FOCUS SUR L'ACN

Confiance numérique, cybersécurité, identité numérique, IA de confiance, souveraineté technologique et économique… L'ensemble de ces sujets mobilisent l'Alliance pour la Confiance Numérique. Dans le cadre de ces entretiens, les membres de cette organisation professionnelle nous livrent leur vision sur ces enjeux structurants pour la filière numérique française et européenne.

L'ACN : la voix de la filière de la confiance numérique française

Jean-Pierre Quémard

Édouard Jeanson

Jean-Pierre Quémard, président d'honneur, et Édouard Jeanson, VP, nous présentent l'ACN, ses missions et ses principales contributions.

Quelles sont les missions de l'ACN ?
Créée en 2011, l'Alliance pour la Confiance Numérique est l'organisation professionnelle qui aujourd'hui réunit les entreprises du secteur de la confiance numérique : la cybersécurité, l'identité numérique, et l'intelligence artificielle de confiance. Aujourd'hui, le monde de l'industrie de confiance regroupe 2 100 entreprises qui réalisent un chiffre d'affaires de 13,4 milliards d'euros. C'est un marché en forte croissance : plus de 8 % par an en moyenne. Aujourd'hui, l'ACN rassemble 90 entreprises, dont les leaders du secteur, mais aussi 85 % de start-ups, TPE PME et ETI.

Quelles sont vos missions et votre vocation ?
Nous défendons les intérêts de la filière en étant force de proposition auprès des pouvoirs publics (gouvernement, ANSSI, DGE, Parlement) aux niveaux français et européen afin notamment de les alerter sur des sujets qui nécessitent une réflexion, mais aussi pour proposer des évolutions sur de grands enjeux ou problématiques. Il y a quelques années, notre feuille de route ACN avait largement inspiré le Plan 33. Au niveau européen, nous avons poussé une position sur le European Cybersecurity Act ainsi que sur le projet européen d'identité numérique. En parallèle, nous contribuons au débat public en apportant des éclairages sur nos sujets stratégiques.

Quelles sont vos principales publications ?
Nous alimentons notre communauté de réflexions sur des sujets techniques, sur l'état de l'art… L'idée est aussi d'être visible et de faire connaître l'expertise française sur ces thématiques à une échelle internationale. Nos travaux sont, par ailleurs, en accès libre. Chaque année, nous publions l'Observatoire ACN de la confiance numérique que nous diffusons à l'occasion du Paris Cyber Week. C'est un document structurant, car il permet de diffuser des données économiques fiables et suivies sur notre filière, qui n'existent pas dans les statistiques officielles.
À cela s'ajoutent des prises de positions sur différents textes et règlementations. Ces documents détaillent tous les aspects de ces textes, nos positions, les grands enjeux, les points d'attention ou bien encore les mesures techniques que nous souhaitons voir mises à l'œuvre.
Nous proposons aussi des documents et des guides sur des sujets ciblés. Par exemple, pendant la pandémie, nous avons publié un document transverse sur la problématique de la sécurisation du télétravail. Nous avons souhaité apporter un éclairage sur ce sujet qui a concerné toutes les entreprises et qui a étendu la surface des cyberattaques, car tout le monde n'était pas forcément préparé pour ce basculement inopiné et brutal. Nous avons notamment mis l'accent sur les outils permettant de sécuriser le télétravail et d'apporter de la confiance numérique. Nous éditons aussi des documents ancrés dans l'actualité politique. Nous avons ainsi publié un document de propositions pour la présidence française de l'Union européenne qui recense les différents textes relatifs à la confiance numérique, l'autonomie stratégique et la souveraineté numérique européenne avec un focus sur nos positions et l'avis de notre filière, qui souligne la nécessité d'accélérer vers un marché numérique de confiance et qui met en avant les moyens et leviers législatifs qui peuvent être actionnés sous la présidence française de l'Union européenne pour y parvenir plus rapidement. ×

L'identité numérique : enjeux et perspectives

Alban Féraud

Alban Féraud, VP ACN, répond à nos questions sur l'identité numérique qui est un pilier du développement du numérique de confiance. Il revient notamment sur la montée en puissance du sujet et les enjeux qu'elle soulève.

Pourquoi entend-on de plus en plus parler de l'identité numérique ?

L'identité numérique est une brique essentielle à la souveraineté numérique et technologique. Elle est, en effet, une condition nécessaire à un contrôle souverain du monde numérique au niveau des États, mais aussi des utilisateurs qui ont besoin de pouvoir contrôler leurs données, leurs actions et protéger leur identité contre des fraudes. Plus récemment, la crise de la Covid avec le télétravail et l'accélération de la dématérialisation a renforcé ce besoin de pouvoir s'identifier à distance en toute confiance.

