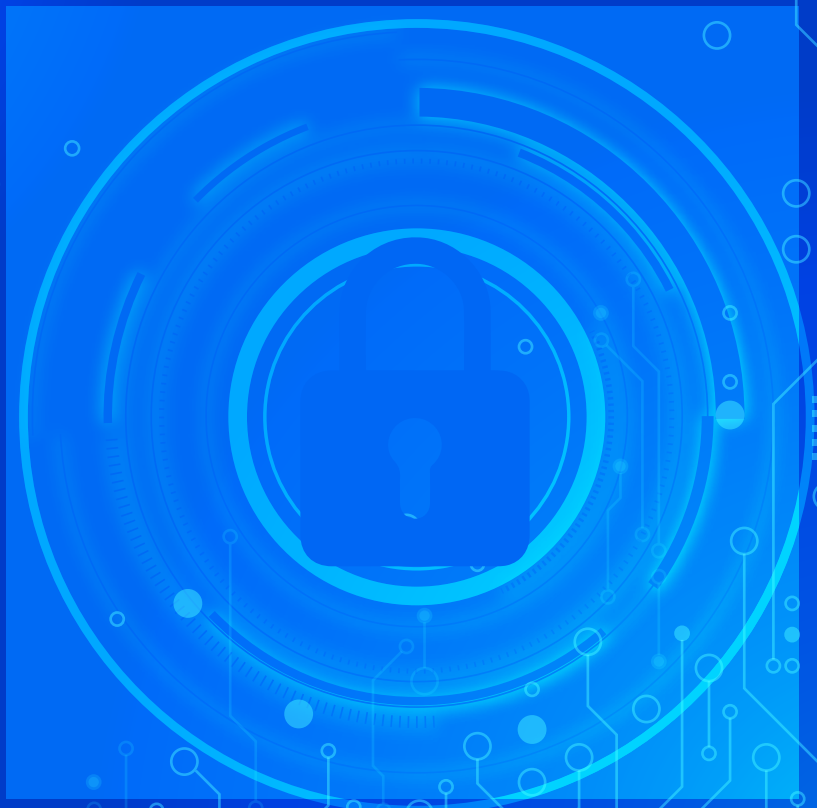
COLLOQUE

CYBERSÉCURITÉ : RÉALITÉS, ENJEUX… COMMENT LES GRANDES ÉCOLES RELÈVENT LES DÉFIS ?

CAMPUS CYBER
7 AVRIL 2022



CONFÉRENCE DES GRANDES ÉCOLES

sommaire

Introduction

MICHEL VAN DEN BERGHE,
directeur du Campus Cyber

Je suis ravi d'accueillir votre colloque au sein de ce campus de 26 000 mètres carrés. Ce projet formé au plus haut niveau de l'Etat accueillera l'ensemble de l'expertise française en termes de cybersécurité, à raison de 30 % de grandes structures, comme Thales, Athos ou Cap Gemini, de 25 % d'instances étatiques comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou le ministère des Armées et de 30 % d'espaces collaboratifs.
L'objectif est de faire travailler ensemble 1800 experts et plus de 100 entreprises d'ici fin juin 2022, pour faire monter le niveau de cybersécurité de la nation.
Trois grands objectifs nous ont été fixés :

- faire rayonner l'excellence française par un lieu totem ;
- rapprocher la recherche, l'innovation et l'enseignement pour faire émerger les licornes de demain ;
- former des experts car plus de 15 000 postes ouverts ne sont pas pourvus et sur 12 000 jeunes suivant une formation numérique, moins de 300 pensent s'orienter vers les métiers de la cybersécurité (dont moins de 10 filles).

Huit écoles seront ouvertes au sein du campus qui s'attache à travailler sur l'attractivité en changeant l'image de la cybersécurité. En effet, plus de quarante métiers existent aujourd'hui dans ce domaine.

« L'objectif est de faire travailler ensemble 1800 experts et plus de 100 entreprises d'ici fin juin 2022, pour faire monter le niveau de cybersécurité de la nation. »

LAURENT CHAMPANEY,
directeur de la Conférence des grandes écoles (CGE)

Merci de nous accueillir sur ce campus qui est effectivement un bel outil au service de la cybersécurité.
En introduction à cette journée, je rappelle que la Conférence des grandes écoles représente 230 écoles de toutes natures, d'ingénieurs pour la moitié et de commerce pour un quart mais aussi de la culture, du design, d'architecture… Toutes ces écoles ont toutes pour caractéristique de former des dirigeants pour les entreprises et les organisations et de faire de la recherche pour préparer leur avenir.
Nous formons des dirigeants en mesure d'imposer des changements dans le comportement des entreprises et des organisations dans le domaine de la cybersécurité.
Nos écoles ont pour métier la formation des jeunes à de nouvelles compétences sur le champ de la technologie de l'information et de la cybersécurité mais aussi des dirigeants actuels tout au long de leur carrière.
Nos écoles font de la recherche pour faire monter la France en compétences et pour protéger nos patrimoines scientifique et culturel.
Enfin, nos écoles sont elles-mêmes des entreprises qui comptent des dirigeants ayant les mêmes problématiques que les autres entreprises, de protéger l'entreprise, les étudiants et leurs données.

« Nous formons des dirigeants en mesure d'imposer des changements dans le comportement des entreprises et des organisations dans le domaine de la cybersécurité. »

LE MONDE AU RYTHME DE LA CYBERSÉCURITÉ : QUELLES RÉALITÉS, QUELS ENJEUX POUR DEMAIN ?

- Laurent Champaney, président de la CGE
- Daniel Benabou, éditeur du « *Guide de la sécurité numérique pour les dirigeant.e.s* », président du CEIDIG et directeur général de l'IDECSI
- Général Marc Boget, commandant de la Gendarmerie dans le cyber espace

PRÉSENTATIONS

GENERAL MARC BOGET

Je suis un officier de Gendarmerie sur titres puisque j'ai commencé ma carrière dans le privé après un diplôme d'ingénieur à l'Ecole nationale supérieure de Mécanique et des Microtechniques de Besançon. J'ai également un cyber de l'Ecole centrale de Paris. Commandant de la Gendarmerie dans le cyberespace, je suis à la fois un opérationnel et un spécialiste des systèmes d'information. J'attends la fin des travaux pour m'installer sur le Cyber Campus. En revanche, les 7000 personnes du pôle cyberespace sont réparties sur l'ensemble du territoire national, outremer compris.

DANIEL BENABOU

J'ai traversé trois grands univers professionnels différents : les médias avec le groupe L'Etudiant, dont j'étais le directeur général délégué, l'édition et le digital avec Vente-Privée.com, avant de rencontrer le cofondateur d'IDECSI, une société française, qui s'est intéressée à la protection des données des dirigeants et des étudiants. J'anime également l'association CEIDIG (pour Conseil de l'Information et de l'Economie du Digital) qui a mené la campagne d'information *Ensemble, protégeons notre économie, protégeons nos entreprises.* Son ambition est que la question de la sécurité numérique devienne naturelle pour l'économie et les entreprises. Cette campagne a mobilisé tous les grands acteurs du numérique. Dans cet esprit, j'ai souhaité que la diffusion du *Guide de la sécurité numérique pour les dirigeant.e.s*, soit relayée par les institutions du monde de l'entreprise, comme le Medef ou la CPME mais aussi par les Grandes écoles et la CGE.

Daniel Benabou, Laurent Champaney et le Général Marc Boget

DÉBAT

LAURENT CHAMPANEY | A la question de savoir s'il existe déjà une communication cyber au sein de la CGE, la réponse est que nous pourrions créer un groupe de travail à l'issue de ce colloque.

