capables de dire aujourd'hui en temps réel si une information vue en ligne est vraie ou fausse. Le rapport à l'information va beaucoup changer, l'IA générative accélère le mouvement. Malheureusement, l'attaquant va beaucoup plus vite que celui qui se défend. C'est un vrai défi pour les démocraties. La capacité d'analyse critique risque de disparaître de plus en plus chez les plus jeunes. Nos parlementaires prennent le taureau par les cornes, essaient de sortir des lois. Mais le monde avance très vite.

Synopia : *Quelle est votre vision de la fuite des cerveaux ?*

AC : Il existe en France une capacité d'innovation et de création qui est extraordinaire. Les grandes entreprises américaines viennent créer des laboratoires en France. Elles voient que nous avons encore des restes en matière d'écoles mathématiques. Pour toutes ces pépites qui se créent, y aura-t-il un espace pour qu'elles puissent se développer en restant françaises ou européennes ? C'est le vrai défi auquel nous sommes confrontés.

Le marché français numérique est trop faible. Il faut arriver à coopérer avec des partenaires sans perdre de vue nos intérêts, notre autonomie stratégique, là où cela est nécessaire.

Synopia : *Selon vous, existe-t-il une confluence du cyber et du spatial actuellement, en raison de l'avènement du new space et de la multiplication des constellations et autres objets spatiaux ?*

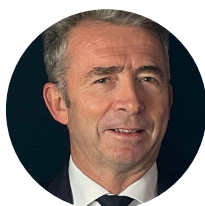
AC : Les satellites et leur environnement sont des objets qui sont importants et marqués par une très forte dynamique et une forme de « démocratisation » avec l'arrivée de nouveaux acteurs en sus des États et grandes organisations. Les nouveaux acteurs qui arrivent dans le champ cyber spatial peuvent être participants ou être victimes d'attaques informatiques. Pour une attaque cyber, il faut un vecteur pour aller du point A au point B. Le point B est le cœur, la cible, ici les satellites et/ou leurs centres de contrôle ou stations terminales. Attaquer un système demande de connaître la façon dont il fonctionne, pour trouver ses maillons faibles... C'est un élément en plus, mais il n'y a pas de convergence ou de vision complète cyber et espace isolée du reste, tout cela est global. Le domaine est en pleine expansion avec un volet cyber dont il doit se saisir, tant de façon technique que fonctionnelle. C'est plus une révolution pour les acteurs du spatial que pour les acteurs cyber.

Synopia : *Si vous aviez un message à faire passer aujourd'hui aux étudiants, quel serait-il ?*

AC : Je dirais que le cyber est un milieu extraordinaire qui doit encore être amélioré, et pour lequel on peut se passionner. C'est un milieu où il faut maîtriser ou comprendre la technologie pour faire de l'opérationnel, un milieu qui touche toutes les activités humaines tant techniques qu'informationnelles. Il y a des pans entiers à développer, des zones d'innovation quasiment sans limites. C'est un milieu où il y a une multitude de métiers qui évoluent constamment. Surtout, c'est un milieu où il y a de nombreuses passerelles et qui bouge en permanence.

C'est l'aventure et le nouveau monde des millenials, voire des plus anciens aussi... Foncez et vivez vos passions.

FORUM DU NUMÉRIQUE 2024



**GÉNÉRAL (2S) CHRISTOPHE
GOMART**
ANCIEN DIRECTEUR,
RENSEIGNEMENT
MILITAIRE



Thierry Fouquet (TF) : *Vous qui avez connu les guerres sous différentes formes, que diriez-vous de cette spécificité de la guerre numérique ?*

Christophe Gomart (CG) : Au-delà de l'influence et des *fake news*, il existe une véritable guerre liée au monde cybernétique aujourd'hui. Nous avons des engins de plus en plus automatisés comme les drones. Par exemple, les Russes sont très puissants en guerre électronique et en particulier dans les techniques de brouillage qu'ils ont mis en place sur le front ukrainien et qui leur ont permis de minimiser le nombre d'attaques de drones. Au-delà de la guerre de haute intensité telle qu'on peut la voir, c'est une véritable guerre numérique qui se joue et qui explique la puissance russe. Ces derniers excellent dans ce domaine d'influence et de propagation de *fake news*.

TF : *Est-ce qu'il y a une bonne coopération entre un organisme d'intérêt vital comme EDF par exemple, l'État et les services de renseignement, dans le domaine cyber ?*

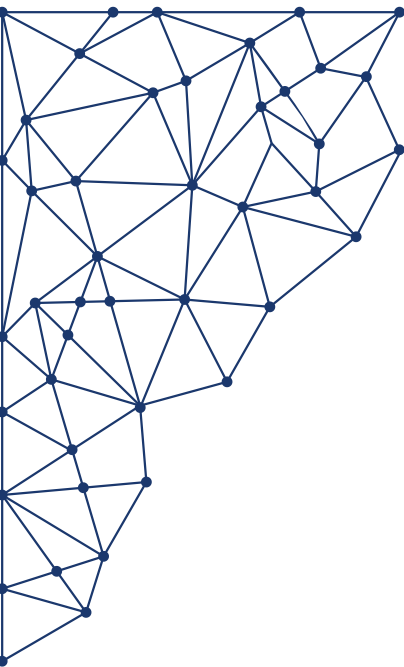
CG : En partie défensive, il est évident que tous les opérateurs d'importance vitale, comme EDF ont un accès direct avec l'ANSSI en termes de protection. De fait, l'ANSSI cherche à former le plus grand nombre d'entreprises et d'individus. Cette formation est essentielle aujourd'hui, en termes de sécurité informatique non seulement au niveau national, mais aussi individuel. Toutefois, on ne peut que constater le manque de coordination générale au sein de l'État en ce qui concerne la défense cyber. Les services travaillent encore de manière trop cloisonnée. Cette gouvernance constitue une véritable vulnérabilité pour notre pays.

TF : *L'humain est-il la première faille lorsqu'on parle de cybersécurité ?*

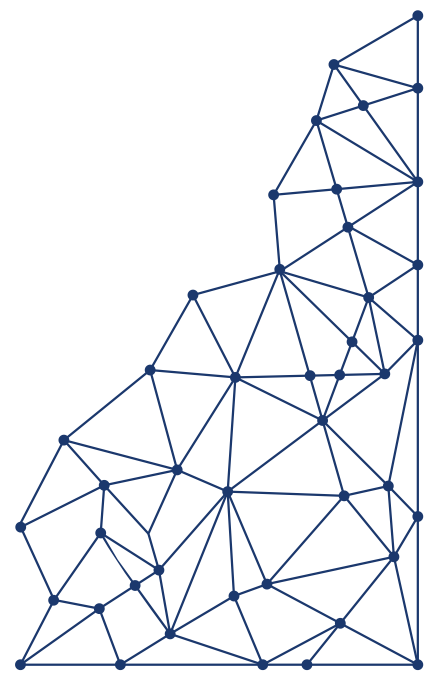
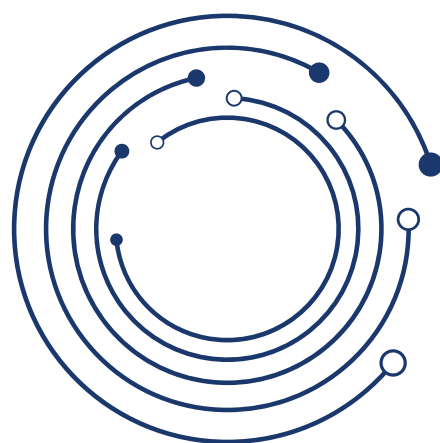
CG : La faiblesse principale de la cybersécurité est l'homme derrière son clavier d'ordinateur. 90 % du renseignement provient de sources ouvertes. Par exemple, nous avons vu une photo prise par un touriste russe, où il se tient devant un système antimissile russe. Ce système a ensuite été détruit par les Ukrainiens. Comment l'ont-ils trouvé ? Les photos que vous prenez avec vos téléphones sont géolocalisées. Cela a permis au service de renseignement ukrainien d'identifier l'emplacement exact du système antimissile et de le bombarder.

TF : *Comment passe-t-on du renseignement militaire régalien normé au renseignement privé, nécessitant des règles, mais pas trop ?*

CG : Je suis pour la liberté. C'est essentiel qu'il y ait des règles en termes de protection des données personnelles. Cependant, les réglementations ne doivent pas empêcher l'innovation, l'inventivité et la créativité : ce sont nos armes pour nous défendre et nous protéger face à la guerre numérique. Or, nous le voyons tous les jours : trop de réglementations nuit à la compétitivité de nos entreprises et cela nous rend davantage vulnérables et dépendants de technologies non souveraines. Il faut donc dessiner une ligne de crête entre sécurité numérique, sécurité nationale et liberté individuelle.



INFRASTRUCTURES NUMÉRIQUES EUROPÉENNES : UN DÉVELOPPEMENT EN COOPÉRATION



FORUM DU NUMÉRIQUE 2024



NICOLAS DEVAUX
ADJOINT AU DIRECTEUR
EN CHARGE DE LA RSE
ET DE LA PRÉPARATION
DE L'AVENIR,
ENEDIS



Thierry Fouquet (TF) : *Linky est un outil de récolte de données. Aujourd'hui, il y a de plus en plus de personnes qui utilisent Linky pour être vertueux dans leur consommation. Comment pourrait-on faire le parallèle entre les réseaux électriques dont vous vous occupez et les réseaux numériques ?*

Nicolas Devaux (ND) : Effectivement, quand nous parlons d'énergie, nous nous disons que le numérique peut paraître assez lointain. Linky est un compteur qui facilite les démarches et permet de mieux maîtriser votre consommation et votre facture d'électricité. Le compteur a évolué, il a été mécanique, électromécanique, puis électronique, et enfin numérique. Linky est aussi un IOT, c'est-à-dire un capteur d'une chaîne numérique qui a été mise en place et qui, comme toute infrastructure numérique, génère énormément de *data*, mais surtout permet à Enedis de promouvoir de nouveaux services et tenter de répondre aux attentes des citoyens en développant de nouveaux usages, comme les véhicules électriques, les énergies renouvelables ou la production décentralisée. Aujourd'hui, les réseaux d'énergie se sont numérisés.

La particularité de Linky est la disposition d'un service public en France. De plus, à travers toutes les coopérations que nous pouvons développer, nous nous rendons compte qu'ensemble nous sommes plus forts. C'est ce que cherche à faire Enedis pour relever les futurs défis qui sont de deux ordres : le premier, c'est le défi de la croissance, que ce soit dans le numérique ou dans l'énergie, c'est-à-dire « comment accueillir tous ces besoins de stockage de données et ces besoins d'énergie ? ». Le second, c'est l'enjeu de résilience. Une résilience, d'abord, face au changement climatique mais aussi face aux grands événements comme les Jeux Olympiques et Paralympiques 2024 à Paris. Pour faire face à ces défis, il faut monter en compétence en éduquant les salariés des entreprises pour qu'ils maîtrisent les outils numériques basiques.

TF : *Vous êtes engagé depuis très longtemps dans une coopération européenne. Expliquez-nous l'intérêt de cette coopération.*

ND : Nous sommes tous solidaires en Europe à travers les interconnexions qui nous relient via les réseaux de transport et les réseaux de distribution. En revanche, pour faire évoluer les réglementations et être plus fort en Europe, Enedis s'est engagé dans un certain nombre d'associations, dont European DSO qui regroupe 35 acteurs de 18 pays différents, pour partager et promouvoir les meilleures pratiques.

Les collaborations sont généralement verticales, se concentrant sur le renforcement entre pairs, notamment en cybersécurité et régulation. Cependant, les collaborations horizontales avec divers partenaires sont cruciales pour créer de la valeur et renforcer la résilience des infrastructures numériques, essentielles dans un monde compétitif.

Cela est particulièrement pertinent pour des régions attractives comme les Hauts-de-France qui bénéficient de leur énergie de qualité et de leur position stratégique en Europe, mais où les infrastructures manquent encore de résilience.

TF : *Les données collectées par le réseau Linky, tout en respectant le RGPD¹, sont partiellement mises en open source pour aider des acteurs, notamment ceux engagés dans des problématiques écologiques. Comment cela se concrétise-t-il numériquement ?*

ND : Le site de l'Observatoire de la Transition Écologique permet d'avoir accès à des données que vous allez pouvoir télécharger et sur lesquelles vous allez pouvoir travailler. Linky a un partenariat depuis quelques années avec Simplon, une ESUS² qui forme des jeunes et des moins jeunes dans le domaine du numérique. Nous collaborons avec eux dans le domaine de l'intelligence artificielle. Pour ceux qui souhaitent se former, l'accès à ces données est comme un eldorado.

Les données collectées et traitées, telles que celles sur l'évolution des véhicules électriques, sont partagées dans le respect des règles, notamment avec les collectivités locales. Ces données aident à cibler les investissements et à rendre les politiques publiques plus efficaces, en identifiant par exemple les zones de précarité énergétique. Ainsi, les zones en développement économique comme Dunkerque nécessitent des données pour une croissance réfléchie. La question cruciale est d'utiliser ces données de manière responsable et efficace, en évitant les erreurs du passé et en limitant l'impact numérique. L'approche souhaitée est de fournir uniquement les données nécessaires, plutôt que de tout donner, pour soutenir une démarche de sobriété numérique et de responsabilité.