En France, l'État a beaucoup avancé sur ce sujet avec la mise en place d'un titre régalien doté d'une puce : la carte d'identité numérique. Chaque citoyen voit ainsi son identité légale se prolonger dans le monde numérique de manière dématérialisée. En Europe, de nombreuses initiatives ont aussi été prises en ce sens. Le règlement eIDAS a mis en place un premier cadre de reconnaissance et d'interopérabilité pour les identités numériques en Europe. En juin dernier, le texte a été mis en révision avec des ambitions très élevées. Il introduit notamment le concept assez novateur de portefeuille d'identités numériques. La Commission européenne souhaite ainsi donner un cadre et une définition légale à des éléments relevant des domaines techniques et technologiques. L'idée est d'ailleurs de généraliser le déploiement de ces portefeuilles dans tous les États membres : il est donc essentiel de s'assurer qu'ils répondent à un haut niveau d'exigence en termes de sécurité. Un autre sujet qu'on peut citer est celui de la vérification d'identité à distance. Pour le régulateur, il s'agit de poser les exigences techniques adéquates pour garantir le bon niveau de sécurité pour la vérification d'identité à distance.

Enfin, je dirai qu'il faut aussi démystifier le recours à la biométrie faciale qui est une technologie qui permet de vérifier la concordance entre un visage et une personne. Les craintes relatives à une utilisation abusive de cette technologie dans notre pays n'ont pas lieu d'être.

L'identité numérique est un enjeu majeur de la transition numérique et un axe stratégique en termes de cybersécurité. Pourquoi ?

La relation avec la cybersécurité est duale. L'identité numérique est un moyen au service de la cybersécurité. On ne peut pas garantir la sécurité dans le monde numérique si on n'est pas en capacité de contrôler l'identité des personnes qui y accèdent. Mais elle est aussi un enjeu de cybersécurité. L'identité numérique et ses infrastructures peuvent être la cible de cyberattaques. Elles se doivent donc d'être résilientes face à la menace. C'est un enjeu de taille, car l'identité numérique de confiance est une condition sine qua non pour un monde numérique sécurisé fonctionnel. Il est impératif de s'assurer que les systèmes sont protégés contre les cyberattaques et de garantir un haut niveau de confiance. La certification de sécurité de ces identités numériques est, d'ailleurs, une position portée par l'ACN. Se pose également la question des systèmes d'identité qui doivent être performants pour que l'identité numérique soit correctement reliée aux identités légales. Il faut garantir une continuité du droit dans le monde numérique pour que les personnes qui agissent sous leur identité numérique puissent être tracées et tenues responsables de leurs actes en cas de problème. À cela s'ajoute la protection des données pour éviter la constitution de bases de données qui pourraient être exploitées de manière malveillante.

Quels sont les enjeux relatifs au développement de l'identité numérique ?

Le premier point est celui de l'acceptation sociale. Il y a un travail de pédagogie et de sensibilisation qui doit être mené pour expliquer cette notion et faire comprendre que le sujet ne pose pas de risques et qu'il est sous contrôle. Cela implique de disposer d'un cadre juridique clair et adapté pour rassurer les citoyens et garantir que des moyens sont déployés pour protéger leurs données, garantir un contrôle sur les utilisations…

Un second point tourne autour de la notion de souveraineté numérique. L'enjeu est d'avoir une identité numérique de niveau de sécurité élevé, souveraine sous le contrôle des États membres. Il s'agit aussi de garantir ce même cadre pour l'exploitation des données rattachées à cette identité. Si cette démarche permet notamment d'éviter que les données européennes soient utilisées à des fins malveillantes, c'est aussi la garantie que les données professionnelles ne soient pas exploitées par des industriels étrangers et qu'elles servent bien l'industrie et les entreprises technologiques européennes. Et dans ce contexte d'accélération du développement de l'IA, c'est un véritable enjeu. L'identité numérique souveraine doit bénéficier aux entreprises et start-up européennes dans le cadre d'un contrôle démocratique européen.

Quelles pistes de réflexion pourriez-vous partager avec nos lecteurs dans ce cadre ?