Quelle est la nature de la menace ?

G. M. B. | Je vous donne quelques chiffres pour la qualifier :

- le coût de la cyber délinquance à l'international a été estimé entre 6 000 et 7 000 milliards de dollars ;
- un revenu de 1 500 milliards de dollars pour les cyber délinquants ;
- une attaque par rançongiciel toutes les 11 secondes.

Nous constatons trois types de cyber délinquance. Les premières sont les attaques aux vulnérabilités inconnues.
Viennent ensuite les escroqueries de masse (phishing, virements…) pour lesquelles la réponse ne peut pas être uniquement judiciaire car elles sont de faibles montants sur de nombreuses victimes. Christian Rodriguez a doté le pôle cyber d'un grand commandement qui lui est directement rattaché et il lui a confié l'intégralité de la problématique cyber, de la prévention jusqu'à l'investigation, ce qui est assez unique en Europe.
La troisième catégorie est constituée des délinquants multicartes qui achètent des vulnérabilités, de la puissance de calcul, de la puissance de blanchiment. Les rançons en jeu atteignent plusieurs millions de dollars (entre 70 et 100 millions de dollars en moyenne).

« AUJOURD'HUI, IL N'EXISTE PAS D'INDICATEUR NI DE BUDGET SUR LA CYBERSÉCURITÉ DANS LES ENTREPRISES.

L. C. | Comment nos voisins européens sont-ils organisés ?

G. M. B. | La collaboration est la clé du succès. Mes experts sont en contact journalier avec les polices ou les groupes fermés d'experts techniques du monde entier. Côté Police judiciaire, les mécanismes internationaux fonctionnent bien dans le domaine cyber. Sur la partie technique, la Gendarmerie nationale n'a pas accès aux groupes fermés d'experts sans compétence technique.
A la question de savoir si l'éditeur Kaspersky doit être banni de nos systèmes d'information, je vous renvoie à la recommandation de l'ANSSI.
Le contexte ukrainien n'est pas une source d'accélération de la lutte cyber, même si nous observons avec attention ce conflit qui s'est traduit par une prise de position des hackers majoritairement en faveur des Ukrainiens.

L. C. | Daniel, pouvez-vous dresser un état des lieux de l'évolution de la société ?

D. B. | Le patron de la Banque fédérale américaine a indiqué, il y a quelques mois, que le principal risque pour l'économie mondiale russe est d'ordre cyber.
La dynamique de la menace recouvre une véritable industrie, avec des fournisseurs, des conseillers, des développeurs. Ces organisations recherchent davantage de performance. Or la technologie est aussi au service des méchants. Nous sommes donc en compétition avec eux en permanence, ce qui entraîne la sophistication des menaces.
La transformation numérique est extrêmement brutale. Google qui est né il y a vingt ans et Amazon, quatre ans avant, ont fait muter le numérique. Les trois piliers à travailler pour se l'approprier sont la formation, les outils et la réglementation, à renforcer vis-à-vis des délinquants et à l'échelle des entreprises qui sont un peu perdues.
Le niveau de maturité de la sécurité numérique doit rejoindre celui de la sécurité physique.
La culture digitale favorise l'ergonomie, l'accès à nos données, le partage et l'efficacité, ce qui est difficilement compatible avec la sécurité, dont le symbole est un cadenas.

L. C. | Nous avons l'impression que la technique résoudra le problème de sécurité.

D. B. | Au CEIDIG, nous travaillons à déshabiller la sécurité numérique de sa dimension technique pour en faire un sujet stratégique pour les dirigeants.

L. C. | **Passons à la question de la formation. Général, trouvez-vous facilement des experts ?**

G. M. B. | Le marché RH est particulièrement tendu dans le cyber. La ressource est rare. Comme la Gendarmerie ne peut pas lutter avec le privé sur le plan salarial, elle a développé d'autres méthodes pour attirer et fidéliser des talents. Ainsi, 40 % des officiers recrutés ont un profil scientifique. Nous formons l'ensemble des gendarmes au cyber et certains plus spécifiquement pour les faire monter en compétences à la hauteur des enjeux.
Une enquête mondiale de Thales montre que la prise en compte des problématiques cyber est très faible dans les collectivités locales et chez les industriels.
Le déficit de compétences cyber dans tous les métiers pose un réel problème aux entreprises. Les salaires augmentent en raison de la concurrence avec l'offre américaine. Microsoft compte former 250 000 étudiants aux Etats-Unis pour combler la moitié de ce déficit. L'un des sujets majeurs, outre la sensibilisation, est la formation en faisant de la cybersécurité un pôle d'excellence, un moteur d'innovation et une philosophie du partage.

L. C. | **Participez-vous à des actions de sensibilisation auprès des jeunes ?**

G. M. B. | La Gendarmerie participe à un maximum d'actions auprès de jeunes de tous âges pour les éduquer aux risques d'Internet et des lycéens et étudiants post-Bac pour les inciter à intégrer ces filières.
Nous développons une approche pluridisciplinaire pour une prise en compte globale du risque cyber qui n'est pas qu'une affaire de *geeks*. Avec l'association des maires de France, nous avons envoyé le questionnaire *Immunité Cyber* aux 30 000 communes pour leur faire prendre conscience du risque cyber en neuf questions et les accompagner.

L. C. | La formation des dirigeants et des ingénieurs sur la sécurité en entreprise est actuellement tournée vers la sécurité des personnes.
La cybersécurité doit-elle être traitée de la même manière ?

G. M. B. | Le dirigeant doit savoir anticiper le risque, la gestion de la crise technique, la communication de crise, la gestion du personnel et la protection physique des données, par des mesures organisationnelles concernant la segmentation des réseaux ou la sensibilisation des salariés.
La Gendarmerie investit beaucoup sur la sensibilisation des forces vives. Quand une entreprise subit une attaque, je projette toujours un triptyque composé d'un chasseur de la police judiciaire, d'experts techniques et des négociateurs du GIGN pour récupérer des éléments d'enquête.

L. C. | **Vos services sont-ils bien connus des dirigeants ?**

G. M. B. | Pas suffisamment. Pour un dépôt de plainte, il y a environ 250 attaques, d'où la volonté de la Gendarmerie de se structurer pour être plus efficace et plus visible.

L. C. | **Quelle est la responsabilité du dirigeant vis-à-vis de la protection des données de ses salariés ?**

G. M. B. | En cas d'attaque, le dirigeant n'a plus d'outils de travail ni aucun moyen d'action. Il doit gérer ses salariés et ses partenaires et il encourt un risque sérieux de fermer l'entreprise.

L. C. | **Que conseillez-vous en termes de formation des dirigeants ?**

D. B. | Je conseille de lire le guide du CEIDIG *L'Essentiel de la sécurité numérique pour les dirigeants et les dirigeantes*. L'ANSSI édite également des guides.
Mon premier conseil est de faire de la cybersécurité un sujet récurrent des directions et de dresser un état des lieux pour définir ce qui doit être protégé en priorité et comment reconstruire son système d'information en cas d'attaque. Aujourd'hui, il n'existe pas d'indicateur ni de budget sur la cybersécurité dans les entreprises.

L. C. | Ouvrons le sujet de la recherche.
Comment nous situons-nous en France ?

G. M. B. | A noter d'abord que 40 % des ingénieurs cyber sont français. Ils sont reconnus, y compris outre-Atlantique, pour leur qualité. La Gendarmerie dirige un certain nombre de projets européens avec ses partenaires, y compris des structures universitaires de haut niveau.
Il est fondamental d'avoir des experts de haut niveau pour exister au plan technique international.

