

[Parole d'expert]



INTERVIEW de Guillaume Poupard

directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)



Q1 – Pouvez-vous nous rappeler quel est le rôle de l'ANSSI dans un écosystème numérique en évolution tant en France qu'en Europe ?

« L'ANSSI a été créée il y a 10 ans, à un moment où l'on a pris conscience que les questions de sécurité numérique allaient devenir un enjeu majeur.

Le choix français de créer une autorité unique en charge de la question de la sécurité numérique pour le compte de l'Etat est original et différent des autres pays en termes d'organisation. Ce choix repose sur deux principes très forts :

Premièrement, la séparation de l'offensif et du défensif, qui est un choix structurant, courageux et efficace. Ainsi, l'ANSSI ne s'occupe que de défensif et intègre l'ensemble de ces questions. Nous sommes sur de la prévention, de la sensibilisation, de la détection des attaques avec un côté opérationnel très fort, et sur de la réponse à incident et de l'aide aux victimes. Nous ne sommes pas une agence de renseignement ou d'enquête, nous ne menons pas d'attaque ni de contre-attaque.

Deuxièmement, l'agence est rattachée aux services du Premier ministre, ce qui est un symbole fort et confirme la conviction selon laquelle le sujet « Cyber » ne doit pas être restreint à un domaine particulier. Ainsi, nous ne sommes pas typés « Défense », « Intérieur » ou « Economie ». Cette position interministérielle nous permet de faire des choses en propre et de travailler avec les autres, chacun dans son domaine de compétence.

L'ADN de l'ANSSI, c'est un cœur défensif incluant aussi bien de la technique que de l'opérationnel, qui s'inscrit dans un écosystème, avec pour objectif d'aller aussi vite que les attaquants. Cela met la barre assez haut !

Si je devais décrire cet écosystème, je dirais qu'il se structure en 3 grands pôles :

- Un pôle étatique ambitieux - les différents exécutifs ont toujours réaffirmé l'importance de la sécurité numérique.
- Un pôle constitué par tous ceux qui doivent se protéger, anticiper, réagir. On a fait le choix en France d'une approche par la réglementation. Pour l'ingénieur que je suis, et sans aller sur un terrain politique, il me semble que faire ce choix permet de gagner du temps, de partager une ambition commune, de créer du lien entre les acteurs et de forcer une coopération. Ceci pour éviter d'attendre les catastrophes pour se parler. C'est ce que l'on a fait dès 2013, avec ce qu'on appelle les « opérateurs d'importance vitale » (OIV)¹. Bien évidemment, les solutions à apporter ne sont pas les mêmes en fonction des acteurs. En ce qui concerne les plus « petits » (PME, collectivités locales), nous travaillons beaucoup avec eux pour les sensibiliser et les aider à anticiper et mieux prendre en compte ces sujets.

¹ Organisations privées ou publiques, qui exploitent ou utilisent des installations jugées indispensables pour la survie de la Nation.



- Le troisième pôle est constitué des offreurs de services, produits et solutions en matière de sécurité numérique. Nous nous devons d'avoir une industrie nationale innovante en la matière et l'ANSSI contribue à structurer ce pôle notamment par le biais des Visas de sécurité (certifications et qualifications).

Cet écosystème est efficace si ces trois pôles - Etat, certains opérateurs sensibles, et acteurs privés capables d'apporter des solutions - fonctionnent de manière équilibrée. Cela répond à une question de souveraineté nationale pour la France et d'autonomie stratégique au niveau européen.

Tout cela est très ambitieux évidemment, mais je suis convaincu que c'est tout un écosystème qui doit bouger ensemble sinon cela ne fonctionne pas. »

Q2 – Au-delà des aspects réglementaires, quels sont les forums qui existent pour échanger sur ces questions ?

« Les forums sont multiples. La réglementation notamment fait émerger des communautés. C'est ce qui est en train de se produire avec les opérateurs de services essentiels (OSE)², qui sont des acteurs importants pour la société et l'économie. On voit se créer un ensemble assez homogène sur un sujet où la plupart des acteurs comprennent qu'ils ne sont pas en position de concurrence. Le partage est compliqué mais il a un intérêt et l'ANSSI cherche à l'encourager en veillant bien à ce qu'il ne devienne pas une forme de faiblesse.