L'ACN a produit une position sur ce règlement eIDAS 2 qui va être fondateur pour l'identité numérique en Europe. Nous saluons bien évidemment cette initiative et l'ambition de déployer des portefeuilles d'identité numérique utilisables partout en Europe. Pour autant, garantir un niveau de sécurité élevé de ces identités est crucial. En parallèle, pour que ce texte aboutisse, il est important d'associer l'industrie dans cette démarche pour développer des modèles d'affaires en conformité avec le cadre juridique et légal.

La cybersécurité : un enjeu incontournable

Édouard Jeanson

Alexis Caurette

François Esnol-Feugeas

Regards croisés de Édouard Jeanson VP, Alexis Caurette et François Esnol-Feugeas, membres du bureau ACN, sur la cybersécurité.

Depuis quelques années, la filière cybersécurité est de plus en plus dynamique. Qu'avez-vous pu observer au sein de l'ACN ?

La filière cybersécurité connaît une très forte dynamique économique et technologique avec une croissance annuelle moyenne de 8,1% entre 2015 à 2020. Face à l'évolution de la menace, la filière doit s'inscrire dans une démarche continue d'innovation et d'adaptation. Cette cybermenace est notamment liée à des enjeux géopolitiques. On assiste à un ciblage fréquent des opérateurs d'importance vitale et de services essentiels. Des pays comme la Chine, la Russie et les États-Unis sont assez explicites sur le développement de leur capacité cyberoffensive. Depuis peu, la France a également rendu publique sa doctrine dans ce domaine. À cela s'ajoutent des enjeux mafieux avec des cyberattaquants qui se professionnalisent et se structurent. Il y a en effet aujourd'hui, une véritable infrastructure mafieuse avec des acteurs qui sont spécialisés dans la mise à disposition d'outils d'attaque comme les malwares et les ransomwares ; la collecte et la vente d'information ; l'intrusion initiale dans les systèmes... En réponse, l'offre technologique se sophistique notamment avec le recours à l'IA (solutions EDR, XDR...) et permet un meilleur équipement des entreprises les plus vulnérables ou qui ne se sont pas encore dotées des bons outils. Personne n'est à l'abri. Les cibles sont de plus en plus diverses : établissements de santé, collectivités territoriales, fournisseurs de services numériques, grandes entreprises... Entre 2019 et 2020, l'ANSSI a recensé une augmentation de plus de 255 % de signalements d'attaque. Toutes les entreprises ne communiquent pas forcément quand elles sont victimes d'une cyber-attaque. On estime que 71 % des attaques ransomware réussies ne sont pas rendues publiques, ni par les entreprises ni par les tiers.

Justement, quel est le niveau de maturité des entreprises ? Quels sont les freins qui persistent ?

Il est très hétérogène. Parmi les acteurs très matures, on retrouve toutes les entreprises qui opèrent dans des secteurs critiques ou régulés : la défense, la banque... Les PME et les ETI ont un niveau de maturité beaucoup plus faible. Cela s'explique par une moindre compréhension des enjeux et une réelle difficulté à exprimer leurs besoins. Elles savent qu'elles sont exposées au risque cyber, mais le perçoivent comme un coût et un problème supplémentaire à gérer. Elles sont aussi face à une offre de solutions diverses et complexes. En effet, il faut une expertise avérée pour orchestrer l'ensemble des services et solutions qu'il faut déployer pour sécuriser un environnement. Dans ce cadre, la filière s'emploie à amener une réponse cohérente et compréhensible adaptée aux PME et ETI. À cela s'ajoute la nécessité de mener un travail de fond pour mettre à leur disposition des solutions unifiées, interopérables et faciles à utiliser et à déployer pour couvrir leur besoin dans son ensemble.

Et quels sont les enjeux pour les acteurs de la filière ?

Nous avons en France et en Europe une très forte capacité d'innovation en matière de cybersécurité. Nos experts sont recherchés dans le monde entier et notre expertise est reconnue mondialement. Pourtant, nous avons du mal à accompagner le développement de nos entreprises, à les aider à grandir pour en faire des licornes et à les garder dans notre giron. Le financement de la filière cybersécurité est ainsi un véritable problème de fond. S'il y a de belles levées de fonds, le scaling-up n'est pas encore au niveau attendu et les moyens déployés en ce sens restent relativement faibles. Se pose également la question de la souveraineté des solutions, des technologies ainsi que la souveraineté économique. En effet, protéger ses entreprises et ses industries est avant tout une question de souveraineté !

Au-delà des défis et enjeux techniques, il y a également un enjeu humain et de compétences. Qu'en est-il ?