D. B. | En France, le dispositif d'aide à l'innovation est excellent. En revanche, les ingénieurs ont besoin d'aide pour mettre leur produit sur le marché.

L. C. | **Les résultats de la recherche sont-ils transférés dans les petites et grandes entreprises ?**

D. B. | Une des difficultés des responsables de la sécurité des systèmes d'information (RSSI) est que l'offre de produits cyber est pléthorique. Le marché est en construction. Nous devons donc encourager l'innovation.

L. C. | **Les petites entreprises qui n'ont pas de RSSI sont-elles suffisamment accompagnées ?**

G. M. B. | Global Cyber Alliance labellise des acteurs de cet écosystème. Ce campus est le bon modèle car il regroupe des structures de recherche, de formation, du privé et du public de toutes tailles.

« LES ÉTUDIANTS DEVRAIENT ÊTRE IMPLIQUÉS DANS UN EXERCICE CYBER TROIS OU QUATRE FOIS PAR AN…

L. C. | Deux tiers des écoles de la CGE sont publiques et les enseignants-chercheurs publient beaucoup, sans forcément se protéger. **Nos activités de recherche sont-elles menacées ?**

G. M. B. | Je ne citerai pas le nom d'un grand groupe français de la santé pour qui la protection de la recherche est la priorité suprême. La pépite est la donnée et non les outils. La donnée de recherche doit donc être éminemment protégée. A titre de repère, le budget alloué à la cybersécurité doit représenter 10 à 15 % du budget IT.

L. C. | **Les entreprises ont-elles conscience que leurs données de recherche et développement sont sensibles ?**

D. B. | Jamais assez car ces données constituent leurs bijoux précieux. Des dispositifs accessibles peuvent limiter le risque. Les recommandations de l'ANSSI sont de :
- protéger ce qui est essentiel pour l'activité de l'entreprise, ce qui suppose de l'identifier ;
- se faire conseiller en l'absence de responsable de la sécurité en interne ;
- sauvegarder et gérer ses procédures de restauration qui sont primordiales ;
- instaurer des procédures d'authentification forte et gérer les droits en les distinguant du statut social (un dirigeant n'a pas à avoir accès aux données, s'il n'en a pas besoin).

L. C. | **La recherche fait-elle l'objet d'une guerre entre états ?**

G. M. B. | Oui, les services de renseignements travaillent avec l'ANSSI sur ces menaces qui visent à déstabiliser l'Etat ou à faire de l'espionnage industriel.

L. C. | **Les écoles publiques sont régulièrement inspectées sur la sécurité et la santé au travail. La cybersécurité intégrera-t-elle ces contrôles ?**

G. M. B. | Ne pas considérer le risque cyber au plus haut niveau de l'entreprise est dangereux. Au-delà de la sécurisation technique, il est primordial de sensibiliser les utilisateurs, de réaliser régulièrement des tests de phishing, de travailler sur le plan de continuité d'activité et de se faire auditer régulièrement par un organisme externe. Appréhender la cybersécurité au plus haut niveau offre une vue à 360 degrés.

D. B. | Dans mon entreprise, nous investissons énormément sur la sensibilisation des utilisateurs, pour les aider à mieux gérer la sécurité de leurs données grâce à des outils numériques très puissants.

L. C. | Nos étudiants se situent entre des clients et des collaborateurs, puisqu'ils utilisent notre système d'information interne. Devrions-nous réaliser ces exercices de sécurisation avec eux, au même titre que les exercices d'évacuation ?

G. M. B. | Les étudiants devraient effectivement être impliqués dans un exercice cyber trois

ou quatre fois par an, ce qui accessoirement sécurisera votre réseau.

L. C. | La menace d'un accès physique, par exemple pour voler un disque dur, est peut-être plus forte dans nos écoles.

G. M. B. | Cette menace existe mais des dispositifs permettent de s'en prémunir facilement. La Gendarmerie dispose d'outils nomades chiffrés à la volée. La personne qui volerait mon portable ne pourrait pas l'utiliser.

L. C. | **Une personne rentrant dans l'école et se connectant à un ordinateur peut-elle récupérer les codes d'accès au système d'information ?**

G. M. B. | Oui, elle pourra exécuter un programme pour utiliser une vulnérabilité du poste pour pénétrer le système d'information.

L. C. | **L'usurpation d'identité liée à la sécurisation des diplômes est-elle un risque majeur ?**

G. M. B. | Ce risque existe depuis très longtemps. Dans le cyber, il semble toutefois plus difficile de faire illusion.

L. C. | **Le contrôle des diplômes est-il une préoccupation des entreprises ?**

D. B. | Sur LinkedIn, des personnes s'inventent effectivement un parcours mais le contrôle des références auprès de l'établissement permet de contourner cet écueil.

> « AUCUNE SOCIÉTÉ DÉMOCRATIQUE STABLE ET PERFORMANTE NE PEUT FONCTIONNER SANS CYBERSÉCURITÉ.

G. M. B. | Un participant suggère d'utiliser le *gaming* pour sensibiliser les étudiants. La Gendarmerie investit dans ce domaine car il existe des initiatives très intéressantes.

L. C. | Combien d'écoles font des exercices cyber ? L'Etat pilote des exercices de gestion de crise liée à des accidents ou à des intrusions.

G. M. B. | Je ne pense pas que ces exercices sont applicables aux écoles mais les gendarmes peuvent travailler avec elles. Les écoles ont de la ressource pour jouer le rôle de l'écosystème extérieur et stresser la structure.

L. C. | Le niveau de rémunération et les conditions de recherche en France sont confrontés à la concurrence américaine.

G. M. B. | Les jeunes qui s'intéressent au cyber ne sont pas uniquement motivés par le salaire mais par l'intérêt du travail au quotidien.

D. B. | En résumé, aucune société démocratique stable et performante ne peut fonctionner sans cybersécurité.

FORMATION DES ÉTUDIANTS AUX MÉTIERS ET ENJEUX DE DÉFENSE, SÉCURITÉ, CYBERSÉCURITÉ : QUELLE PLACE DES GRANDES ECOLES ?

- Joël Courtois, conseiller spécial du directeur général, chargé de la cybersécurité de l'École pour l'informatique et les techniques avancées (EPITA)
- Didier Danet, directeur du master spécialisé Opérations et gestion des crises en cyber défense de l'Académie militaire de Saint-Cyr Coëtquidan
- Mylène Jarossay, Chief Information Security Officer au sein du groupe LVMH et présidente du Club des experts de la sécurité de l'information et du numérique (CESIN)
- Rémy Février, maître de conférences de l'équipe Sécurité-Défense-Renseignement du Conservatoire national des arts et métiers (CNAM) et ancien officier supérieur de la Gendarmerie nationale

PRÉSENTATIONS

JOËL COURTOIS

Nous attendons du Campus Cyber qu'il permette à tous les acteurs de communiquer pour faire progresser le niveau des entreprises. Des groupes de travail sont dédiés à la définition des métiers (des référentiels métiers ont été développés par l'ANSSI et par certaines entreprises) et des compétences nécessaires. Cette matrice croisée sera mise à la disposition des écoles, afin qu'elles bâtissent des cursus en phase avec les besoins.