TF : *Comment peut-on renforcer la coopération régionale pour gérer l'impact de l'installation de nouveaux data centers ?*

ND : Il est important de travailler en équipe pour que cette réindustrialisation corresponde aussi aux enjeux énergétiques de demain. Nous pouvons dire la même chose de la mobilité électrique, de l'accueil des énergies renouvelables. Aujourd'hui, il y a toujours cette logique de sobriété.

TF : *Est-il possible de travailler de manière plus coopérative avec des grosses entreprises ou des agences publiques ?*

ND : Oui, notamment l'ANSSI³, mais il y a d'autres acteurs. 1 700 salariés de la direction régionale peuvent être un point de fragilité si nous ne les accompagnons pas. Nous nous questionnons sur comment les sensibiliser au quotidien et comment nous installons des pratiques saines. Aujourd'hui, chaque salarié a une tablette sur laquelle il fait ses interventions, à la place du papier. Ce sont forcément des points de connexion vers le réseau que l'on se doit de sécuriser : c'est notre travail. Récemment, nous avons fait un exercice de crise cyber pour préparer les Jeux Olympiques et Paralympiques 2024. Ce sont des sujets sur lesquels nous travaillons comme tous les opérateurs énergétiques.

¹ Règlement général sur la protection des données.

² Entreprise solidaire d'utilité sociale.

³ L'Autorité Nationale de la Sécurité des Systèmes d'Informations

FORUM DU NUMÉRIQUE 2024



ADRIEN FATIBENE

RESPONSABLE
PARTENARIATS ET
DÉVELOPPEMENT,
CAMPUS CYBER



Thierry Fouquet (TF) : *Qu'est-ce qu'un campus cyber, quelle est sa réalité et sa fonction ?*

Adrien Fatibene (AF) : Le Campus Cyber des Hauts-de-France est actif depuis deux ans. Nous sommes un département d'EuraTechnologies qui est l'un des plus gros incubateurs de *start-up* d'Europe sur le digital depuis 2009. Nous avons pour rôle d'accompagner les collectivités régionales, les PME, ETI et les grands groupes, sur les enjeux de la cybersécurité. Nous faisons de la sensibilisation, du diagnostic de premier niveau et de l'exercice de gestion de crise pour ces entreprises et ces collectivités. Nous accompagnons des entrepreneurs régionaux, pour les aider à créer leur entreprise cyber. Nous jouons aussi un rôle fédérateur. Nous avons d'ailleurs sorti une cartographie des acteurs de la cybersécurité en région où nous avons référencé environ 150 entreprises « *pure players* » ou fournisseurs de services.

TF : *EuraTechnologies est une idée de coopération privée et publique, a-t-elle été voulue dès le début dans ce campus ?*

AF : Cette idée est au cœur même de notre modèle. Sur l'actionnariat d'EuraTechnologies, nous avons des actionnaires publics et privés. Le digital est très transversal, la cybersécurité aussi. Dans les Hauts-de-France, nous avons un écosystème intersectoriel qui est très riche et constitué aujourd'hui de pôles de compétitivité, de parcs d'innovation, de pôles d'excellence, d'incubateurs sur différentes thématiques. Nous venons travailler avec l'ensemble de ces acteurs parapublics et privés pour essayer de booster la dynamique territoriale.

TF : *Comment convaincre les entreprises d'adopter une approche coopérative régionale en matière de cybersécurité plutôt que nationale ?*

AF : Il y a un tissu local qui est très riche, avec des solutions très pertinentes. Le campus cherche à être le plus objectif et nous ne cherchons pas à privilégier un acteur plutôt qu'un autre. Le campus part toujours de leurs besoins et nous essayons de les accompagner. Cela commence par un diagnostic, puis une sensibilisation. Petit à petit, nous essayons de les amener vers un mode de réflexion, un schéma de pensée qui va automatiquement les conduire vers les bonnes solutions et les bonnes entreprises.

TF : *Comment former des talents locaux et les convaincre de rester en région ?*

AF : Nous manquons cruellement de talents : des ingénieurs, mais aussi des *business developers*. L'une des caractéristiques et des forces de la région est son maillage territorial, avec des écoles de qualité qui viennent apporter des solutions à des étudiants, mais aussi, *in fine*, à des entreprises. Ce qui me frappe dans cette région, c'est l'écoute et la relation entre les écoles et le monde professionnel sur les besoins de demain, afin de venir apporter une réponse utile. Cependant le défi dans les années à venir sera de réussir à former suffisamment de talents dans le domaine du cyber.

FORUM DU NUMÉRIQUE 2024



HERVÉ FEVRIER

PRÉSIDENT,
LANDELLES CONSULTING



Thierry Fouquet (TF) : *Hervé Février, vous êtes un des grands spécialistes mondiaux des câbles sous-marins. Vous avez travaillé pendant sept ans chez Facebook et dix-sept ans chez Alcatel. Pouvez-vous expliquer les enjeux géopolitiques actuels de ces câbles sous-marins ? Qui sont les opérateurs ? Et enfin pouvez-vous nous donner quelques indicateurs sur le nombre de kilomètres de câbles ?*

Hervé Février (HF) : Le réseau sous-marin de câbles de télécommunications représente près de 1,4 million de kilomètres sous tous les océans. Du point de vue des acteurs, historiquement, les grands opérateurs télécoms – AT&T aux États-Unis, BT en Angleterre, France Télécom en France – ont créé l’embryon de ce réseau de câbles optiques de grande capacité à partir des années 1985. Aujourd’hui, les principaux acteurs sont Google et Meta. Mais parallèlement, ils permettent à d’autres opérateurs d’avoir accès à ces câbles (par exemple : Orange, Vodafone...). Ces deux sociétés américaines ont fait exploser le marché des câbles sous-marins. Le trafic télécom international est fourni à plus de 98 % par ce réseau de câbles sous-marins.

Du point de vue des fournisseurs de câbles, il y a trois acteurs principaux. Un acteur américain, SubCom, un acteur européen, Alcatel Submarine Networks (dont une usine est à Calais et une autre usine à Greenwich), et un acteur japonais, NEC. Il y a une quinzaine d’années, la Chine a planifié sa pénétration dans le marché en créant différentes sociétés pour le marché intérieur et extérieur. Aujourd’hui, HMN Tech détient à peu près 15 % du marché, essentiellement par limitation géopolitique, mais est désormais un acteur à part entière maîtrisant l’ensemble de ce métier.

TF : *Aujourd’hui le marché des câbles sous-marins est peu discuté car il est relativement petit, environ 2 milliards d’euros par an, mais aussi parce que ces infrastructures ne sont pas visibles directement. Nous constatons que les infrastructures des câbles sous-marins sont souvent moins sécurisées, à la différence des data centers. L’Europe commence à se rendre compte de l’importance de ces câbles. Quel est le constat que vous pouvez faire de la situation actuelle ?*

HF : L’Europe, selon moi, a réalisé l’importance des câbles au démarrage du conflit en Ukraine en février 2022. Malheureusement nous avons la mémoire courte. Rappelons-nous que lorsque l’Angleterre s’est engagée dans la Seconde Guerre mondiale, la première chose qu’ils ont fait, c’était de couper tous les câbles télégraphiques arrivant en Allemagne. Cette menace ou cette importance des réseaux de communication est largement connue dans le monde militaire et dans la défense. Aujourd’hui, en France, je ne pense pas que les infrastructures qui s’occupent des câbles sous-marins soient au niveau de cybersécurité requis pour assurer les échanges de données dans les câbles sous-marins.

L'Europe est très fragmentée sur ce sujet, la réflexion se fait pays par pays. Nous avons vu des pays européens s'intéresser au sujet en y voyant une opportunité économique : l'Irlande et le Danemark ont attiré un certain nombre de câbles, ainsi que des gros *data centers*, etc. Du point de vue des grands clients, l'Europe est aussi très fragmentée, non seulement en termes d'opportunités, mais aussi en termes de législations. Elles sont très volumineuses et très différentes les unes des autres. Il est essentiel de développer une stratégie commune, européenne, sur ces enjeux.

TF : *Est-il légitime de craindre que les câbles sous-marins ne soient pas détenus par des puissances régaliennes, des États, ou l'UE, et que la majorité des flux viennent de câbles appartenant aux grands opérateurs américains ?*

HF : Oui, cette crainte est légitime. La majorité des câbles sous-marins sont aujourd'hui possédés ou contrôlés par de grandes entreprises privées américaines, comme Google ou Meta, plutôt que par des États ou des entités publiques. Cela pose des enjeux de souveraineté et de sécurité stratégique pour l'Europe. Il est donc crucial que l'Union européenne développe une véritable stratégie dans ce domaine, en renforçant sa coopération avec les acteurs du marché tout en veillant à préserver ses intérêts. À titre de comparaison, les États-Unis imposent des conditions strictes à tout câble qui atterrit sur leur territoire, illustrant une maîtrise politique et géopolitique que l'Europe doit chercher à égaler.

TF : *Il faudrait donc aller vers de la coopération intelligente, régulée, claire, transparente ?*

HF : Un câble sous-marin appartient aujourd'hui aux propriétaires des paires de fibres optiques présentes dans le câble (principalement les sociétés fournisseurs de contenu Internet – les GAFAM). Participer, coopérer pour avoir un réseau souverain et résilient est donc en effet très important.

TF : *Dans les années 1980, nous étions dans la télématique, alors que sortait le web partout dans le monde. Il y a aussi ce problème qui est que les opérateurs télécoms européens, au moment où il aurait fallu investir, investissaient des sommes misérables par rapport aux Américains. Qu'en pensez-vous ?*

HF : Du point de vue des câbles sous-marins, ce sont les besoins de Google et Meta qui ont créé la nécessité de les produire. C'est juste un coût énorme pour ces deux opérateurs, rien d'autre. Il n'y a aucune monétisation de la capacité de transport optique. Je prends l'exemple de l'Atlantique. Avant que Google ne commence à travailler sur les câbles sous-marins, les quinze années précédentes, il n'y avait pas eu un seul consortium d'opérateurs télécoms européens et américains qui avait pu faire un nouveau câble télécom. C'est uniquement par le besoin et la quantité de données transportées que de nouveaux câbles ont été créés. Aujourd'hui, les budgets de CAPEX des opérateurs télécoms européens vont vers les infrastructures pour les mobiles (comme la 5G), et ceux des fournisseurs de contenu Internet vont vers les réseaux internationaux permettant de connecter en un seul réseau leurs *data centers* et les principaux points de *peering* (points d'interconnexions entre les réseaux des opérateurs de télécom et ceux des fournisseurs de contenu Internet) dans chaque pays (une grande partie de ce budget est allouée aux réseaux sous-marins).

FORUM DU NUMÉRIQUE 2024



CÉLINE HELLER
DIRECTRICE
COMMERCIALE EUROPE,
SOVERAINETÉ
NUMÉRIQUE,
GOOGLE CLOUD



Thierry Fouquet (TF) : *Comment pouvons-nous mettre souveraineté et Google dans la même phrase ?*

Céline Heller (CH) : L'objectif aujourd'hui est de collaborer entre les différents acteurs pour assurer à l'Europe une autonomie numérique et stratégique, tout en pouvant bénéficier de la puissance existante des *cloud* programmeurs américains, mais pas seulement. Il faut aussi assurer des besoins de régulation, des besoins politiques et des besoins d'usage, ce dont Google Cloud est conscient.

L'entreprise a pris la décision d'investir massivement dans des programmes de coopération avec des acteurs européens. Nous parlons de Thales en France, TSI en Allemagne, Indra en Espagne, TIM Telecom Italia en Italie. L'Europe reste une plaque géographique qui est importante. L'objectif de tous ces programmes d'investissement est de permettre aux utilisateurs locaux, que ce soient des entreprises ou des utilisateurs individuels, de bénéficier de la puissance existante du *cloud* de Google, tout en respectant les prérequis et les prérogatives européennes locales. Ces prérequis et prérogatives peuvent être très variables d'un pays à un autre au sein même de l'UE car personne n'a la même vision et les mêmes besoins.

Pour autant, nous ne pouvons pas demander à des entreprises internationales basées en France d'avoir des données localisées uniquement en France, parce que cela viendrait impacter leur marché. Ça a été le cas des entreprises allemandes qui ont joué un rôle clé en revendiquant une plus grande autonomie sur la gestion de leurs données. Elles ont cherché à savoir précisément comment et par qui leurs données sont gérées. Cela leur a permis de tirer parti des technologies performantes et innovantes, tout en s'assurant que les données restent sous contrôle européen, si nécessaire. Cette approche est essentielle pour que les entreprises et le secteur public en Europe puissent continuer à innover et à offrir des services publics modernes.