C'est un sujet qui nous tient particulièrement à cœur. Nous avons travaillé avec l'ANSSI sur les premières cartographies des métiers de la cyber, mais aussi sur le label de formation SecNumEdu. Nous avons noué un partenariat

avec l'École 2600 de cybersécurité qui s'adresse à des personnes qui ont déjà une première expérience professionnelle et qui souhaitent se reconvertir dans ce domaine. Nous avons participé au lancement des bachelors de l'EPITA, de l'ESIEA... Nous encourageons la féminisation de ce domaine en collaborant avec des associations comme Women4Cyber qui font découvrir ces métiers aux lycéennes et collégiennes. Nous sommes mobilisés sur le sujet de la formation pour le CSF (comité stratégique de filière) industries de sécurité. En tant que membre fondateur du Campus Cyber, nous contribuons au volet dédié à la formation. Aujourd'hui, tous les acteurs sont conscients qu'il y a urgence à former, reconvertir et faire monter en compétences des hommes et des femmes pour faire face à ce risque cyber.

L'intelligence artificielle (IA) de confiance : le défi des prochaines années

Jean-Luc Gibernon, Vincent Bouatou et Nicolas Bouvattier reviennent sur le sujet de l'IA de confiance et son importance pour le développement de la confiance numérique.

Jean-Luc Gibernon

Vincent Bouatou

Nicolas Bouvattier

Nous entendons de plus en plus parler d'IA de confiance. De quoi s'agit-il ?

L'IA est un ensemble de technologies qui vise à simuler des processus de l'intelligence humaine par des machines et des systèmes informatiques. La notion de confiance dans l'IA est liée à la grande complexité de ce domaine et la nécessité de s'assurer de sa fiabilité. À partir de là, le sujet de la confiance dans l'IA pose quatre enjeux : l'explicabilité, la prévention des biais, la résistance aux agressions et l'éthique dans le numérique. Au-delà comme pour toute technologique critique se pose aussi la question de la souveraineté puisque son développement nécessite des investissements massifs. Nous sommes, en effet, face à une course à l'IA entre les États-Unis et Chine, alors que l'Europe doit pouvoir se positionner comme un fournisseur de technologies et une puissance autonome.

En matière de cybersécurité, quelles sont les perspectives qu'elle offre ?

L'IA peut apporter beaucoup à la cybersécurité. Le principal apport est celui de la détection des attaques. Elle a la capacité d'adresser des choses plus finement et à détecter un comportement anormal que l'œil humain ne pourrait pas ou difficilement identifier. L'idée n'est pas que l'IA remplace l'humain, mais apporte plutôt un soutien aux opérateurs en charge de ce volet. La prochaine étape serait, dans cette continuité, de capitaliser sur l'IA non seulement pour détecter les attaques, mais également comprendre ce que font les cyberattaquants, décortiquer les attaques afin de les catégoriser et réagir automatiquement en fonction de l'attaque.

Quelles sont également les problématiques qu'elle soulève ?

Elles dépassent largement le cadre de la cybersécurité. Il y a d'abord la capacité à mettre à disposition des capacités de calcul très importantes pour l'apprentissage et des données pour le développement des algorithmes d'IA. Au-delà, la présence de biais dans des jeux d'apprentissage peut impacter la capacité du système à prendre des décisions.
Les principaux débats sur l'IA concernent aussi l'éthique. C'est d'ailleurs un sujet qui mobilise le Parlement européen. On commence à voir des prises de position de certains États membres visant à cadrer le recours à l'IA. L'objectif est de réaffirmer les valeurs fondamentales de l'Union européenne, de désigner les pratiques inacceptables telles que le social scoring ou la surveillance de masse, tout en veillant à bien distinguer les autres usages de l'IA et les risques qui leur sont associés. Une réflexion de fond doit être menée pour ne pas entraver l'innovation et le développement des acteurs européens dans ce domaine et afin de permettre à l'Europe de disposer de cet outil technologique indispensable à la maîtrise de notre avenir numérique.

Comment abordez-vous ce sujet au sein de l'ACN ?

Dans ce cadre, le rôle d'une organisation comme l'ACN est d'éclairer le débat pour imposer la notion de confiance, aider à définir les critères qui la caractérisent et à distinguer les différents usages de l'IA. Il s'agit aussi d'attirer l'attention des législateurs, des pouvoirs publics et autres décideurs sur des mesures trop larges qui pourraient entraver l'innovation, diminuer la compétitivité de l'Europe et, in fine, s'avérer contre-productives au regard de l'objectif de protection de nos valeurs fondamentales.