De la même façon, au niveau national, nous animons la communauté des centres opérationnels qu'ils soient publics ou privés. En effet, c'est le métier et l'intérêt de partager sur les sujets data qui réunit les gens. La frontière entre sphères publique et privée est peu marquée dans le domaine de la sécurité numérique.

A l'échelle européenne, nous avons mis en place un réseau entre les Etats, dont les échanges vont au-delà des espérances, preuve que cela répond probablement à un vrai besoin. Notamment, un groupe informel s'est constitué dans le cadre de l'élaboration de la directive network and information security (NIS) concernant des mesures destinées à assurer un niveau de sécurité élevé dans l'Union³. Il vise à échanger sur la base du volontariat sur la façon dont les questions de sécurité nationale sont prises en compte dans l'ensemble des Etats membres. Ainsi, des pays qui ont commencé un peu plus tôt comme la France, peuvent partager leur expérience avec les autres. Ce n'est pas de la philanthropie, c'est bien un intérêt partagé. Rester focalisés sur le périmètre national ne sera en effet pas suffisant s'il existe des zones de non droit en matière de sécurité numérique et c'est donc bien le niveau de sécurité de toute l'Europe qu'il faut développer.

A l'échelle mondiale, une coopération se met en place, plus facilement avec certains pays qu'avec d'autres bien sûr. Nous croyons beaucoup à l'Appel de Paris, porté par le Président de la République le 12 novembre 2018 pour la confiance et la sécurité dans le Cyberspace. Ce n'est pas idéaliste, c'est même plutôt intéressé : il s'agit de reconnaître que si les tensions continuent à monter entre les grands blocs, à un moment, les dommages vont devenir

² <https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/faq-operateurs-de-services-essentiels-ose/>

³ « Network and Information Security », ou « NIS », 2016/1148 du 6 juillet 2016, directive sur la sécurité des réseaux et des systèmes d'information, <https://www.ssi.gouv.fr/actualite/option-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/>



inacceptables. Et il faudra bien se poser des questions sur la façon dont on veut que le cyberspace fonctionne. »

Q3 – Comment se fixe-t-on des règles pour faire en sorte que cet espace numérique, ce bien commun, ne soit pas uniquement un champ de bataille ?

« J’ai l’habitude de décrire cet espace numérique comme étant très multi-échelle, or les échelles ne s’opposent pas les unes aux autres, elles se complètent. Ainsi, il existe un échelon national, qui est très fort, un échelon européen qui fonctionne, est indispensable et en phase de développement. Et puis un échelon international qui est majeur parce qu’autrement c’est l’aspect conflictuel qui prendra le dessus... »

Q4 – La vision du Cercle de la Donnée est que la data est au cœur de l’économie aujourd’hui et le sera encore plus demain. Quel rôle peut jouer l’ANSSI dans ce contexte-là ?

« En ce qui concerne la donnée « cyber », strictement liée à la sécurité nationale, très technique et spécifique, relative à la connaissance des attaques, il s’agit de la partager avec le plus de personnes possible, en évitant que les attaquants en fassent partie. Vous comprenez bien que cette donnée ne peut pas être totalement « open », et cela complique la donne. Mais on a absolument besoin de partager cette donnée avec tous ceux à qui elle peut bénéficier, et ils sont nombreux, pour éviter des attaques lourdes, complexes et dommageables pour les victimes.

Concernant la donnée en général, c’est une toute autre question. La donnée est devenue une sorte de matière première, convoitée, que certains n’hésitent pas à voler (je pense notamment aux vols de données de santé à Singapour ou en Norvège, sûrement destinées à alimenter une intelligence artificielle). Il faut avoir conscience que nous vivons dans un monde partiellement hostile. Cependant, face à ce risque, réagir en se renfermant, en gardant les données pour soi, en refusant de les partager, n’est pas la bonne solution. Les données de santé sont un exemple intéressant car elles sont sensibles mais peuvent également permettre des innovations, par exemple contre le cancer.

L’enjeu est de trouver un juste équilibre, qui protège la donnée tout en permettant son utilisation. »

Q5 – Croyez-vous en la professionnalisation du numérique, à l’instar de ce qui existe dans le secteur de la santé justement, avec un accès permissionné et une réglementation stricte qui permettent d’exploiter la donnée sans anonymisation avec un niveau de sécurité acceptable, et, à la clé, des bénéfices réels ?