TF : *Vous avez souvent évoqué le mot « confiance ». Certains disent que les données doivent être protégées et que Google n'est pas digne de confiance. Expliquez-nous ce que vous mettez derrière cette confiance.*

CH : La confiance ne se déclare pas, elle se gagne dans la durée. Quand on est salarié d'une entreprise américaine tout en étant français, c'est quelque chose dont on se rend bien compte, même dans le quotidien à titre personnel. L'ambition française est que Google contribue avec Thales dans le cadre d'une *joint-venture* S3NS, à créer un *cloud* qui sera labellisé par l'ANSSI pour devenir le *cloud* de confiance.

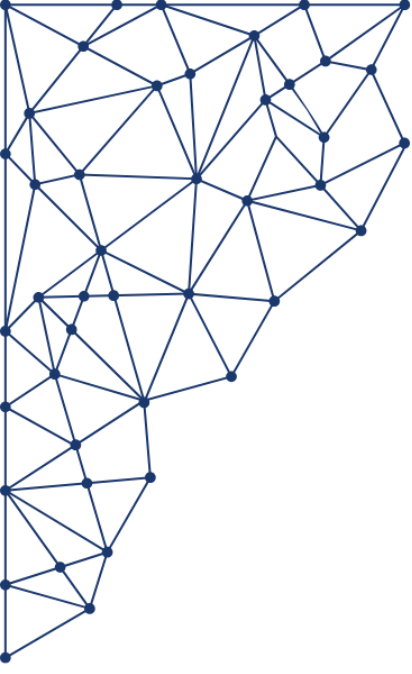
Ce projet est très complexe et repose sur un travail de fond depuis plus de deux ans et demi entre les ingénieurs de Google et Thales pour garantir que la technologie de Google soit opérable par Thales, conforme aux réglementations françaises, et efficace pour tous. Le point commun le plus fort entre Thales et Google est l'obsession permanente de la sécurité.

TF : *La particularité de notre marché est la réglementation qui ne fait que progresser dans le respect du citoyen, de l'utilisateur. Comment intégrez-vous ce nouveau cadre ?*

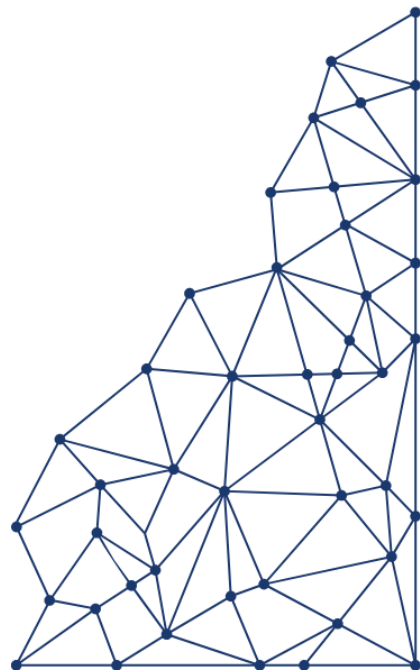
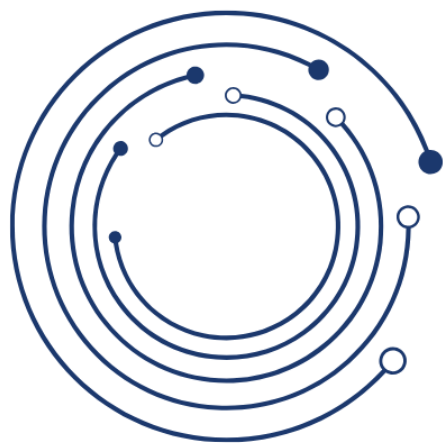
CH : L'ambition est de nous coordonner mais aussi de collaborer malgré une Europe très fragmentée. C'est notre rôle de nous adapter, de faire en sorte que les lois soient respectées d'un pays à un autre spécialement dans un territoire européen compliqué, mais qui a un grand marché.

TF : *Vous affirmez qu'il faut arrêter de faire le combat de la dette technologique permanente. La coopération est-elle le seul moyen de rattraper ce retard ?*

CH : Absolument. Prenons le sujet de l'IA générative. C'est une transformation et une révolution majeure dont nous ne voyons que le début. La France, grâce à toutes ses écoles et ses formations, a un gisement de cerveaux disponibles et de personnes qui peuvent être parmi les meilleurs au monde. Quand nous regardons qui sont les décideurs dans les organisations globales autour de l'IA, il y a énormément de Français. L'objectif est donc de regarder vers le futur et de bénéficier à la fois de ce qui existe au niveau technologique, mais également au niveau de la ressource humaine sur le territoire français. La France a des atouts majeurs et ce retard peut être rattrapé par la coopération, ce qui est porteur d'espoir.



INNOVATION : LA MAÎTRISE DU DESTIN NUMÉRIQUE EUROPÉEN



FORUM DU NUMÉRIQUE 2024



STEVEN BOURGEOIS

DIRECTOR OF
GOVERNMENTS, PUBLIC
SECTOR, EUROPEAN
AFFAIRS,
EURATECHNOLOGIES



Thierry Fouquet (TF) : Pouvez-vous nous décrire EuraTechnologies, son dimensionnement, ses métiers principaux et les enjeux auxquels vous êtes confrontés aujourd'hui ?

Steven Bourgeois (SB) : EuraTechnologies est un incubateur et un hub de startups et d'innovation dont l'objectif est de faire émerger les champions de la tech européenne de demain avec un impact positif et durable sur le territoire, notamment en termes d'emplois. Chaque année, nous accompagnons plus de 200 projets en incubation ou en accélération, sur nos 5 sites répartis dans 4 villes : Lille, Roubaix, Willems et Saint-Quentin. Au total, nous avons permis la création de plus de 8 000 emplois au cours des 15 dernières années via nos programmes d'incubation et d'accélération, et ce sont plus de 6 000 salariés qui aujourd'hui travaillent dans le quartier d'affaires d'EuraTechnologies. Ces résultats nous ont permis d'être classé premier hub de startups en France par le *Financial Times*⁴ en 2024, ce qui est une reconnaissance sans égal.

Ce qui nous donne notre singularité, c'est la spécificité de notre actionnariat, incarnant un modèle de coopération public-privé réussi. EuraTechnologies a en effet été lancé en 2009 par une initiative publique de la Métropole Européenne de Lille, la Région des Hauts-de-France et la Ville de Lille, notamment sous l'impulsion de Pierre de Saintignon, qui était alors premier adjoint à la mairie de Lille. Puis après une première ouverture de capital en 2017, nous avons accueilli en 2022 de nouvelles structures comme l'AFM (Association Famille Mulliez), Entreprises & Cités, EDF, la Caisse des Dépôts pour une levée de fonds de 24 millions d'euros. Cette ouverture de capital était nécessaire car dans un monde post-COVID, il nous a fallu repenser notre modèle d'accompagnement des startups et notre modèle locatif pour être davantage attractif, notamment dans un marché devenu ultra concurrentiel avec une multiplication par cinq du nombre d'incubateurs en cinq ans. Adapter notre stratégie passe par davantage d'investissement, et davantage de lignes de services pour les startups. Nous avons lancé de nouveaux projets différenciants comme le Campus Cyber Hauts-de-France Lille Métropole qui a vu le jour en 2022, opéré par EuraTechnologies, dont la mission est de sécuriser le territoire et d'accompagner les jeunes pousses cyber de la région, ainsi que les PME, entreprises et collectivités locales.

TF : Est-ce que l'un des enjeux progressifs d'EuraTechnologies n'est pas de passer de la création de la start-up à l'idée de faciliter l'émergence d'entreprises de taille internationale ? Est-ce que l'avenir des entreprises que vous incubez et que vous accompagnez est forcément au minimum à l'échelle européenne ?

⁴ <https://www.ft.com/content/6b6f48df-f4e8-4c64-b697-14fa64ad03ef>

SB : Nous accompagnons nos porteurs de projets aux différents stades de leur développement. Tout d'abord via l'incubation, nous accompagnons l'entrepreneur qui a une idée pour l'aider à créer son entreprise, tester le marché, développer sa solution, acquérir ses premiers clients. Ensuite, nous accompagnons des startups plus matures via un programme d'accélération afin de leur permettre de passer à l'échelle. Cela passe par l'accompagnement au lancement de leur produit sur d'autres marchés, s'étendre à l'international, et lever des fonds plus conséquents pour soutenir leur phase de développement et d'hyper-croissance. Nous avons en effet pour ambition de permettre aux startups de se développer à l'échelle européenne.

Toutefois, l'un des enjeux actuels pour les startups est l'accès au financement, avec un marché de l'investissement en berne qui s'est régulé par rapport à la période faste post-COVID. Entre 2022 et 2023, les levées de fonds des startups ont connu une baisse de 38 % en France pour un nombre quasi-constant de deals, et la tendance était généralisée dans le monde et en Europe. En Europe, nous pâtissons d'un manque de fonds d'investissement capables d'investir massivement en *late stage*, à l'inverse des États-Unis qui disposent de fonds aux capacités colossales qui investissent dans les fleurons européens.

TF : *Sentez-vous que l'Union européenne cherche à favoriser des actions communes pour accompagner les start-ups ?*

SB : Travailler de manière collaborative à l'échelle européenne avec d'autres acteurs de l'écosystème startup est indispensable pour développer une approche commune de l'accompagnement, même si aujourd'hui, la plupart des initiatives sont nationales. EuraTechnologies fait partie du réseau de l'*European Startup Network* (ESN), avec qui nous coopérons pour proposer des solutions faveurs de l'écosystème auprès de la Commission européenne. Faire partie de l'ESN nous permet d'une part d'avoir des liens avec des acteurs similaires de la *tech* dans toute l'Europe, et d'autre part, de participer au programme *EIC⁵ Tech to Market (T2M) Entrepreneurship* au titre de l'EISMEA (*European Innovation Council and SMEs Executive Agency*). Ce projet européen vise à accompagner des chercheurs innovants en *deeptech* lauréats des programmes *EIC Pathfinder* et *EIC Transition*.

Ce type d'initiative est nécessaire pour développer des scale-ups, mais pas suffisant. L'accès au financement pour le développement de technologies et pour préserver notre souveraineté financière est crucial. La Commission doit poursuivre l'investissement en R&D et la mise à disposition de fonds dans des secteurs stratégiques. C'est primordial car nos startups sont extrêmement prisées par des fonds hors-Europe notamment grâce à la qualité de notre main-d'œuvre.

TF : *Quand nous voyons la différence de levée de fonds entre les Américains et les Européens, nous observons que nous ne disposons pas des mêmes ressources économiques. Comment appréhendez-vous cette différence ?*

SB : Tout d'abord, il s'agit d'une question de capacité financière, non pas sur le volume de financement, mais plutôt sur la structuration.

⁵ EIC : European Innovation Council : Conseil européen de l'innovation.

En Europe, n'avons pas d'union des marchés de capitaux et il serait intéressant de développer des fonds d'investissement transnationaux pouvant investir dans les meilleures startups européennes. Cet investissement permettrait d'accompagner nos startups en *late stage*.

Il s'agit également d'une question de source de financement, car pour investir, il faut trouver les fonds. En Europe, nous devons davantage mobiliser et flécher les fonds européens d'assurance et de pension vers les investissements en Venture Capital (VC). Aux États-Unis, c'est la source principale des investissements en VC, alors qu'en Europe, ce n'est que la 5^{ème} source des fonds de capital-risque.

Il est toutefois important de souligner que la Commission européenne a pris le sujet du financement à bras-le-corps en développant son propre fonds d'investissement en capitaux propres auprès des *start-ups*. Depuis 2019, ce sont ainsi 10 milliards d'euros qui sont investis dans des *scaleups* et dans des secteurs stratégiques tels que la *deeptech*, la *greentech*, la santé ou encore la cybersécurité. En France, nous pouvons être très fiers de Bpifrance qui est le premier investisseur dans les startups et qui nous est envié partout dans le monde.

Néanmoins, ces initiatives sont publiques et il s'agit de flécher davantage les fonds européens privés vers le *late stage*.

FORUM DU NUMÉRIQUE 2024



ANNE DUBOSCQ

DIRECTRICE DES AFFAIRES
PUBLIQUES,
OVHcloud



Thierry Fouquet (TF) : *Vous êtes directrice des affaires publiques d'OVHcloud. Comment présenteriez-vous votre entreprise ?*

Anne Duboscq (AD) : OVHcloud est un opérateur de *cloud* qui, depuis sa création, prône la liberté de choix des utilisateurs dans la technologie. La question est de savoir comment faire pour garantir la liberté de choix des services numériques que nous utilisons et la manière dont nous allons gérer nos données.

C'est pour cela qu'OVHcloud a fait de la liberté de choix son combat principal. Cela s'incarne par des valeurs comme la confiance. En effet quand nous transmettons ces données, nous nous assurons qu'elles ne soient pas transférées ou vendues. Notre deuxième valeur est la transparence car les utilisateurs cherchent à maîtriser ce qui va se passer avec ces services et la troisième porte sur la responsabilité en matière environnementale qui est aussi un sujet extrêmement important dans notre secteur. De manière plus générale, nous avons une vraie volonté de montrer qu'en Europe, nous pouvons avoir des services numériques performants qui représentent une troisième voie entre l'Asie et les États-Unis.