Didier Danet, Joël Courtois, Mylène Jarossay et Rémy Février

MYLENE JAROSSAY

La place et la dépendance au numérique sont extrêmement fortes. Tous les métiers contribuent à la cybersécurité car les délinquants utilisent, outre de la technologie, de l'ingénierie sociale. Les entreprises doivent donc s'appuyer sur divers procédés pour se défendre (des processus, de la technologie, de l'organisation, du droit…). La compréhension du risque cyber est transversal à tous les métiers. Nous espérons que toutes les écoles s'emparent du sujet cyber pour développer une compétence minimale dans tous les métiers.

DIDIER DANET

L'Ecole de Saint-Cyr Coëtquidan est à la fois une école d'ingénieurs et de sciences sociales et politiques. La cyber défense s'est développée en trois temps :

- dans les années 90 (cf. « *Cyberwar is coming* »), nous dépendons d'Internet qui est fragile, il convient donc de protéger les systèmes d'information et de sensibiliser les utilisateurs ;
- en 2014, le pacte cyber défense est déployé par le ministère de la Défense qui considère que le cyber est un champ de bataille nécessitant de développer une stratégie défensive et offensive et d'anticiper les risques et la gestion des crises ;
- plus récemment, le chef d'Etat-Major des Armées estime que :
  - le cyber n'est pas un espace isolé, il se fond dans des champs immatériels créés par l'homme (les champs électromagnétiques, le cyber et les perceptions) qui s'interpénètrent dans les milieux naturels ;
  - la conflictualité intervient avant la guerre, sous le seuil du conflit armé. Nous formons donc nos élèves sur ces trois couches successives.

DÉBAT

J. C. | Le CNAM a-t-il également segmenté cette problématique ?

RÉMY FÉVRIER | Le cyber n'est effectivement pas une dimension à part. Au CNAM, nous avons créé le premier certificat de spécialisation de renseignement économique.
Comment établir un projet stratégique d'entreprise sans volet SI et cyber ? Je milite pour l'intégration de la cyber dans la stratégie des entreprises.
De même, la cybersécurité ne doit pas être limitée aux écoles de commerce et d'ingénieurs. La CGE est pionnière. Pour être intervenu dans une vingtaine d'établissements, je suis toujours surpris de l'appétence des élèves et des professeurs pour la cybersécurité. L'avenir est à une fusion entre écoles de commerce et écoles d'ingénieurs. La DSI n'est toujours qu'une fonction support dans l'entreprise, sans rôle stratégique. Au-delà de leur formation initiale d'ingénieurs et de manager, les top managers enclins à connaître la technique doivent devenir des interlocuteurs crédibles pour la direction générale.

J. C. | La cybersécurité est-elle un critère de recrutement d'un commercial de LVMH ?

M. J. | Non mais la cybersécurité doit effectivement rentrer dans la culture d'entreprise. Les COMEX en ont maintenant conscience, du fait des événements cyber majeurs que subissent les entreprises depuis trois ans. Les directeurs cyber doivent pouvoir expliquer à tous les métiers qu'ils participent à la chaîne de défense.

J. C. | Les acteurs de l'entreprise déjà en place doivent être formés, en commençant par le plus haut niveau.

R. F. | J'ai animé de nombreuses conférences devant des patrons de grands groupes. Leur expliquer qu'ils auront des problèmes si l'intégrité des données personnelles (de clients et salariés) confiées à leur entreprise permet de renforcer leur écoute. Plus de 95 % des entreprises françaises ont toutefois moins de 20 salariés et leur PDG pense avant tout à la pérennité de l'entreprise, dont la cybersécurité leur semble très éloignée.

J. C. | Le risque juridique de responsabilité personnelle du dirigeant, le risque financier fort pour l'entreprise et l'ingénierie sociale utilisée par les délinquants (par la mise sur écoute de ses proches, par exemple) font réagir les dirigeants.

M. J. | Comme les menaces évoluent, les méthodes de défense doivent être renouvelées en permanence.

D. D. | Nous ne pouvons effectivement pas concevoir une formation cyber sans des équipes de recherche qui travaillent sur les menaces de demain. Dans le domaine militaire, les enjeux diffèrent mais l'ingénierie sociale est également utilisée pour agir sur les militaires en opération.

« L'AVENIR EST À UNE FUSION ENTRE ÉCOLES DE COMMERCE ET ÉCOLES D'INGÉNIEURS.

« LA COLONNE VERTÉBRALE D'UNE ENTREPRISE EST LE SYSTÈME D'INFORMATION.

M. J. | La cellule de crise traduit la nécessaire pluridisciplinarité des formations.

D. D. | Des psychologues sont avant tout nécessaires en ingénierie sociale. En tant qu'enseignant en sciences de gestion, je constate les liens entre le marketing et les actions dans le domaine de l'influence et du renseignement.

J. C. | Il convient certainement de sensibiliser les directeurs de formation.

R. F. | La cybersécurité doit servir de catalyseur de rapprochement entre les métiers.

J. C. | Nous pouvons en tirer les premiers enseignements :

- inciter les écoles à croiser leurs spécialités ;
- monter des formations pour les acteurs des entreprises en place ;
- motiver plus de jeunes à intégrer ces métiers, 15 000 postes ne trouvant pas de candidats.

Quels leviers activer pour motiver les jeunes ?

M. J. | La diversité de ces métiers d'aventure qui se renouvellent constamment peut attirer les jeunes qui ont le goût du mouvement. Ces métiers requièrent de l'investissement et de l'engagement personnel.

R. F. | Les élèves sortant des Grandes écoles de commerce sont complexés vis-à-vis du domaine technique, alors que des jeunes trouveront leur place pour sécuriser les entreprises.

J. C. | **Peinez-vous à recruter dans les masters spécialisés ?**

D. D. | Mon problème est de convaincre un jeune qui s'est engagé dans l'institution pour être chef d'infanterie que la cybersécurité fait partie de son métier, y compris en tant que capitaine sur le terrain. Je démontre, au travers du renseignement, que la lutte informatique est aussi l'affaire des personnes parlant des langues étrangères.

Les entreprises devraient se rapprocher de l'administration et du monde militaire pour croiser les expériences.

J. C. | **Sur quels types d'activité de recherche les élèves d'une école d'ingénieurs peuvent-ils être impliqués ?**

D. D. | Nous les impliquons dans des projets de recherche sur l'intelligence artificielle et l'influence. Nous organisons plus largement des *policy challenges* pour faire comprendre aux élèves comment appréhender globalement une problématique cyber en jouant le rôle d'un conseiller de gouvernement.

R. F. | Nos élèves juristes n'ont *a priori* pas d'appétence pour la cybersécurité, puis ils découvrent les liens avec le Règlement général sur la protection des données (RGPD). La recherche en cybersécurité est pour moi un sous-ensemble de la sécurité économique, sur laquelle nous avons du retard à rattraper par rapport à des pays alliés qui mènent une guerre souterraine.
La part technique devient aujourd'hui minoritaire. La colonne vertébrale d'une entreprise est le système d'information. Le développement des ERP en mode SaaS revient à confier ses applications et ses données à des prestataires à travers le monde, sous couvert de réduction des coûts. Les informations stratégiques devraient *a minima* être conservées au sein de l'entreprise.

J. C. | Dans le domaine de l'intelligence artificielle, le plus important est la sélection des données.

D. D. | C'est pourquoi nous réunissons, tout comme le groupe de recherche Geode (géopolitique de la data sphère) des ingénieurs informaticiens et des spécialistes des sciences sociales.

M. J. | Il y a un an, le logiciel standard SolarWinds a été infiltré et la version diffusée a atteint 15 000 clients. Les juristes devraient apporter leur éclairage sur la sécurité des logiciels achetés.