« A mon sens, l’anonymisation ne fonctionne pas. On peut y avoir recours de manière micro, sur des données avec peu de champs mais pas sur des traitements complexes ou des croisements de données.



La vraie question est la suivante : comment casser l'idée communément admise et faussement intuitive que la donnée doit être amenée et transmise à ceux qui en ont besoin ? Pourquoi les Intelligences artificielles ne se déplaceraient-elles pas ? Pourquoi ne fonctionnerait-on pas avec des accès permissionnés ? Après tout, quand nous apprenons nous-même, nous nous déplaçons.

Depuis des années, on s'escrime à vouloir désensibiliser des données, qui, au final, ne valent plus grand-chose pour les transmettre. Pourquoi ne pas imaginer des sentinelles des données, gardiens du temple, qui décideraient d'ouvrir ou non la porte aux intelligences artificielles qui en demanderaient l'accès ? On pourra ainsi mieux contrôler qui vient et qui ne vient pas. Et ne donner que le résultat du « machine learning » et non pas la source. »

Q6 – Devant l'accroissement de la menace dans le secteur du Numérique, l'ANSSI a-t-elle les moyens de couvrir ce périmètre et comment voyez-vous l'avenir pour faire face à ces grands enjeux ?

« Il ne faut jamais demander à un directeur s'il a assez de moyens (*rires*).

Bien sûr, nous avons besoin de moyens en propres mais la solution est de partager le sujet avec ceux qui sont et seront acteurs, les aider à décrypter, les accompagner. Il faut travailler ensemble, expert et acteurs, publics et privés.

L'important est de normaliser le risque cyber, de faire en sorte qu'il soit traité comme les autres risques. L'échec complet serait de voir que la sécurité numérique en France se résume seulement l'ANSSI, car en réalité, c'est bien l'affaire de tous. »

Q7 – Comment le Cercle de la Donnée peut-il contribuer aux missions de l'ANSSI ?

« Comme je vous le disais, nous ne sommes pas une « Cyber Agency » et à ce titre, nous ne sommes pas là pour protéger le contenu (la donnée en elle-même), mais bien pour protéger le contenant (les systèmes d'information).

Aussi, l'approche du Cercle de la Donnée, qui s'intéresse au contenu, vu par le prisme des aspects métier, de façon pluridisciplinaire me semble tout à fait complémentaire de ce que nous faisons à l'ANSSI. »





PRESENTATION Guillaume POUPARD - ANSSI



Guillaume Poupard est ancien élève de l'École polytechnique, promotion X92. Ingénieur de l'armement en option recherche, il est titulaire d'une thèse de doctorat en cryptographie réalisée sous la direction de Jacques Stern à l'École normale supérieure de Paris. Il est également diplômé de l'enseignement supérieur en psychologie.

Il débute sa carrière comme expert puis chef du laboratoire de cryptographie de la Direction centrale de la sécurité des systèmes d'information (DCSSI). Il rejoint en 2006 le ministère de la défense, toujours dans le domaine de la cryptographie gouvernementale puis de la cyberdéfense.

En novembre 2010, il devient responsable du pôle « sécurité des systèmes d'information » au sein de la direction technique de la Direction générale de l'armement (DGA). Le 27 mars 2014, il est nommé directeur général de l'Agence nationale de sécurité des systèmes d'information.

PRESENTATION Cercle de la Donnée



Le Cercle de la Donnée est un think tank indépendant réunissant des spécialistes de la donnée, soucieux d'excellence et d'éthique et s'intéressant aux usages de la donnée, au-delà de la seule dimension technologique.

Le Cercle de la Donnée veut faire émerger et transmettre les bonnes pratiques, approfondir les multiples expertises, briser les classiques cloisonnements professionnels et ainsi contribuer à la structuration d'une filière de la donnée, basée sur l'excellence, l'éthique et l'interdisciplinarité.

Il est soutenu par des partenaires qui partagent les valeurs du Cercle, dont fait partie MarkLogic, éditeur de logiciel.

En Savoir + : <https://www.linkedin.com/company/cercledonnee/>

Pour agrandir le Cercle et/ou participer à ses travaux : contact@lecerclede ladonnee.org