TF : *OVHcloud continue de se développer. Dans combien de pays êtes-vous présents ?*

AD : Nous sommes présents dans 140 pays avec 3 000 collaborateurs et près d'un milliard d'euros de chiffre d'affaires. OVHcloud est présent aux États-Unis, où nous réalisons environ 30 % de croissance et où nous nous différencions grâce à la qualité de service, la performance et un prix compétitif.

Il est intéressant de noter qu'aux États-Unis, il n'y a pas de question sur le niveau de performance des services d'OVHcloud. Là où parfois en Europe, nous avons tendance à penser que les services européens vont être moins bien, moins intéressants, moins performants. Aux États-Unis, ce n'est pas la question. Un développeur ou un client va regarder deux services comparables, et ce qu'il peut obtenir. Nous sommes également un *pure player*, c'est-à-dire que nous nous concentrons exclusivement sur les services *cloud* et donc il n'y a pas de risque de concurrence avec nos clients dans d'autres domaines, comme l'e-commerce.

TF : *Avez-vous un enjeu de taille que vous avez identifié dans le monde ou bien la clé principale est-elle de garder de la qualité et un prix concurrentiel ?*

AD : Nous avons trois principaux différenciants : le ratio prix performance, la protection des données, et l'empreinte environnementale.

TF : *Vous êtes une entreprise privée. Vous n'êtes pas responsable du destin numérique de l'Europe. Néanmoins, nous sentons dans votre discours que vous y êtes attachée. Vous parliez en introduction de cette troisième voie. Pourquoi est-ce important ? Et comment faire pour que vous soyez un acteur qui participe à conforter ce destin européen du numérique ?*

AD : La responsabilité est collective et si nous voulons vraiment reprendre la main sur le destin numérique en Europe, nous devons mener une action coordonnée :

- du côté des utilisateurs, c'est-à-dire en prenant conscience des outils numériques qu'ils utilisent et des données qui vont transiter par le biais de ces services, et en faisant des choix éclairés ;
- et du côté des industriels, en proposant ce type de services.

Enfin, il y a également une responsabilité politique : nous avons besoin de mener des politiques publiques ambitieuses, notamment pour déverrouiller le marché.

Ce n'est que de concert que l'on arrivera à assurer une véritable liberté de choix et reprendre la main sur le destin numérique.

TF : *Quel regard portez-vous sur les dispositifs de financement européens en particulier ?*

AD : L'argent est un enjeu pour se développer. En revanche, la question du financement et de la subvention n'est pas censée être la réponse à tout. Bien au contraire, je pense que l'accès aux capitaux est probablement un enjeu qui va bien au-delà de chercher simplement à avoir des subventions qui, en plus, très souvent en Europe, vont être saupoudrées entre différents projets. Elles ne vont pas représenter des enveloppes suffisantes pour atteindre une taille critique ou obtenir l'impact nécessaire et attendu. Aujourd'hui, si nous voulons vraiment reprendre en main ce destin numérique, nous devons répondre à l'enjeu de financement, mais également à l'enjeu de talent, de formation. Enfin, il existe un enjeu de politique publique et de régulation en matière de commande publique et un enjeu de recherche. Je pense que les acteurs du numérique sont aujourd'hui des champions mondiaux ayant bénéficié d'un environnement favorable dans leur pays d'origine et c'est ce qui leur a permis de se développer.

TF : *Le cadre de régulation qui se renforce est évoqué par certains : est-ce que vous pouvez soutenir certaines réglementations ?*

AD : La question qui se pose est : « Quelles sont les règles du jeu qui s'appliquent dans le Cloud ? ». Pendant longtemps, il n'y en a pas eu. C'est normal. C'est une technologie qui est en train d'émerger et d'évoluer. Nous sommes plutôt favorables à ce que des règles soient fixées. Quand il s'agit de rééquilibrer la concurrence sur le marché, de mieux former les utilisateurs en matière de protection des données, et d'avoir un cap ambitieux en matière d'empreinte environnementale, nous ne pouvons que nous en féliciter.

FORUM DU NUMÉRIQUE 2024



LÉO HAMON

RESPONSABLE DES
AFFAIRES PUBLIQUES,
IBM



Thierry Fouquet (TF) : *En tant que grand opérateur, la souveraineté européenne est-elle seulement un enjeu économique ?*

Léo Hamon (LH) : IBM existe depuis plus de 110 ans, nous sommes un industriel de la technologie. Notre métier est de concevoir des technologies et de les rendre les plus performantes possibles. Nous avons une division qui s'appelle *IBM Research*, qui a plus de 3 000 chercheurs, plusieurs prix Nobel, et est une des plus grandes organisations de recherche au monde.

Nous avons eu le temps de voir la réglementation évoluer en France et nous nous sommes toujours adaptés. Pour nous, ce n'est pas une contrainte. Nous avons annoncé au sommet *Choose France* un nouvel investissement sur le quantique. Nous allons recruter 50 personnes, des chercheurs, des ingénieurs, d'ici un an. Nous allons les placer dans notre centre de recherche à Saclay et ils vont travailler avec des chercheurs du CNRS, d'Inria, et de l'Université Paris-Saclay.

TF : *Aujourd'hui deux choix s'imposent à nous : soit nous nous passons d'IBM sur le domaine quantique quitte à être en retard, soit nous essayons d'établir des liens et des contrats de confiance avec les sociétés américaines pour rester au contact des nouvelles technologies. Comment percevez-vous les choses de ce point de vue-là ?*

LH : *IBM Research* a une vision sur le quantique et une ambition qui est de construire des supercalculateurs hybrides quantiques HPC (*high performance calculator*), et intelligence artificielle à l'horizon 2033. L'objectif est d'avoir un ordinateur opérationnel dans moins de dix ans. Pour cela, nous nous sommes associés avec des acteurs japonais de la recherche comme l'Université de Tokyo et Fujitsu, qui fait du calcul hautes performances, du quantique, et qui est concurrent d'IBM. Nous avons envoyé des chercheurs là-bas et aujourd'hui, nous sommes en train de travailler sur une feuille de route à dix ans pour construire ce supercalculateur. L'objectif est de collaborer, de travailler en écosystème, et ce n'est que grâce à cet échange que l'on arrivera à cette ambition commune de mettre ce supercalculateur sur le marché dans une dizaine d'années.

TF : *Vous considérez donc la coopération comme essentielle pour le développement de vos structures et des futurs écosystèmes comme le quantique. Pensez-vous que cette coopération soit possible avec des acteurs ayant des règles éthiques et des objectifs similaires ?*

LH : Je pense que nous ne pouvons pas nous en passer. Nous le voyons aujourd'hui, nous sommes dans un monde d'interdépendances. C'est ce qui structure la relation entre les États-Unis et la Chine. Le numérique est partout, infuse partout, il est transversal et donc il y a de l'interdépendance. La question de l'autarcie est complètement illusoire pour l'Europe.

En revanche, il y a des retards européens qui sont structurels. Comment l'Europe s'insère-t-elle dans cette interdépendance, de manière choisie et pas subie, ce qui est pour le moment un peu le problème ? Le mot écosystème est très utilisé pour le numérique. Il faut créer des écosystèmes d'innovation qui lient notre recherche publique avec des *start-ups* qui, ensuite, vont prendre ces innovations *deep tech*, des technologies de rupture, et vont les mettre sur le marché. Nous avons évoqué les marchés de capitaux. Il faut qu'il y ait des VC (*venture capital*) qui, ensuite, financent ces *start-ups* pour qu'elles grossissent. Il faut aussi qu'il y ait des grands groupes. Les trois cofondateurs de Mistral ont fait leur thèse Cifre chez Meta et chez Google. Aujourd'hui, Mistral est une pépite française. Peut-être que la prochaine pépite française du quantique sortira d'une thèse du lab d'IBM à Saclay.

TF : *Vous sentez-vous suffisamment intégrés dans la co-construction du cadre réglementaire ?*

LH : Oui, nous discutons et nous sommes écoutés. Nous ne sommes pas forcément toujours entendus. Nous avons tendance à en faire trop en Europe et à surtransposer en France. C'est un vrai problème. Pour nous aussi, c'est beaucoup d'investissement de se mettre en conformité avec ces lois. Pour une PME ou une *start-up* européenne, c'est très lourd. En revanche, il y a des réglementations européennes absolument nécessaires car il faut que nous gardions une liberté de choix pour les organisations, qu'elles soient publiques ou privées. Il faut qu'elles puissent vraiment choisir les partenaires avec lesquels elles travaillent.

Mais pour que cette liberté de choix soit réelle, il faut qu'en face, il y ait une offre qui soit diversifiée et donc la présence d'un marché sur lequel une libre concurrence s'exerce. Aujourd'hui, sur certains segments de la technologie, nous avons des acteurs qui sont en situation d'oligopole, qui verrouillent le marché. Les clients, en réalité, n'ont pas de liberté de choix.

FORUM DU NUMÉRIQUE 2024



SIMON MARÉCHAL
RESPONSABLE RÉGIONAL
HAUTS-DE-FRANCE,
ASSOCIATION EMMAÛS
CONNECT



Thierry Fouquet (TF) : *Comment définiriez-vous Emmaüs Connect ?*

Simon Maréchal (SM) : Notre métier chez Emmaüs Connect est l'inclusion numérique. Nous faisons partie de la grande famille du mouvement Emmaüs, fondé il y a 75 ans par l'Abbé Pierre. Emmaüs Connect existe depuis dix ans, suite à l'accroissement de la digitalisation et de la dématérialisation qui est venu bouleverser nos vies. Aujourd'hui, tout le monde est concerné par le numérique dans sa vie quotidienne et pour un certain nombre de personnes, il existe des difficultés d'usage ou d'accès au numérique. Notre travail consiste à proposer un ensemble de services plutôt à destination de personnes fragiles comme les personnes non diplômées et éloignées de l'emploi. De plus, aujourd'hui ce n'est pas seulement un sujet générationnel.

Le 15 mai 2024, le baromètre du numérique publié par l'Arcep, l'Arcom, et le ministère de l'Économie indique que 78 % des Français considèrent qu'internet est nécessaire pour être intégré dans la société. Il y a une prise de conscience de la population, de manière générale, qu'internet et plus largement le numérique est partout et qu'aujourd'hui, nous devons nous en servir. Dans le même temps, 25 % des Français ne maîtrisent pas le numérique, c'est un chiffre conséquent. Un autre chiffre, encore plus inquiétant est qu'un Français sur deux limite son usage du numérique soit en raison de difficultés d'accès, lié aux coûts des équipements et aux coûts de la connexion et soit en raison de difficultés d'usage. Pour certains réfractaires, le numérique n'est pas du tout un sujet et ils ne veulent pas en entendre parler.

TF : *Pouvez-vous nous décrire vos actions faites pendant le Covid et juste après le Covid, et en particulier par rapport à ce déficit de matériel ?*

SM : Lors de la crise Covid, certaines familles n'ont pas eu d'accès à une connexion internet, et avec l'association Emmaüs Connect, nous avons décidé grâce aux dons, d'acheminer les équipements auprès de ces personnes. Lors de cette période, 45 000 équipements ont été distribués. Ce projet LaCollecte.tech, est aujourd'hui une filière de réemploi solidaire des équipements numériques que nous collectons localement, auprès des citoyens ou des entreprises pour leur donner une seconde vie. Les acteurs avec qui nous travaillons sont des acteurs qui sont dans le champ de l'insertion des personnes éloignées de l'emploi ou handicapées que nous remettons à l'emploi et qui vont reconditionner ou recycler les équipements. Ces produits sont ensuite redistribués au niveau de la Région Hauts-de-France.

Ce type de filière locale contribue à assurer une souveraineté en termes d'accessibilité aux gisements d'équipements numériques, dont la fabrication dépend aujourd'hui essentiellement de pays étrangers, afin de les réemployer dans une logique d'économie circulaire pour nos propres besoins. Aujourd'hui, il y a une prise de conscience au niveau de l'État sur cet enjeu d'inclusion numérique, de souveraineté numérique mais aussi de dépendances des matériaux qui ne sont pas produits en Europe.

FORUM DU NUMÉRIQUE 2024



HUGO WEBER

VP, CORPORATE AFFAIRS &
IMPACT,
MIRAKL



Thierry Fouquet (TF) : *Vous faites partie des entreprises qu'on cite souvent comme des exemples d'entreprises françaises capables de se développer à l'international. Pouvez-vous nous rappeler le métier de Mirakl ?*

Hugo Weber (HW) : Mirakl apporte une solution technologique qui va permettre au client d'être intégré sur des *marketplaces* autre que leur site principal et de pouvoir aussi rajouter des produits qui ne sont pas fabriqués par eux. Par exemple sur le site internet de Decathlon, vous allez aussi retrouver des produits d'autres marques, qui sont des PME, des ETI françaises. C'est cette mécanique de *marketplace* qui a fait la réputation, la croissance, la rentabilité d'Amazon. Mirakl, en accompagnant des distributeurs et des acteurs industriels, permet aux entreprises européennes, françaises, internationales de se battre à armes égales face aux géants de la tech. Mirakl sert 450 clients dans le monde et aujourd'hui 80 % du chiffre d'affaires de Mirakl est réalisé à l'international.