D. D. | La nécessité de travailler avec des juristes n'est pas propre à la cybersécurité. L'ESSEC travaille sur le droit en tant que technique au service du management. Nous manquons de juristes stratèges.

J. C. | Ce domaine est passionnant mais nous peinons à le démontrer à nos jeunes. Aujourd'hui, la cybersécurité fait partie des mots-clés de Parcoursup. Le ministère devrait attirer l'attention de tous les CIO sur ces nouveaux métiers.

D. D. | Le pôle d'excellence cyber de Rennes qui a une vocation nationale, a réalisé un important travail de recensement.

J. C. | **En tant que recruteurs, que pensez-vous de la certification Pix ?**

M. J. | Au-delà des certifications, j'observe le parcours du candidat et les projets sur lesquels le jeune a travaillé.

J. C. | La certification Pix s'intéresse aux plus jeunes. Dans les collèges et lycées, les formations informatiques n'évoquent quasiment pas la cybersécurité, jugée trop compliquée.

M. J. | La complexité ne doit pas être un frein. J'en veux pour preuve les expériences d'apprentissage de la philosophie à des enfants de six ans.

R. F. | Les décideurs subissent les SI plus souvent qu'ils ne les accompagnent. Un vrai travail d'influence doit être mené auprès des décideurs ministériels.
Je suis impressionné par la réceptivité des jeunes au risque numérique depuis cinq ans. Les jeunes commencent à prendre du recul par rapport au numérique.

D. D. | Nous ne partons pas de rien. En géographie, les professeurs traitent des routes numériques. En histoire, les confrontations entre puissances sont également numériques. Nous devons maintenant réaliser un état des lieux pour identifier les manques et sensibiliser les jeunes sans commencer par la technique, par exemple au travers du harcèlement.

J. C. | Un groupe de travail du Campus Cyber porte sur les vocations et la féminisation. **Pourquoi n'y a-t-il pas plus de femmes dans ces métiers ?**

R. F. | Beaucoup de femmes s'autocensurent sous le poids de l'histoire. Les femmes sont pourtant souvent moins naïves et vulnérables que les hommes.

D. D. | Le domaine cyber compte entre 10 et 12 % de femmes mais les métiers des relations internationales, de la psychologie et du droit sont beaucoup plus féminisés.

M. J. | Je suis convaincue que l'équilibre sera atteint car les métiers passionnants du cyber ne sont pas genrés. En outre, la diversité au sens large favorise la qualité de la défense.

J. C. | La recherche de compétences des entreprises s'est beaucoup diversifiée, comme pour l'intelligence artificielle. La mission des Grandes écoles est de proposer des programmes de formation intégrant la cybersécurité.

R. F. | L'un des enjeux des *smart buildings* intégrant de l'intelligence artificielle est de recruter des personnes capables de contrer des attaques dès leur construction (le « *hacking by design* »).

J. C. | Les métiers du luxe gèrent aussi de nombreuses données sensibles. Ils doivent donc être sensibilisés à la fuite de données.

M. J. | Toutes les entreprises doivent protéger leurs secrets (de fabrication, de stratégie commerciale, de ses salariés et de ses clients). Les cabinets d'architecte qui publient sur des espaces partagés, doivent apprendre à protéger leur patrimoine.

« JE SUIS CONVAINCUE QUE L'ÉQUILIBRE SERA ATTEINT CAR LES MÉTIERS PASSIONNANTS DU CYBER NE SONT PAS GENRÉS. EN OUTRE, LA DIVERSITÉ AU SENS LARGE FAVORISE LA QUALITÉ DE LA DÉFENSE.

J. C. | Des outils développés en France sont pourtant très performants pour protéger les données.

R. F. | Il existe un phénomène de snobisme. Dans un pôle de compétitivité, j'ai découvert un

serveur dont l'infogérant était une filiale d'un grand groupe étranger. Le dirigeant n'a pas souhaité changer de prestataire appartenant à un groupe prestigieux. Le *branding* nuit à l'écosystème national.

J. C. | Pour favoriser l'attractivité, je souhaite publier des capsules vidéo. Nous travaillons également sur un jeu vidéo pour apprendre à utiliser les outils en y intégrant une dimension sociale. Les entreprises du campus sont censées collaborer à cet effort de formation.

R. F. | Aucune école ne peut plus se passer de filières cyber. Elles doivent injecter des unités d'enseignement cyber tout au long du parcours de l'élève pour amener des jeunes au management des systèmes de cyber informations. Même s'ils n'en font pas leur métier, ils devront savoir réagir face aux menaces relevées par le RSSI.

« AUCUNE ÉCOLE NE PEUT PLUS SE PASSER DE FILIÈRES CYBER. ELLES DOIVENT INJECTER DES UNITÉS D'ENSEIGNEMENT CYBER TOUT AU LONG DU PARCOURS DE L'ÉLÈVE POUR AMENER DES JEUNES AU MANAGEMENT DES SYSTÈMES DE CYBER INFORMATIONS. MÊME S'ILS N'EN FONT PAS LEUR MÉTIER, ILS DEVRONT SAVOIR RÉAGIR FACE AUX MENACES RELEVÉES PAR LE RSSI.

M. J. | Je suis d'accord sur la nécessité d'éveiller la réflexion des jeunes sur les risques cyber dans l'exercice de leur métier, quelle que soit leur discipline.

J. C. | La sécurisation des IoTs renvoie à la sensibilisation cyber à l'intérieur même des formations d'ingénieurs dans des domaines autres que l'informatique.

D. D. | Des élèves militaires utilisaient un logiciel pour mesurer leur performance sur leurs parcours qui les localisaient. Les IoTs sont un enjeu de sécurité pour tout le monde.

R. F. | La vulnérabilité des systèmes d'information industriels est ce qui m'effraie le plus pour le pays car ils ont une durée de vie très longue. Ils ont donc été conçus à une époque où il n'était pas imaginable qu'ils puissent être connectés.

D. D. | C'est pourquoi les hôpitaux peinent à sécuriser leur SI qui datent d'époques lointaines.

J. C. | Concevoir des systèmes intelligents tout en conservant la main sur le niveau de sécurité est un vrai défi.

En conclusion, venez nous rejoindre dans la cybersécurité car ces métiers sont passionnants !

CYBER GUERRE : LA RECHERCHE AU CENTRE DE TOUTES LES CONVOITISES

- François Dellacherie, directeur général de Télécom SudParis
- Hakima Chaouchi, conseillère scientifique sur la stratégie de recherche et d'innovation en TIC au ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation
- Nicolas Glady, directeur général de Télécom Paris et président de la commission Aval de la CGE
- Hubert Duault, responsable de programme Cybersécurité de l'Institut national de recherche en informatique et en automatique (INRIA)

DÉBAT

FRANÇOIS DELLACHERIE

La cyber guerre met en jeu la souveraineté numérique. **Quels sont les impacts croisés entre la souveraineté numérique et l'évolution de la gouvernance sur Internet ?**

HAKIMA CHAOUCHI

Internet est un ensemble de réseaux gérés de manière indépendante et tissés ensemble par des protocoles de communication distribués à l'échelle mondiale. Le *cloud* a permis d'utiliser le numérique dans les domaines industriels, sociétaux et gouvernementaux.
La souveraineté numérique doit être intégrée dans la gouvernance de l'Internet pour répondre aux besoins gouvernementaux, industriels et militaires. Nous recommandons trois champs d'action :

- impliquer les acteurs dans les travaux de l'organisation mondiale Internet Governance Forum, dont la Branche France a été créée en 2004 ;
- coordonner les travaux sur la puissance de calcul, le contrôle des données et la connectivité sécurisée ;
- développer les compétences pour construire, utiliser et maintenir le cyber espace.