TF : *Avec une entreprise de ce calibre, vous sentez-vous plus français ou international ?*

HW : Les deux ne sont pas incompatibles. Aujourd'hui, 100 % des développeurs de Mirakl sont basés en France, à Paris et à Bordeaux. Toute notre technologie est développée à partir de la France ainsi que notre recherche et développement. Nous servons des clients internationaux et nous accompagnons des entreprises françaises à l'international. Decathlon est actif dans une dizaine de pays européens. Nous sommes français et internationaux.

TF : *Vous soutenez la création de réglementation, même si parfois nous avons en France une aptitude à remettre des couches sur des réglementations européennes. Quel est votre regard sur ce cadre ?*

HW : J'adhère totalement à l'idée d'une réglementation européenne car elle a des enjeux de réglementation différents des États-Unis et de la Chine.

L'usage que nous faisons des données avec nos clients n'est pas du tout le même usage qu'en Chine. Par exemple, certains acteurs de *e-commerce* chinois vont récolter des données pour alimenter un *social scoring*, qui est utilisé par le parti communiste chinois. Cette pratique n'existe pas en Europe. Cependant, le risque que nous percevons est que cet excès de réglementation que nous avons en Europe ne freine la capacité d'innovation des acteurs européens.

D'autant que nous vivons toujours dans un monde où les ressources financières et les ressources humaines sont limitées. Pour des entreprises européennes, nous sommes obligés de nous mettre en conformité. D'autres acteurs extra-européens, à la différence, n'y sont pas contraints. Nous n'avons pas envie de faire ce choix. Pour chaque texte européen, c'est à peu près un million d'euros d'investissement qui est demandé.

Sur le marché numérique européen, il y a 27 réglementations différentes pour 450 millions d'utilisateurs en Europe. Nous le voyons bien, même si nous avons des textes comme le DSA⁶, le DMA⁷, l'AI Act⁸ qui sont censés s'appliquer au niveau du marché unique et des 27 pays de l'Union européenne, nous avons systématiquement des interprétations différentes en fonction des pays.

TF : *Vous êtes plutôt pour une homogénéisation des pratiques et des réglementations en Europe ?*

HW : Je pense que tout le monde est en faveur de cette harmonisation. Mais il ne semble pas y avoir aujourd'hui d'ambition politique pour y parvenir. Intégrer cette réglementation a des coûts pour les entreprises partout dans le monde, particulièrement pour les entreprises européennes. Laissons-nous le temps de digérer cette réglementation et testons les effets qu'elle peut avoir. Incitons l'investissement dans l'innovation. Aujourd'hui, nous manquons de volontarisme politique pour accompagner la croissance des entreprises européennes.

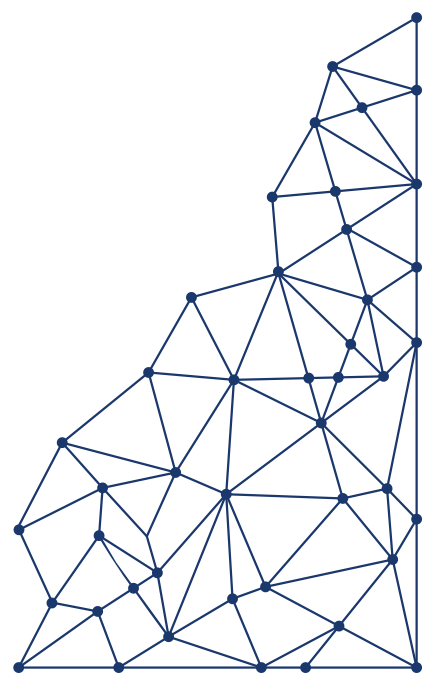
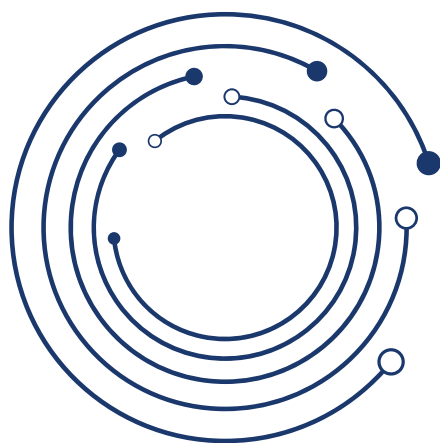
⁶ Digital Services Act : règlement européen sur les services numériques.

⁷ Digital Markets Act : règlement européen sur les marchés numériques.

⁸ Règlement européen sur l'IA.



COGNITIF : LA PROTECTION DE NOS DÉMOCRATIES FACE À LA DÉSINFORMATION



FORUM DU NUMÉRIQUE 2024



DAVID COLON

ENSEIGNANT ET CHERCHEUR,
SCIENCES PO



Thierry Fouquet (TF) : *Comment « équiper » nos cerveaux pour qu'ils soient le rempart à toutes les menaces numériques actuelles ?*

David Colon (DC) : Nos démocraties sont, depuis la fin de la guerre froide, menacées par les régimes autoritaires. Ces derniers perçoivent les systèmes d'information numérique comme une menace existentielle puisqu'ils permettent de propager des idées et des valeurs démocratiques jusque chez eux. Les régimes autoritaires ont entrepris de se doter d'armes nouvelles à l'ère de la guerre de l'information, notamment des équipes cyber, mais également une industrie de défense qui se préoccupe de l'aspect cognitif. Ces équipes ont pour cible principale le cerveau des jeunes occidentaux depuis les années 2000. Les propagandistes russes rêvaient, depuis des décennies, de concevoir des virus psychologiques qui pourraient se propager d'un esprit à l'autre, puis accélérer l'effondrement des régimes démocratiques. C'était un vieux rêve soviétique qui est devenu réalité, comme on a pu le voir aux États-Unis avec la propagation des thèses complotistes de *QAnon*. Pour les régimes autoritaires, remporter la guerre de l'information est une question de survie.

TF : *Quels sont nos moyens de détection et de parade des menaces dans la guerre de l'information ? Peut-on envisager des contre-attaques ?*

DC : Les théoriciens russes de la guerre de l'information, en particulier ceux du renseignement militaire, ont trouvé la principale faille de sécurité dans toutes nos organisations : l'être humain. Selon Norbert Wiener, il n'existe pas de "ligne Maginot du cerveau". Nous avons inventé il y a une quinzaine d'années des outils d'analyse prédictive du comportement et de la personnalité. La première fois que les croyances conspirationnistes *QAnon* ont été testées dans des sondages aux États-Unis, c'était en 2021 : 15 % de la population adhère à ces croyances. Aujourd'hui, ce chiffre est monté à 25 %. Ces derniers croient que leur gouvernement, leur armée, leur monde économique, leurs médias sont dirigés en secret par une secte pédo-sataniste qui vend, tue des enfants et boit leur sang. Ils croient ensuite que le recours à la violence est nécessaire dans la vie politique. En France, selon Sopra Steria, 25 % des Français se déclarent convaincus que les vaccins contre le Covid-19 ont causé des millions de morts. La désinformation est une croyance absurde et criminelle qui a causé des milliers de morts, des personnes dans nos familles qui ne se sont pas vaccinées, parce qu'elles étaient exposées à la propagande russe ou à la propagande chinoise sur TikTok ou ailleurs. D'après les termes de l'OMS, la désinformation constitue une « infodémie » et nous devons la traiter comme telle. Cela requiert d'abord de la traiter à l'échelle internationale. Une éventuelle riposte n'aura de véritable efficacité que si elle est coordonnée avec tous les acteurs cyber. La coopération internationale existe aujourd'hui à travers l'engagement des États-Unis et de la France. Nous devons faire confiance à des jeunes, leur confier des responsabilités parce qu'en face, les plus grands manipulateurs de masse ont une vingtaine d'années. Aleksandr Kogan, qui était l'ingénieur en chef de Cambridge Analytica, avait 25 ans.

Il a changé à jamais la face de nos environnements informationnels et de nos sociétés. Il nous manque une stratégie nationale de lutte contre les manipulations de l'information. Ce sont dans nos cerveaux que nous devons encourager tout ce qui peut contribuer à la résilience, à l'immunité cognitive, à travers une démarche de cyberdéfense psychologique. Le champ psychologique est un champ à investir prioritairement à toutes les échelles et dans toutes nos organisations.

TF : *Qu'attend-on pour interdire TikTok au niveau français ou européen ?*

DC : Les mesures restrictives de liberté sont contre-productives. Elles n'empêcheront jamais quelqu'un qui veut se connecter à TikTok de modifier le DNS (*Domain Name System*) et d'y accéder. Cela ne fait qu'encourager la défiance envers les pouvoirs établis, ce qui est précisément le but recherché par les régimes autoritaires. Enfin, cela permet aux régimes autoritaires d'établir une forme de pseudo-équivalence avec ce qu'ils font, notamment à l'égard de leurs opposants. Par conséquent, le meilleur moyen de nous défendre est de défendre notre modèle de liberté et de nous inspirer de ce qui a été fait dans les pays qui ont développé un très haut niveau de résilience cognitive. La Finlande est, de tous les pays de l'OCDE, celui qui connaît la plus ancienne ingérence russe depuis la guerre froide. En même temps, c'est celui dans lequel le niveau de confiance dans les institutions est le plus élevé, parce que des mesures ont été prises pour encourager la résilience de la population à l'égard de la propagande russe et de la guerre cognitive. Si j'étais au gouvernement, je me préoccuperais plutôt de l'éducation des gens qui votent maintenant. Nous devons mettre en place des solutions numériques. Il faut bien évidemment des mesures systémiques, mais il faut surtout une prise de conscience de la nécessité d'agir avant que la situation ne soit véritablement trop grave.

FORUM DU NUMÉRIQUE 2024



MANUEL DAVY

CEO & FOUNDER, VEKIA,
PRÉSIDENT,
LA CITÉ DE L'IA



Thierry Fouquet (TF) : Manuel Davy, vous êtes le CEO et fondateur de Vekia, en plus d'être le président de la Cité de l'IA Hauts-de-France. Pourriez-vous nous présenter votre entreprise ?

Manuel Davy (MD) : Je viens de la recherche scientifique et j'ai été chercheur au CNRS et à l'Inria avant de créer Vekia. L'approvisionnement est un geste très commun dans les entreprises, qui est souvent difficile à maîtriser parce qu'il y a des fluctuations de demande, de production, de transport, de coût... et beaucoup de références à gérer ! Nous avons besoin de beaucoup d'intelligence pour chaque prise de décision, d'intelligence rationnelle, et d'analyses. Vekia est une plateforme construite sur le concept d'intelligence artificielle qui calcule ces fluctuations et ces coûts et propose des commandes toujours parfaites.

TF : Pourquoi avez-vous choisi cette voie ?

MD : Je suis intéressé par la réussite des entreprises avec l'intelligence artificielle. Je l'ai fait comme chercheur, puis comme entrepreneur. La Cité de l'IA, en tant que mouvement associatif, est un prolongement naturel. Je suis en train de créer une deuxième entreprise qui va réaliser des projets pour aider les entreprises à réussir grâce à l'IA. L'IA est ce qu'on appelle un *pharmakon*, c'est-à-dire le poison et le remède en même temps. Sur la guerre de l'information, c'est typiquement le cas. Les *deepfakes* sont rendus industrialisables aujourd'hui par des personnes mal intentionnées. Mais la meilleure façon de les contrer est de les détecter.

TF : L'entreprise va-t-elle devenir un champ d'éducation et de sensibilisation ?

MD : Les entreprises sont un acteur fondamental de la transformation de la société, en particulier aujourd'hui puisque presque toutes les entreprises se demandent comment former leur personnel à l'IA générative.

TF : Qu'est-ce qui peut nourrir un optimisme lucide ?

MD : L'intelligence artificielle est une immense opportunité pour les sociétés et les entreprises, pour trois raisons. La première est la performance économique : c'est un enjeu de souveraineté, de réindustrialisation et de maîtrise de notre propre destin. L'IA peut avoir des impacts tellement forts sur les économies d'énergie, la productivité et la créativité que c'est une chance pour les territoires et les pays qui savent s'en emparer. La deuxième raison, c'est qu'elle offre la possibilité d'accéder à de meilleurs emplois et de décharger l'être humain de ses tâches répétitives. L'intelligence artificielle apporte une forme de libération qui recentre l'humain sur ce qu'il sait faire en tant qu'être humain. Enfin, troisième raison : par l'amélioration de la performance et l'efficacité des entreprises, nous avons aussi un levier fort sur l'impact environnemental, notamment l'empreinte carbone. Donc, l'IA constitue une véritable opportunité.

FORUM DU NUMÉRIQUE 2024



JEAN-PAUL PINTÉ

DOCTEUR EN SCIENCES DE
L'INFORMATION ET DE LA
COMMUNICATION, MAÎTRE
DE CONFÉRENCE,
UCL



SYNOPIA

ESPOL

INSTITUT DE
GESTION,
ÉCONOMIE
& SCIENCES

edn

UNIVERSITÉ
CATHOLIQUE
DE LOUVAIN

ETHICS
EA 7146

Thierry Fouquet (TF) : *Vous avez un blog qui s'appelle « cybercriminalité.blog » où vous essayez de mettre un maximum d'informations qualifiées, y a-t-il vraiment un enjeu d'accès à la connaissance ?*

Jean-Paul Pinte (JPP) : Nous avons une perdition des modes de recherche. Tout se passe trop sur un seul moteur, un seul espace. Je me bats depuis l'université pour cette veille stratégique, de manière à retirer le grain de l'ivraie. Il ne faut pas attendre que les informations viennent à vous. Il faut savoir aller les chercher. La cybercriminalité a investi depuis longtemps le champ de l'intelligence artificielle. Nous nous apercevons que la population, les jeunes et les autres, n'ont pas été formés à cette surveillance d'un territoire informationnel, alors qu'il existe énormément d'outils qui permettent de le faire. Tous les territoires (des couches d'Internet, du Web de surface, du *Deep Web*, du *Dark Web*) investissent dans l'intelligence artificielle, ce qui fait qu'on injecte du *Dark Web*, des données, sur le Web de surface. Des personnes ont des ADN numériques ou des réputations salies à cause de cela. Cependant, ils ne savent pas comment le maîtriser.

TF : *Je suis parfois stupéfait du manque de prise de conscience des élites, qu'elles soient économiques, ou politiques. Est-ce une impression de ma part, ou vous le confirmez ? Pensez-vous qu'il y a un niveau de conscience suffisant ?*

JPP : Il y a un grand décalage que nous sommes en train de résorber en ce moment parce qu'il y a eu des structures qui ont été mises en place. Ces services permettent aujourd'hui d'avoir une prise de conscience. Pourtant il n'y a pas cette conscience de l'évolution des modes opératoires des cybercriminels. Les cibles se disent qu'elles ne sont sûrement pas ciblées. Aujourd'hui, une petite entreprise peut se faire attaquer, se retrouver en faillite très rapidement.

TF : *Quels types de solutions faut-il mettre en place ?*

JPP : Il aurait fallu déjà démarrer il y a longtemps. Nous pouvons rattraper une partie du retard, mais les différents gouvernements ont perturbé la bonne continuité des réformes. Je n'ai pas vu se développer réellement des volontés, à part peut-être celles qui sont en cours, de redonner de l'ordre dans tout cela. Il y a des moyens de développer notre formation dans le domaine cyber. Aujourd'hui, avec cette couche d'intelligence artificielle, il y a 60 % des travaux universitaires qui sont faits avec des outils comme ChatGPT, ce qui fait que je suis obligé de faire une veille sur ChatGPT de manière à m'apercevoir que des paragraphes complets sont simplement incrémentés, avec entre eux, des paragraphes qui sont rédigés par l'étudiant pour faire le lien, ce qui montre que la génération n'est pas prête. Il faut aujourd'hui penser à tout cela et savoir que l'intelligence artificielle va ajouter une couche à tous ces modes opératoires que nous utilisons aujourd'hui pour vous tromper. Tout ce qui est technologie, *phishing*, *walling* etc, sont déjà infectés par des modes opératoires de l'IA.

FORUM DU NUMÉRIQUE 2024



FÉLIX VON NOSTITZ
MAÎTRE DE CONFÉRENCES
EN SCIENCE POLITIQUE,
ESPOL



Thierry Fouquet (TF) : *Félix von Nostitz, vous êtes maître de conférences en sciences politiques, coresponsable du master Digital politics and governance à l'Université catholique de Lille. Vous avez travaillé sur l'impact de la désinformation politique sur les réseaux sociaux. Quelles sont les conclusions auxquelles vous êtes arrivé ?*

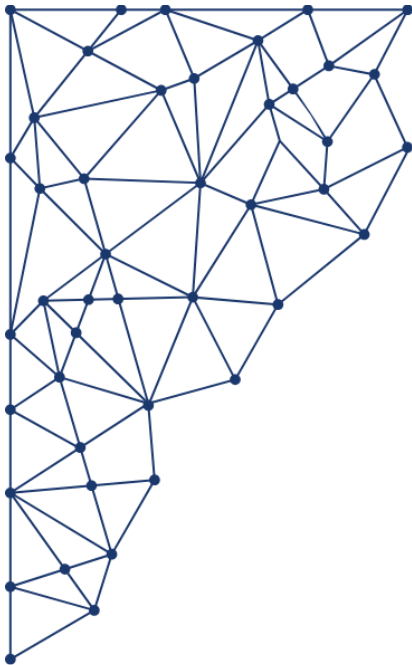
Felix von Nostitz (FVN) : Nous essayons de comprendre comment les réseaux sociaux changent le comportement électoral, comment les personnes s'informent pour choisir leur parti, leur candidat. Aujourd'hui, les citoyens utilisent encore la télévision et les médias classiques pour s'informer. Il y a encore peu de monde qui s'informe sur les réseaux sociaux. Ce sont les personnes très politisées, et surtout dans l'extrême, qui s'informent sur les réseaux sociaux. Les médias classiques restent encore les sources préférées pour s'informer. D'autre part, il y a un risque conséquent de désinformation sur les réseaux sociaux. Par exemple, l'algorithme de TikTok est basé sur l'économie de l'attention, qui signifie que si nous sommes intéressés par un sujet, TikTok nous proposera des sujets connexes. Les personnes les plus engagées s'appuieront sur les réseaux sociaux, ce qui n'est pas le cas de la grande majorité des personnes, qui ne sont pas très intéressées par la politique.

TF : *Vous avez étudié aussi l'évolution des pratiques des partis politiques à l'orée de ces technologies. Est-ce que vous pouvez nous partager quelques résultats de vos recherches ?*

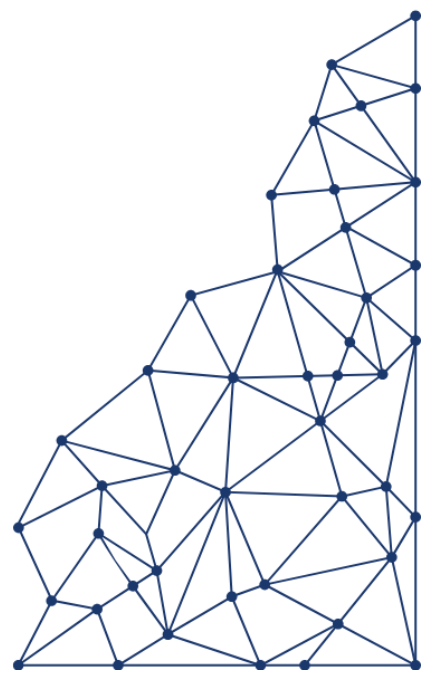
FVN : *Au début de notre étude, nous pensions que c'était plutôt le petit parti innovant qui utilise beaucoup de numérique, mais ce sont beaucoup de grands partis qui l'utilisent parce que cette technologie coûte très cher.*

TF : *Pensez-vous que ces évolutions peuvent avoir un impact sur la qualité des élections ?*

FVN : La désinformation peut avoir un impact sur la qualité des élections. Par exemple en Slovaquie, lors des dernières élections, il y a eu un *deepfake* du candidat de l'opposition deux jours avant les élections qui a déstabilisé le candidat et le vote. Beaucoup d'observateurs ont confirmé que ce *deepfake* a perturbé le résultat des élections qui était très serré. Il y a également eu le *deepfake* de Joe Biden qui a dissuadé les personnes de voter lors des primaires.



CYBER ET SÉCURITÉ : LE RENFORCEMENT DE LA SÉCURITÉ NUMÉRIQUE DANS L'ÉTAT DE DROIT



FORUM DU NUMÉRIQUE 2024



FRANÇOIS GORRIEZ
AVOCAT,
CABINET MATHIAS AVOCAT



Thierry Fouquet (TF) : *Comment pouvons-nous lutter contre la cybercriminalité, tout en respectant l'État de droit ?*

François Gorriez (FG) : Il n'y a pas besoin d'être juriste pour parler de droit. Le monde de la santé, le monde alimentaire, ou encore celui des transports, tous connaissent des réglementations de sécurité depuis de nombreuses années.

Le droit de la cybersécurité est assez ancien. La première loi date de 1988 (loi Godfrain). Cette loi a introduit la fraude informatique dans le code pénal et sanctionne notamment, l'accès et le maintien frauduleux dans un système de traitement automatisé de données, l'altération du système d'informations et l'introduction, la suppression et la modification frauduleuse de données, ainsi que le faux et l'usage du faux dans des documents informatisés. Par la suite, le droit de la cybersécurité a été surtout impulsé par l'Union européenne, avec des textes récents, notamment le RGPD, la norme ISO 27001, l'IA Act ainsi que le *Cyber Resilience Act*.

La stratégie de l'Union européenne est de faire monter le niveau de sécurité de l'Union par les réglementations. Ces réglementations visent à permettre d'installer de la confiance dans l'économie par des grands principes, comme la transparence, l'obligation d'*accountability*⁹ pour les acteurs économiques, visant à prendre des mesures de sécurité et être en mesure de démontrer leur bonne application. Elle vise aussi à augmenter la cyber résilience de l'UE avec des dispositions particulières en matière de gestion de crises, d'incidents ou encore de partage d'informations en matière de vulnérabilités. L'enjeu aujourd'hui est la lisibilité de ces normes, qui coûtent cher à mettre en œuvre d'un point de vue financier et intellectuel. Le deuxième enjeu est l'harmonisation. Il n'y a pas de frontière dans le domaine numérique contrairement au domaine juridique. Enfin, le risque numérique rejoint aussi les questions de droits et de libertés fondamentales.

TF : *Une loi française récente a fixé à 15 ans l'âge d'accès aux réseaux sociaux. Plusieurs États souhaitent légiférer sur ce sujet. Comment voyez-vous évoluer les choses ?*

FG : Je pense que l'hygiène informatique passe par l'éducation, dès le plus jeune âge. Nous devons prendre le temps d'adopter des mesures de sécurité et aussi de comprendre ce à quoi nous nous engageons lorsque nous allons sur une plateforme.

⁹<https://www.cnil.fr/fr/definition/accountability#:~:text=L'accountability%20d%C3%A9signe%20l'obligation,%C3%A0%20la%20protection%20des%20donn%C3%A9es.>

FORUM DU NUMÉRIQUE 2024



GEORGES LOTIGIER

FOUNDER ET BOARD MEMBER,
HORNETSECURITY-VADE



Thierry Fouquet (TF) : *Quand on décide de lutter contre la cybercriminalité, comment fait-on ?*

Georges Lotigier (GL) : Je trouve que nous sommes très naïfs sur ce sujet, particulièrement en France. L'humain, en cybersécurité, est le maillon faible : on ne nous apprend pas à adopter les bons réflexes dès le départ dans notre utilisation du numérique. Or, se balader sur Internet, c'est comme se balader dans les bois pour le petit Chaperon Rouge, il y a des risques. Je milite pour un enseignement numérique dès l'enfance, bien avant qu'on atteigne la majorité numérique. Par exemple, certains pays le font comme Israël où dès le collège, les élèves reçoivent une formation en informatique et en cybersécurité. C'est primordial pour l'avenir.

Un autre enjeu, c'est l'extraterritorialité des lois américaines. Toutes les entreprises y sont soumises : propriété intellectuelle, utilisation du dollar, activité hors Europe, concurrence, informations stockées par une société américaine... Le *Cloud Act* signifie pour une entreprise américaine, qu'elle a l'obligation de transmettre toute information stockée, même hors du territoire américain, au gouvernement américain s'il en fait la demande. Le simple fait d'utiliser Facebook transmet des données personnelles aux États-Unis. L'extraterritorialité des lois américaines met les grandes industries européennes en danger. La loi américaine est très différente de la loi française ou européenne. En France, chacun est propriétaire de ses données personnelles, aux USA c'est par défaut l'entreprise qui héberge les données.

TF : *Pourquoi sommes-nous laxistes sur le Cloud Act ?*

GL : Souvent parce que c'est la solution de facilité : les Américains sont excellents pour créer de nouveaux produits qui nous séduisent. Nous sommes colonisés d'un point de vue numérique, et de plus en plus dépendants du numérique. Nous n'avons pas de marché informatique national ni européen. À titre d'exemple, en France, près de 85 % des outils de cybersécurité utilisés sont Américains ou Israéliens. Nous devons nous unir en Europe pour proposer un contrepoids suffisamment fort. Nous avons besoin d'une Europe forte sur le numérique et la cybersécurité. Le RGPD est une bonne initiative, mais elle est défensive, et si une donnée est hébergée en France mais sécurisée par une solution américaine, elle reste potentiellement accessible.

Concernant Hornetsecurity-Vade, actuellement, 25 % de notre chiffre d'affaires provient des États-Unis et 15 % du Japon. Notre société fait 120 millions d'euros de chiffre d'affaires, ce qui est déjà très significatif pour un éditeur, alors que certains concurrents américains directs font un chiffre jusqu'à dix fois plus élevé. Comme il n'y a pas de marché intérieur, nous avons plus de mal à grandir que les sociétés américaines. Il faut être assez audacieux et plus international.