HUBERT DUAULT

Dans le cadre du plan de relance et du soutien de la souveraineté numérique, l'INRIA est impliqué sur deux axes : le soutien à la recherche et le programme de transfert du Campus Cyber pour le compte de l'ensemble de la communauté académique.

Ce programme se décline en quatre volets sur cinq ans :

- la détection, la mise en œuvre et le portage de projets de recherche ;
- le financement de projets de transfert de la recherche ;
- le transfert des compétences de recherche ;
- la promotion de l'entreprenariat dans le monde académique en accompagnant les doctorants.

François Dellacherie, Hakima Chaouchi, Nicolas Glady, Hubert Duault

F. D. | Pourquoi l'un des enjeux de la cybersécurité est-il la formation ?

NICOLAS GLADY | Le recrutement est une préoccupation pour 58 % des dirigeants, en particulier dans le secteur numérique. Les espaces informationnels sont des espaces de conquête à défendre. Les métiers de la cybersécurité sont très larges. La cybersécurité doit être inscrite dans le *design* de chaque outil car les attaques se multiplient. Les utilisateurs eux-mêmes doivent être sensibilisés car la force de la chaîne dépend du maillon le plus faible. L'enjeu est gigantesque car nous n'avons pas les compétences pointues pour sécuriser nos infrastructures numériques et les utilisateurs sont insuffisamment sensibilisés.

« LES UTILISATEURS EUX-MÊMES DOIVENT ÊTRE SENSIBILISÉS CAR LA FORCE DE LA CHAÎNE DÉPEND DU MAILLON LE PLUS FAIBLE. L'ENJEU EST GIGANTESQUE CAR NOUS N'AVONS PAS LES COMPÉTENCES POINTUES POUR SÉCURISER NOS INFRASTRUCTURES NUMÉRIQUES ET LES UTILISATEURS SONT INSUFFISAMMENT SENSIBILISÉS.

H. C. | Comment la menace cyber évolue-t-elle en général et dans l'enseignement supérieur en particulier ?

F. D. | Elle augmente, se professionnalise et se diversifie. La surface d'attaque a augmenté au début des années 2000, date de création de l'ANSSI.
La cyber guerre était l'apanage des Etats. Aujourd'hui, des sociétés fournissent des services d'attaque informatique. Tout le monde peut attaquer tout le monde. Avant, les PME et TPE n'étaient pas victimes. En 2020, de nombreux *ransomwares* visaient à détruire des entreprises ou à leur extorquer une rançon. En 2021, l'ANSSI dénombrait une attaque quotidienne par *ransomware*.
Nos Grandes écoles sont des PME qui offrent une surface d'attaque numérique, qui auraient les moyens de payer une rançon et qui seraient déstabilisées par une cyber attaque.

Quels sont les principaux enjeux du programme de transfert opéré par l'INRIA ?

H. D. | Les enjeux du Campus Cyber sont de développer les solutions innovantes et souveraines pour assurer la confiance numérique dans notre environnement. Le programme de transfert vise à réaffirmer le rôle de la recherche.
Le premier enjeu sera de faire travailler ensemble les communautés de la recherche, des grandes entreprises et des PME innovantes. Notre rôle sera d'animer leurs échanges.
Le deuxième sera d'accroître les compétences disponibles en favorisant des cursus mixtes évolutifs pour les ingénieurs.
Le troisième sera d'accompagner l'entreprenariat en créant des cursus entrepreneuriaux.

F. D. | Quels sont les dispositifs pour la formation et comment les financer ?

N. G. | Nos écoles rencontrent un problème de capacité. L'approche doit être fondée sur trois piliers : l'école, l'Etat et les grandes entreprises. Je propose que l'Etat offre un cadre permettant d'assurer la certification et la diplomation, que les écoles maillent le territoire et que les entreprises mettent leurs experts à la disposition de la formation.
Nous n'aurons pas suffisamment de personnes pour répondre aux enjeux si nous ne formons que les jeunes ingénieurs. Les seniors qui ont déjà des compétences technologiques et informatiques pourraient être formés sur des blocs de compétences complémentaires de 100 à 200 heures de cours par des vacataires des écoles qui garantiraient la formation.
Par ailleurs, la VAE combinée à cette logique de bloc pourrait aboutir à des diplômes à moindre coût pour l'Etat.

F. D. | Comment la Recherche appréhende-t-elle la souveraineté numérique ?

H. C. | En cybersécurité, la recherche scientifique y voit l'opportunité d'identifier de nouveaux verrous et de développer de nouvelles solutions technologiques. Les autres communautés de recherche y voient un frein à la visibilité de leur travail de recherche, la recherche étant fondée sur la publication internationale (hormis pour les travaux régaliens).
L'ouverture des données ne signifie pas que la souveraineté numérique n'est pas garantie.
Le dispositif du ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation (MESRI) pour la protection du potentiel scientifique et technique a été revisité en 2011 et plus récemment dans le cadre de la doctrine

du « *cloud* au centre » pour la protection des services informatiques de l'Etat.
La stratégie d'accélération de la 5G et de la 6G pourrait faire évoluer la clôture des chercheurs et le processus d'évaluation des travaux de recherche.

H. D. | Face au paradoxe entre la publication des résultats de la recherche et la nécessité de se protéger, quelles sont les solutions existantes pour les chercheurs ?

F. D. | L'Etat protège ses citoyens et ses chercheurs. L'ANSSI, rattachée aux services du Premier ministre, interagit de plus en plus avec le monde éducatif et de la recherche. La direction générale de la sécurité intérieure (DGSI) renforce ses missions au profit de l'enseignement supérieur, explique comment la menace évolue et quel équilibre trouver pour s'en protéger alors que le métier de chercheur implique de partager ses résultats.
En tant que directeur d'école, quels sont les autres piliers de la cyber défense ?

N. G. | En 2022, une école d'excellence doit être adossée à la recherche, afin de s'assurer que l'enseignement reste à la pointe des connaissances. Dans une école d'ingénieurs, la recherche est ancrée dans l'ADN. Les écoles ne sont plus compétitives en termes salariaux, de budget de recherche et de conditions de travail par rapport au privé et aux autres pays européens. Nous avons un problème d'attractivité et de rétention.

F. D. | Quelles sont les autres actions de l'Etat pour protéger les données de la recherche ?

H. C. | Des attaques ciblent spécifiquement les données de recherche, hébergées dans un *cloud* non souverain. La recherche est considérée comme un élément essentiel de la souveraineté numérique. L'Etat a donc embarqué la recherche scientifique dans sa stratégie d'accélération industrielle, dans un objectif de développement de solutions logicielles et matérielles pour garantir la souveraineté numérique. France 2030 et le PIA 4 s'appuient sur les territoires pour développer ces solutions et organiser ces stratégies d'accélération.
Le MESRI a investi dans les infrastructures numériques de recherche dès le PIA 3 au travers de différents instruments. Je peux citer le contrat de plan État-région (CPER), le réseau national de télécommunications pour la technologie, l'enseignement et la recherche (RENATER) et le grand équipement national de calcul intensif (GENCI). Le développement d'outils collaboratifs vise à rendre les chercheurs autonomes vis-à-vis des GAFAM. Pour répondre à ces besoins, nous avons également besoin d'une bonne articulation entre les outils, comme les pôles universitaires d'innovation et le programme ANR Excellence de l'Agence nationale de la recherche.