Les éditeurs français de cybersécurité ne doivent pas se contenter de faire « à peu près la même chose que les Américains ». Nous devons créer et développer Le meilleur produit. Nous avons en France et en Europe les talents et les écoles pour y parvenir.

TF : *La cybersécurité est un marathon parce que les cybercriminels changent leur technique tous les jours. Est-ce que la bataille est à armes égales aujourd'hui, ou faut-il renforcer la prise de conscience et le fait que le maillon le plus faible reste l'humain ?*

GL : La cybersécurité restera toujours imparfaite, il est impossible de détecter la totalité des attaques et ne prendre aucun risque. Pour cette raison effectivement la prise de conscience et la formation des utilisateurs sont indispensables pour en limiter les conséquences.

De façon générale, je reste assez optimiste. Je vois bien qu'il y a une prise de conscience à cause des évolutions géopolitiques actuelles. Nous avons de très bonnes écoles et de très bonnes technologies. La prise de conscience au niveau des administrations et du gouvernement aide probablement les entreprises à se développer. Le marché européen est en croissance supérieure comparé à celui des États-Unis sur la cybersécurité. Nous avons donc des chances de rattraper notre retard.

FORUM DU NUMÉRIQUE 2024



THÉO PLANTIER

CEO,
OVERSOC



Thierry Fouquet (TF) : *Vous êtes PDG, cofondateur de OverSOC depuis 2019. C'est une solution que vous proposez, qui consolide les données cyber-existantes d'une entreprise, en faisant une cartographie 3D du système d'information. Vous accompagnez l'entreprise, et vous facilitez le travail des équipes opérationnelles, pour qu'elles communiquent facilement et efficacement avec le top management.*

Théo Plantier (TP) : Notre entreprise est née dans le Nord et nous sommes aujourd'hui une vingtaine. Lors de la création, nous sommes partis du constat que 50 % du temps des experts cybernétiques est perdu en traitement de données. Plus l'entreprise est grosse, plus il y a un nombre d'outils importants qui sont déployés. En moyenne, c'est 10 à 15 pour les ETI, et pour les grands groupes, on trouve parfois 30 à 45 solutions différentes.

Nous nous rendons compte qu'elles sont toutes nécessaires, mais la consolidation n'a pas encore été faite. Aujourd'hui, 95 % des entreprises avec lesquelles nous travaillons nécessitent une consolidation de leurs données.

Nous avons également une posture d'outil agrégateur dont la vocation est d'être un plot sur lequel on peut se brancher.

Nous avons la chance d'avoir comme client EDF dont l'enjeu est de créer un environnement de test sécurisé pour l'utilisateur ou le client potentiel, pour actionner le cas d'usage sans forcément avoir accès à la donnée sensible.

Nous l'avons déjà fait par le passé avec le commandement de la cyberdéfense où nous avons éprouvé notre modèle sur de la donnée normalisée. Tout l'enjeu est de leur montrer des sets de données qui sont reconnus, pour leur prouver notre savoir-faire sans avoir besoin de lire des données sensibles.

FORUM DU NUMÉRIQUE 2024



MATHIAS POVSE

DIRECTEUR RÉGIONAL,
EDF HAUTS-DE-FRANCE
2017-2025



Thierry Fouquet (TF) : *Pouvez-vous nous rappeler ce que représente EDF ?*

Mathias Povse (MP) : Le Groupe EDF compte 180.000 collaborateurs dans le monde, sur de multiples métiers, depuis la production jusqu'à la commercialisation, en passant par le nucléaire, l'hydraulique, le thermique, les énergies nouvelles et les services énergétiques associés. De ce fait, son environnement informatique est complexe et réparti à l'international. En Hauts-de-France, le groupe EDF c'est 10 000 collaborateurs engagés au quotidien pour fournir 24h sur 24h l'énergie bas carbone et les services énergétiques dont nous avons tous besoin. Par conséquent, la cybersécurité représente un enjeu majeur pour le groupe.

TF : *Vous êtes victimes de plusieurs millions de tentatives d'attaques par an. Comment faites-vous pour contrer ces attaques et avec qui travaillez-vous ?*

MP : En matière de cybersécurité, le défi est permanent ! L'enjeu est d'anticiper les menaces, réagir et trouver des solutions innovantes face aux attaques, maîtriser des technologies de plus en plus sophistiquées et garantir la sécurité de notre patrimoine et sa résilience. La plupart des attaques sont traitées automatiquement, mais plusieurs dizaines de milliers doivent être traitées individuellement par nos services.

Nous mettons donc en œuvre des moyens conséquents et nous nous dotons des compétences nécessaires. Par exemple, notre propre centre de réponse aux incidents et nos centres de surveillance collaborent activement avec l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Nous travaillons également sur le facteur humain, auprès de nos collaborateurs avec des sensibilisations régulières aux risques cyber et la diffusion de bonnes pratiques.

Il existe également une dimension nationale et internationale. La force d'EDF est d'être une entreprise très implantée au niveau des territoires. Nous cherchons à être au plus près de nos clients, à les aider à décarboner leurs activités, à piloter ainsi qu'à gérer au mieux leur consommation d'énergie et cela nécessite de plus en plus d'outils numériques. Nous constatons une « professionnalisation » des groupes cybercriminels. Cela nous engage à nouer des liens étroits avec les acteurs de l'écosystème cyber français et européen pour renforcer notre souveraineté en matière de cybersécurité. A titre d'exemples, EDF est partenaire du Campus Cyber de Paris et du Pôle d'excellence Cyber à Rennes. Nous sommes constamment à l'écoute des initiatives émergeant en région. Ainsi, en Hauts-de-France, EDF s'est impliquée dès l'origine dans la création du Campus Cyber Hauts-de-France Lille Métropole afin de protéger au mieux les acteurs du territoire, notamment les PME-ETI, les collectivités, nos clients mais également nos sous-traitants.



Thierry Fouquet (TF) : *Vous êtes chef d'escadron, responsable des relations internationales et des partenariats au Centre national de la formation à la cybersécurité de la gendarmerie nationale. Quel est le travail que vous accomplissez avec votre équipe ?*

Jérôme Tabaries (JT) : D'abord une petite précision : le Centre de formation dépend du ministère de l'Intérieur et pas seulement de la gendarmerie nationale. Notre rôle est de former les enquêteurs du numérique, et un peu plus tard, d'autres publics que nous cherchons à élargir. La particularité est que notre rôle n'est pas de sécuriser des réseaux. Ce serait une concurrence déloyale vis-à-vis de sociétés qui le font déjà. Nous faisons du conseil comme sur n'importe quel territoire soumis à la criminalité, de la prévention également, mais ce n'est pas nous qui installons les barrières autour des maisons. Notre rôle est d'intervenir une fois que le crime a été commis et d'en rechercher les auteurs.

TF : *L'organisation et la structuration du domaine du cyber sont très récentes en France ?*

JT : Oui, il y a une montée en puissance très rapide. En 2021, la gendarmerie crée le commandement de la gendarmerie dans le cyberspace. En 2022, elle se dote d'un centre de formation. En décembre 2023, le commandement de la gendarmerie dans le cyberspace devient un service à compétence nationale pour la police et la gendarmerie, et un commandement du ministère dans le cyberspace.

TF : *La cybercriminalité vous confronte à des interventions que, parfois, vous n'avez jamais vécues. Ainsi, on vous emmène régulièrement à la limite de l'état de droit, dans des interventions où vous devez prendre des décisions extrêmement rapides. Ça ne doit pas être facile tous les jours.*

JT : C'est effectivement très compliqué. La cybercriminalité est très volumineuse et inventive. Nous sommes régulièrement confrontés à des cas qu'on ne connaît pas et qu'on ne sait pas toujours traiter dans un cadre juridique convenable. Lorsque nous sommes confrontés à des cas comme ceux-là, le législateur est poussé à prendre des mesures pour qu'on puisse rentrer dans un cadre qui convient. Cela a été le cas pour un dossier connu sur Internet : le dossier EncroChat, dans lequel on a dû pirater un réseau téléphonique chiffré. À l'époque il n'y avait pas de cadre juridique pour ça : il a donc été créé.

Il nous faut plus de lois, car beaucoup de choses ne sont pas couvertes ou prévues par la loi. Par exemple, la *blockchain* est un livre, un registre de compte public, accessible à tout le monde. Lorsque deux jeunes y ont dérobé plus de 9 millions de dollars, ils ont été acquittés par le tribunal car la *blockchain* n'a pas été considérée comme un système de traitement automatisé de données. Cette notion-là est donc un peu trop restrictive pour l'ensemble de nos technologies.

L'intelligence artificielle va également soulever plusieurs défis. Le premier, c'est le volume du contentieux qui va être généré par l'IA. Il y en a déjà beaucoup. Le deuxième défi concerne les outils : quels outils pourra-t-on utiliser pour lutter contre cela ? Aujourd'hui, il existe un cadre juridique qui permet à l'humain, l'enquêteur, de faire ce qu'on appelle une « enquête sous pseudonyme ». En substance, c'est *undercover* sur le net. Un cadre juridique le permet. Demain, si nous avons des outils d'intelligence artificielle qui vont essayer de détecter des comportements criminels en ligne, ils vont être amenés à être en contact avec des criminels, voire à effectuer des actes illégaux eux-mêmes. Quelle personnalité juridique va-t-on donner à ces outils-là pour interagir légalement avec les criminels ? L'intelligence artificielle est un peu une boîte noire. On ne sait pas vraiment comment l'IA prend ses décisions une fois qu'elle est entraînée (même ses créateurs ne le savent pas). Quelle sera la force probante de tous ces outils face au tribunal ? Nous avons des juges et potentiellement des jurés à convaincre.

TF : *Vous souhaitez aussi avoir accès à des données plus facilement, ce que la réglementation vous interdit dans le cadre de vos enquêtes.*

JT : Oui. C'est une piste qui a été évoquée dans le rapport sur l'intelligence artificielle publié par le gouvernement en mars 2024. C'est un rapport qui ne parle pas de cybercriminalité, mais les problèmes éthiques sont identiques. Nous devons nous doter d'outils très performants qu'il faudra entraîner avec des données de très bonne qualité.

FORUM DU NUMÉRIQUE 2024



HERVÉ TROALIC
DIRECTEUR GÉNÉRAL,
IMINETI BY NIJI



Thierry Fouquet (TF) : *Hervé Troalic, vous êtes directeur général d'Imineti by Niji. Que signifie Imineti ?*

Hervé Troalic (HT) : Ça veut dire confiance en Telugu, un dialecte indien.

TF : *Vous êtes conseiller en stratégie digitale, cybersécurité, management et valorisation de la donnée, réalisation de logiciels sur mesure. Comment abordez-vous ces questions de création de la sécurité, dans le respect des personnes et du droit ?*

HT : J'ai coutume de dire que nous sommes un centre d'expertise en cybersécurité pour les entreprises que nous accompagnons. Nous intervenons aussi techniquement, en effectuant des tests d'intrusion, des audits de *phishing*, etc. Notre positionnement est complètement intégré dans l'État de droit, puisque nous respectons tous ses référentiels, en nous les appropriant. Par exemple, nous sommes qualifiés comme auditeur PASSI par l'Agence Nationale de Sécurité des Systèmes d'Information. Nous sommes également accompagnateur *SecNumCloud*. Nous avons fait le choix de nous faire reconnaître sur cette expertise pour aider les entreprises, du mieux que possible, à mettre en œuvre ce qu'elles peuvent mettre en œuvre à la hauteur de leurs moyens.

TF : *Il vous semble donc légitime qu'un cadre s'exerce ?*

HT : Oui, il me semble non seulement légitime, mais indispensable qu'un cadre s'exerce dans le domaine de la cybersécurité. Quand j'ai commencé il y a une trentaine d'années, ce champ d'activité était encore balbutiant. Il n'existait pas de formation spécialisée, pas de normes établies, ni de réglementation claire pour encadrer les pratiques. La plupart d'entre nous venaient d'autres disciplines : des réseaux, de l'administration systèmes, ou du management. On apprenait sur le tas, et il fallait avant tout faire preuve de rigueur et gagner la confiance des clients.

Je me souviens, à mes débuts, il fallait expliquer en détail ce qu'était un test d'intrusion, comment nous le menions, pourquoi il était utile, et surtout rassurer le client. Il fallait le convaincre que nous n'allions ni endommager ses systèmes, ni compromettre ses données. Il n'y avait pas de cadre formel, pas de règles universelles, seulement notre parole et notre sérieux. Le mot « confiance » était au cœur de notre métier, car il comblait l'absence de références établies.

Aujourd'hui, les choses ont heureusement beaucoup évolué. Le secteur s'est structuré : il existe des formations reconnues, des référentiels techniques, des méthodologies éprouvées et une réglementation qui encadre les pratiques. Ce cadre est bénéfique à plusieurs niveaux. Il apporte de la crédibilité à notre profession, facilite la relation avec les clients, et renforce la sécurité globale des systèmes d'information. On ne se pose plus les mêmes questions qu'à l'époque : la base est aujourd'hui solide, ce qui nous permet d'aller plus loin.

En effet, le cadre ne fige pas le métier, il l'accompagne dans son évolution. Il nous pousse à nous améliorer, à explorer de nouvelles méthodes, de nouvelles technologies pour anticiper les menaces de demain. Par exemple, alors qu'autrefois, réussir à imprimer à distance sur le système d'un client constituait déjà une belle preuve de vulnérabilité, aujourd'hui nous devons démontrer notre capacité à prévenir et contenir des attaques beaucoup plus sophistiquées, comme des ransomwares. Il ne s'agit plus seulement de détecter une faille, mais de prouver que nous savons empêcher une compromission majeure ou, à défaut, y répondre immédiatement.

TF : *C'est rare d'entendre quelqu'un dire qu'il ne veut pas obliger ses clients à venir vers lui. Vous dites qu'il ne faut pas obliger les entreprises à faire de la cybersécurité ?*

HT : Il faut que toutes les entreprises prennent conscience de l'enjeu de la cybersécurité. Je pense que ce n'est pas sous la contrainte qu'on obtient les meilleurs résultats. Nous ne devons pas tomber dans un excès où par la loi, nous obligeons tout le monde à atteindre un niveau de sécurité qui serait utopique. Nous sommes des experts de la norme 27001.

Elle ne définit pas un niveau de sécurité mais un niveau de maîtrise. Je pense qu'il vaut mieux emmener les gens vers une meilleure maîtrise de leur sécurité, voire de leurs faiblesses. Toutes les entreprises n'ont pas le même métier. Elles ne déploieront pas la même sécurité. Ensuite, il y a les moyens dont l'entreprise dispose, c'est-à-dire qu'une PME n'a pas un gros budget pour sa cybersécurité : elle va plutôt s'occuper de son approvisionnement, de ses machines ou de son personnel. Enfin, quand on s'adresse à des entreprises d'une certaine taille, nous devons convaincre les dirigeants de l'importance de la protection cyber. C'est là que la maturité du dirigeant par rapport à la problématique est importante.

Pour une entreprise, il existe beaucoup de facteurs de stress. La cybersécurité est un facteur supplémentaire. Il ne faut pas le nier : il faut vivre avec et l'intégrer dans sa stratégie au même titre que n'importe quelle autre menace ou contrainte. Il faut être capable de bouger le curseur au gré des opportunités, des contraintes financières qu'on a, etc.

Nous sommes dans la prévention. Rien n'est plus désagréable que d'être contacté la première fois parce que l'entreprise est en difficulté et qu'il faut éteindre le feu. L'IA Act s'appuie sur le *risk management*. Aujourd'hui, un chef d'entreprise fait de la gestion de risque tous les jours. Lui parler de gestion de risque, c'est lui démontrer que nous avons compris ces enjeux, que nous ne sommes pas là pour lui dérouler quelque chose de prémâché, mais que nous allons comprendre ces problématiques et qu'on va piloter le cyber comme il pilote le reste de son entreprise.

FORUM DU NUMÉRIQUE 2024



BELHASSEN ZOUARI

PROFESSEUR EN
INFORMATIQUE,
SPÉCIALISTE EN
CYBERSÉCURITÉ,
UCL



Thierry Fouquet (TF) : *Comment collaborer d'un point de vue légal avec les autres pays pour lutter contre les cybercrimes ?*

Belhassen Zouari (BZ) : L'objectif principal est d'harmoniser les lois nationales, actuellement trop disparates. Ainsi, certains cybercrimes sont considérés comme des crimes dans un pays et ne le sont pas dans un autre. Afin de combler cette faille, la Convention de Budapest (2004), aujourd'hui signée par 72 pays, est le premier traité international à aborder les crimes informatiques. Cette convention vise aussi à améliorer les techniques d'enquête et les moyens de collaboration entre les pays pour combattre le cybercrime. Cependant, il est difficile d'obtenir des résultats convergents. Par exemple, la pornographie n'est pas considérée comme un crime dans certains pays. Sur le terrain, les criminels connaissent ces failles et passent par des pays où la collaboration est réputée difficile. En effet, certains pays collaborent très bien entre eux, notamment au niveau de l'Europe, car ils ont une vision commune. Le problème n'est pas vraiment technique, mais il est plutôt dans les divergences d'application de loi au niveau national et international. De plus, Internet est connu pour l'anonymat. Les pirates, les *hackers*, profitent de cette caractéristique pour commettre des cybercrimes tout en étant confiants sur le fait qu'on ne pourra pas les retrouver au regard des disparités géographiques.

TF : *En tant que professeur de cyber, qu'est-ce que vous enseignez ?*

BZ : J'enseigne principalement trois aspects importants en cybersécurité :

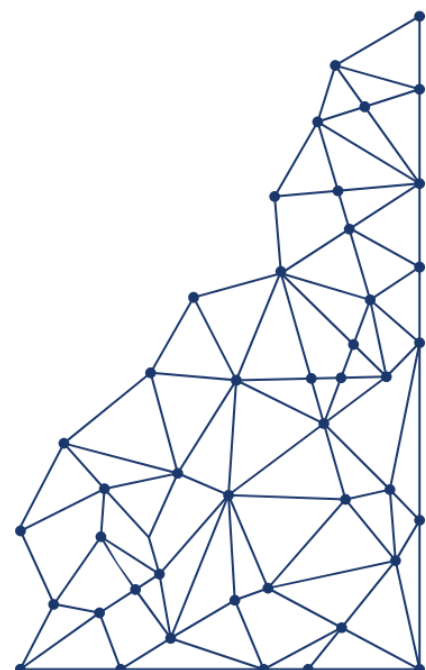
- L'aspect technique et technologique parce que nous voulons former des étudiants qui maîtrisent les techniques les plus modernes en cybersécurité.
- Il existe également les aspects éthiques et réglementaires
- Enfin, les aspects de *management* de la sécurité sont essentiels à l'apprentissage.

TF : *Suite à une formation au sein de l'École du Numérique, quels sont les métiers proposés ?*

BZ : il y existe plusieurs métiers autour du cyber comme les métiers de cyber-technologique, de délégué à la protection des données (DPO), ou bien de responsable de la sécurité des systèmes d'information (RSSI).



REMERCIEMENTS



FORUM DU NUMÉRIQUE 2024



SOPHIE CAVILLON

DOYEN,
FACULTÉ GESTION
ÉCONOMIE ET SCIENCES,
UCL

SYNOPIA
la plateforme des gouvernements

ESPOL

FACULTÉ DE
GESTION,
ÉCONOMIE
& SCIENCES

edn
ÉCONOMIE
DES NÉCESSAIRES

UNIVERSITÉ
CATHOLIQUE
DE LILLE

ETHICS
EA 7446



Je suis ravie de conclure cette belle et riche journée de la deuxième édition du Forum du numérique.

Après l'obtention de mon doctorat en biologie moléculaire il y a plus de 20 ans, je suis devenue maître de conférences à l'Université Catholique de Lille. J'ai également été responsable pédagogique pendant 20 ans, et aujourd'hui, je suis doyenne de la Faculté de Gestion, Économie et Sciences.

Nous avons la certitude de devoir continuer à accompagner nos étudiants vers les métiers du numérique, qui sont en constante évolution. Nous devons leur donner une connaissance solide des technologies émergentes de l'IA et de la cybersécurité. Nous les formons également aux enjeux éthiques.

Certains éléments de géopolitique, voire de stratégie de gouvernance, seraient un plus pour nos étudiants et pourraient nous laisser penser que nous amenons notre contribution à un avenir numérique plus sûr et plus serein pour l'Europe.

Je souhaite remercier l'ensemble des intervenants de ce jour. Je remercie tout d'abord le parrain et la marraine de notre forum, Madame la députée Anne le Hénanff et l'amiral Arnaud Coustillière pour leur contribution importante à cette journée.

Je remercie également les collègues d'ESPOL, de l'EDN, les entreprises, les partenaires, pour leur contribution importante à cette journée.

Je remercie les acteurs de l'ombre, les collègues de la Faculté de Gestion, Économie, et Sciences de l'Université Catholique de Lille dont Sébastien, Fatiha, Marie, Faustine, Juliette, qui ont œuvré aux côtés de Laura pour organiser cette belle journée et nous permettre de vous accueillir dans de bonnes conditions.

Enfin, un grand merci à l'équipe Synopia pour sa confiance renouvelée cette année.

FORUM DU NUMÉRIQUE 2024



LAURA SCHAUB

DIRECTRICE DES PROJETS,
SYNOPIA



LE FORUM DU NUMÉRIQUE N'AUROIT PAS PU SE FAIRE SANS VOUS !

Notre projet n'aurait pas pu se concrétiser sans l'implication de nombreux partenaires, membres et amis de Synopia qui ont su s'engager et contribuer à la richesse de cet événement où intelligence collective et cohésion constituaient les fondamentaux de la réussite de ce deuxième forum.

C'est un honneur pour moi de citer les principaux acteurs qui se sont engagés dans notre projet, et les remercier très chaleureusement en conclusion de ce numéro de la Revue du Forum du Numérique 2024.

Pour Synopia

Quentin Billard, Bruno Cathala, Arnaud Coustillière, Xavier Dupont, Jacky Isabello, Jean-Claude Mailly, Alexandre Malafaye, Xavier Marchal, Jean-Marc Schaub, Joséphine Staron, Bernard Vanneste.

Pour l'Université Catholique de Lille

Le Président Recteur Patrick Scaufaire et ses équipes dont Denis Vinckier.

Pour la Faculté de Gestion, Économie & Sciences, Université Catholique de Lille

Le Doyen de la Faculté Sophie Cavillon et ses équipes dont Fathia Talbi et Justine Tarnaud.

Pour M La Constellation

Thierry Fouquet et Marion Tocci.

Et bien entendu tous nos partenaires, entreprises et mécènes,
universitaires, institutionnels, associatifs, et média :

ORGANISATEURS ET PARTENAIRES

ACADÉMIQUES



GRANDS PARTENAIRES



SOUTIENS DU FORUM



PARTENAIRES ÉVÉNEMENTIELS

& MÉDIAS



NOTRE RAISON D'ÊTRE

« Au service de **l'intérêt général**,
Synopia propose des idées et des solutions
pour **améliorer la gouvernance**
publique et privée, en France et en Europe,
afin de répondre aux défis contemporains
nationaux et internationaux,
et **favoriser les transitions et la cohésion**. »

NOS FINALITÉS

Transformer **les gouvernances**



&

Fabriquer de **la cohésion**

NOS LEVIERS

Influencer par **les idées**

&

Transformer par **les projets**



Retrouver Synopia sur sa chaîne YouTube

REVUE
FORUM DU NUMÉRIQUE
2^{ème} édition

« **SOUVERAINETÉ EUROPÉENNE, QUEL ÉQUILIBRE ENTRE COMPÉTITION ET COOPÉRATION ?** »

Pour de multiples raisons qui touchent à la maîtrise des technologies ou à l'ingérence étrangère, le numérique est l'un des sujets centraux de la souveraineté européenne.

C'est pourquoi les travaux de la 2^{ème} édition du Forum du Numérique ont porté sur les enjeux de souveraineté numérique. Il s'agit d'un sujet dont l'importance est croissante pour l'Union européenne et ses États membres.

Pour gagner en souveraineté, l'Union européenne se doit d'agir sur les 3 fronts suivants :

- le cadre réglementaire et normatif,
- le développement rapide de ses propres capacités numériques, matérielles et immatérielles,
- s'adapter à la dimension indissociable de l'innovation et de la société.

La souveraineté suppose de pouvoir exercer un contrôle sur les technologies numériques, les données, l'infrastructure et les services numériques afin de protéger ses intérêts économiques, politiques et culturels. Cela inclut la protection des données personnelles, la sécurité des réseaux et des infrastructures critiques.

Elle impose d'investir vite et avec des fonds d'origine européenne, dans tous les champs de l'innovation technologique.

Pour autant, dans le domaine du numérique, l'autarcie européenne est impossible. Il est donc utile de réfléchir aux cadres politique et économique dans lesquels le numérique se développe et de chercher à trouver le meilleur équilibre entre la compétition, utile au progrès et à l'innovation, et la coopération, nécessaire à la solidarité.

Le 16 mai 2024, les partenaires du Forum du Numérique et les intervenants présents ont partagé leurs réflexions, leurs travaux, leur expérience et leurs bonnes pratiques.

Contributeurs (28) :

Steven BOURGEOIS, Sophie CAVILLON, David COLON, Arnaud COUSTILLIÈRE, Manuel DAVY, Nicolas DEVAUX, Anne DUBOSCOQ, Adrien FATIBENE, Hervé FÉVRIER, Christophe GOMART, François GORRIEZ, Léo HAMON, Céline HELLER, Anne LE HÉNANFF, Georges LOTIGIER, Alexandre MALAFAYE, Simon MARÉCHAL, Félix VON NOSTITZ, Jean-Paul PINTE, Théo PLANTIER, Jalal POSSIK, Mathias POVSE, Laura SCHAUB, Joséphine STARON, Jérôme TABARIES, Hervé TROALIC, Hugo WEBER, et Belhassen ZOUARI.