> « EN 2022, UNE ÉCOLE D'EXCELLENCE DOIT ÊTRE ADOSSÉE À LA RECHERCHE, AFIN DE S'ASSURER QUE L'ENSEIGNEMENT RESTE À LA POINTE DES CONNAISSANCES.

F. D. | En quoi le Campus Cyber est-il un facteur de réussite pour le programme de transfert ?

H. D. | Le campus offre des lieux propices aux échanges, aux expérimentations, aux interactions entre communautés.

F. D. | Les étudiants qui choisissent la filière cyber s'y épanouissent mais nous peinons à en attirer davantage, faute de suffisamment d'ouverture. Nous devons démontrer que la cybersécurité touche tous les métiers pour convaincre les étudiants de l'existence d'un écosystème dans lequel il est possible d'exercer tout au long de sa carrière.

N. G. | A la question de savoir quels sont les métiers essentiels pour appréhender le risque cyber, je vous renvoie au rapport de l'ANSSI « *Panorama des métiers de la cybersécurité 2020* » et à la note de *Talents du numérique* sur les compétences en cybersécurité en 2019.
Les salaires s'élèvent de 40 à 55 k€ par an à la sortie de l'école et à plus de 70 k€ pour les profils confirmés. Les recrutements s'opèrent à partir de Bac+3 sur des métiers qui ne sont pas seulement techniques.

F. D. | Compte tenu de l'importance de la notion numérique d'usage, nous prévoyons un futur colloque sur la santé et le numérique.
La Covid a été un accélérateur des attaques (+30 % entre 2020 et 2021 selon le rapport de l'ANSSI) car elle a aussi accéléré de façon durable nos usages numériques.

H. C. | La protection du potentiel scientifique et technique (PPST) est un très ancien dispositif du MESRI. Ses déclinaisons les plus récentes concernent les services de l'Etat, dont la recherche publique. Les investissements du MESRI dans les infrastructures numériques et de recherche sont très importants. L'objectif à long terme est de mutualiser les données de la recherche dans des infrastructures maîtrisées et autonomes.

N. G. | Selon un participant, les lycées manquent d'informations sur la cybersécurité pour orienter les élèves. Un travail de clarification reste à mener auprès des enseignants.

H. C. | La stratégie d'accélération cyber portée par l'ANSSI passera par les acteurs de l'enseignement. Une action de sensibilisation qui concerne tous les citoyens, pourrait cibler les lycées. J'ajoute une action du ministère de l'Emploi pour orienter les jeunes vers la cybersécurité.

« NOUS DEVONS DÉMONTRER QUE LA CYBERSÉCURITÉ TOUCHE TOUS LES MÉTIERS POUR CONVAINCRE LES ÉTUDIANTS DE L'EXISTENCE D'UN ÉCOSYSTÈME DANS LEQUEL IL EST POSSIBLE D'EXERCER TOUT AU LONG DE SA CARRIÈRE.

H. D. | Un groupe de travail du Campus Cyber œuvre pour la mise en place d'une plateforme numérique des parcours de formation, dont certains seront présentés à des lycéens.

F. D. | La ludification de la cybersécurité est très importante pour s'adresser aux lycéens. Le concours proposé par l'Education nationale depuis plusieurs années est un premier exemple. Nous devons tous réfléchir à la façon de toucher les plus jeunes.

H. C. | **Pensez-vous réussir le défi de la parité dans les écoles dédiées au numérique ?**

N. G. | A mon arrivée en 2017, les filles étaient 17 %. Aujourd'hui, elles sont 22 % et nous visons 30 %. Il y a toutefois de moins en moins de filles dans les filières techniques et technologiques. Je pense que nous devons adopter des solutions plus pragmatiques, comme l'application de quotas.

F. D. | Je rejoins cet objectif pour nos écoles du numérique. Le défi est encore plus grand dans le domaine de la cybersécurité. Je reste optimiste car les participants au concours de crypto sont à parité totale et la démocratisation de la cybersécurité réduira l'écart entre numérique et cybersécurité.

N. G. | La fondation Femmes@numérique a lancé un appel à projets pour augmenter le nombre de filles dans les formations.
A Télécom Paris, les formations numériques ne souffrent pas d'un déficit d'attractivité pour les filles mais d'un problème de filières. La sensibilisation et la formation ne suffiront pas à atteindre la parité.

QUELLES PROTECTIONS ET GARANTIES POUR LES GRANDES ÉCOLES ET LEURS ÉTUDIANTS ?

- Robert Erra, directeur du Bachelor cybersécurité et professeur d'informatique en licence
- Foucauld Kneuss, chargé de mission auprès de la vice-présidence du Bureau national des étudiants en école de management (BNEM)
- Pierre Landais, adjoint à la vice-présidence en charge du réseau Bureau national des élèves ingénieurs (BNEI)
- Luc Jarry-Lacombe, expert du Comité habilitation numérique (CHN) de la CGE et CEO de BCdiploma
- Julien Nocetti, titulaire de la chaire Gouvernance du risque cyber de Rennes School of Business, membre du Pôle d'excellence cyber (PEC)
- Marion Arnould, élève ingénieure 4ème année de l'EPITA

DÉBAT

LUC JARRY-LACOMBE | BCdiploma est une société que j'ai co-créée il y a quatre ans. Elle certifie des diplômes en installant une application dans les établissements d'enseignement supérieur, afin d'émettre des diplômes 100 % numérique infalsifiable que les titulaires peuvent partager.

Les écoles ont pour obligation de conserver intègres des données personnelles pour délivrer des attestations de diplômes pendant très longtemps. La cybersécurité à long terme n'étant pas le métier premier d'un SI d'une école, nous créons un registre stable et pérenne ne pouvant pas être perdu ou hacké.
Nous travaillons sur le partage des données pour permettre à l'étudiant de présenter une attestation digitale sûre et intègre à un recruteur.
Nous utilisons une technologie brevetée, pour délivrer à un tiers une lecture en temps réel du registre de *blockchain* sous réserve des droits.
L'utilisation est simplissime. Nous travaillons avec les dernières générations de *blockchain*, dont la consommation énergétique est très intéressante.

ROBERT ERRA | Vous sécurisez le diplôme et non les résultats.

L. J.-L. | Notre outil permet de sécuriser toutes sortes de données. Nous travaillons aussi pour la finance sous certification ISO.

R. E. | La politique de sécurité ne semble pas être un critère de choix d'une école.

Foucauld Kneuss, Luc Jarry-Lacombe, Marion Arnould, Robert Erra, Julien Nocetti

FOUCAULD KNEUSS | Je pense que c'est un critère de choix pour certains étudiants, conscients des enjeux de la cybersécurité.

Il convient de mettre en avant les cyber attaques pour démontrer aux étudiants que le sujet n'est pas anodin.

MARION ARNOULD | J'ai commencé à m'y intéresser grâce aux sensibilisations en école.

> « LA FRANCE A DES FILIÈRES D'EXCELLENCE À METTRE EN AVANT POUR HYBRIDER SES PROFILS ET LES ACCULTURER AU CYBER.

PIERRE LANDAIS | Je confirme que la sensibilisation des étudiants fait défaut, avant et pendant leurs études. Des exercices similaires aux alertes incendie pourraient être organisés.

Les étudiants attendent des écoles que leurs systèmes soient opérationnels en permanence et que leurs choix technologiques respectent leurs données personnelles.

R. E. | Les étudiants laissent des traces numériques partout. Savez-vous comment les écoles géreront vos données ?

M. A. | Nous avons été sensibilisés au droit de rectification ou de suppression de nos données. Tous les étudiants ne l'exercent pas car ils ne comprennent pas tout à fait l'enjeu.

R. E. | Comment faire cohabiter les réseaux sociaux et la sensibilisation aux bonnes pratiques de sécurité des données ?

JULIEN NOCETTI | Les enjeux microscopiques sont très concrets mais les enjeux macroscopiques nous dépassent.

Les DSI, les DRH et les Directeurs financiers voient leur métier évoluer avec le risque cyber. La Grande-Bretagne et les Etats-Unis sont plus avancés mais la France a des filières d'excellence à mettre en avant pour hybrider ses profils et les acculturer au cyber.
La communication est très importante en cas de *ransomware*. Les PME ne communiquent pas et ne portent pas plainte alors que l'inverse est recommandé pour sortir de l'isolement et pouvoir mener une démarche collective.

R. E. | Est-il conseillé aux étudiants en stage à l'étranger de ne pas ramener de données confidentielles à la maison ?

P. L. | Nos tuteurs ont l'obligation de contrôler tout ce que nous communiquerons à l'école pour supprimer les données sensibles.

L. J.-L. | Nous passons une demi-journée sur la cybersécurité avec nos stagiaires et apprentis car les impacts économiques sont majeurs pour une société.

M. A. | Epita nous a demandé de faire relire et signer nos documents par nos maîtres de stage. L'entreprise nous demandait de bloquer notre PC le soir et de veiller aux données. Nous n'avions pas accès à une salle sécurisée.

R. E. | Confirmez-vous l'exigence de la Commission nationale de l'informatique et des libertés (CNIL) sur les diplômes qui ne pourraient pas être stockés tels quels mais seulement les données constitutives permettant de les générer de nombre ?

L. J.-L. | Notre premier sujet de recherche est de faire profiter de la puissance de sécurité de stockage à long terme des environnements décentralisés. Il n'est pas question de stocker des documents contenant des données personnelles. Après un an et demi de recherche, nous avons obtenu un brevet en première lecture aux Etats-Unis pour stocker de la donnée chiffrée dans un environnement public et utiliser un système de cryptage pour donner des droits d'accès et de suppression.

R. E. | Combien d'écoles utilisent votre système ?

L. J.-L. | En moins de trois ans, 120 établissements l'ont adopté dans 19 pays.

R. E. | L'obligation de conserver un diplôme pendant 50 ans est contradictoire avec le RGPD. Selon moi, mieux vaut violer le règlement et

permettre aux étudiants de prouver qu'ils sont diplômés. En revanche, les notes ne doivent pas être conservées.
La CGE a mis en place un système prouvant qu'un étudiant est diplômé d'une de ses écoles labellisées.

F. K. | Dans les écoles de management, l'acculturation aux sujets cyber me paraît importante pour pouvoir se positionner en tant que membre du CODIR.

J. N. | Rendre la cybersécurité intelligible aux CODIR est un enjeu car ils la considèrent généralement comme une menace ou une dépense.

R. E. | Je milite pour que la cybersécurité fasse partie de toutes les formations, au même titre que l'informatique. Un stagiaire a accès au SI, alors qu'effacer toutes les données de l'entreprise peut la tuer. Comprendre et appliquer une charte informatique n'est pas encore naturel.

R. E. | **En quoi les examens en ligne sont-ils intrusifs ?**

F. K. | Des étudiants nous ont signalé qu'il leur était demandé d'allumer leur caméra et de faire le tour de leur chambre pendant les examens et les tests de langue.

P. L. | Les certifications linguistiques imposent souvent des contraintes qui sont vécues comme des intrusions dans la vie privée.

R. E. | Ce problème mérite d'être creusé. Idéalement, les étudiants devraient être regroupés dans des lieux distants. Le test of english for international communication (TOEIC) fonctionne ainsi mais son organisation est compliquée pour un seul étudiant.

P. L. | Lors des examens à distance, l'école doit informer les étudiants des conditions de conservation des données vidéo pour instaurer un climat de confiance.

R. E. | J'ai milité pour que les salariés des écoles suivent les mêmes consignes de sécurité que les étudiants. Pour ma part, je n'ai jamais enregistré les examens en ligne de mes étudiants car c'est illégal.

L. J.-L. | L'obligation d'information sur le stockage des données, la qualité et la durée de stockage relève du délégué à la protection des données (DPO).

F. K. | Il n'est pas normal que l'étudiant doive faire la démarche de demander ses données personnelles à l'école alors qu'il en est propriétaire.
Je ne connais pas le *data protection officer* de mon école de management, alors que j'identifie tous les autres directeurs.

R. E. | C'est une question de culture. En général, il faut attendre un incident pour que les règles soient respectées.
Je crois qu'il existe deux masters et une certification Cisco de DPO.

L. J.-L. | Un DPO compétent, pouvant agir sur les questions que nous évoquons après analyse de l'existant, est une grande richesse pour les organisations.

« LA CYBERSÉCURITÉ DOIT FAIRE PARTIE DE TOUTES LES FORMATIONS, AU MÊME TITRE QUE L'INFORMATIQUE.

R. E. | Le RGPD reste à intégrer dans nos pratiques professionnelles et privées.
Les écoles françaises sont-elles plus réticentes qu'ailleurs à la dématérialisation des diplômes ?

L. J.-L. | A BCdiploma, nous observons que la France est plutôt bien placée en matière de dématérialisation. Les réticences dépendent de l'acculturation des collaborateurs clés aux nouveaux outils et à la *blockchain* et non de la localisation.

R. E. | Le bitcoin nous a rendu service.

L. J.-L. | Non, il nous dessert par son empreinte environnementale néfaste et son image de *trading*. Nous profitons plutôt des grands groupes qui poussent la *blockchain* pour assurer la traçabilité.

R. E. | **Que faire en cas de cyber attaque dans les hôpitaux et les cliniques ? Qu'en est-il des écoles ?**
La priorité est de tout couper pour préserver l'image d'une école informatique. En cas d'attaque plus complexe, une cellule de crise doit être montée pour travailler en mode dégradé. La plupart des hôpitaux peinent à répondre à une cyber attaque car leurs systèmes d'information sont anciens. Il reste donc un travail de fond à conduire.
Je propose un tour de table pour conclure.

P. L. | Je retiens la nécessité de sensibiliser les étudiants, les enseignants et les administratifs à la cybersécurité sans attendre

M. A. | J'ajoute la nécessité de rendre les risques compréhensibles par tous.

L. J.-L. | Créer de la valeur ajoutée pour l'utilisateur final en travaillant sur la cybersécurité me passionne.

J. N. | Les enjeux sont de se préparer à l'imprévisible. Dans leur dimension managériale, parvenir à penser le monde complexe de demain pose des questions d'organisation.

R. E. | Les personnes doivent être formées aux outils car le numérique, comme l'automobile, peut être une arme.

F. K. | Il conviendrait de travailler sur un label data et cyber garantissant la sécurité des données des étudiants des écoles de management et d'ingénieurs.

R. E. | Une certification en cybersécurité est une bonne idée.

Mise en pages : **Valérie Latchague Causse**
Crédits photos : © **Christian Jacquet**

CONFÉRENCE DES
GRANDES
ÉCOLES

Conférence des grandes écoles
11, rue Carrier-Belleuse ■ 75015 Paris
tél : 01 46 34 08 42
info@cge.asso.fr ■ www.cge.asso.fr
@ConferenceDesGE