« LA CYBERSÉCURITÉ est un écosystème en pleine expansion »

Explosion de la menace et des risques cyber, enjeux de souveraineté nationale et européenne, renforcement et développement des capacités, création d'un écosystème français et européen, besoins en compétences et en talents… *Mathieu Feuillet (2004), Sous-directeur Opérations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'information)*, dresse pour nous un état des lieux du monde de la cybersécurité et revient sur l'ensemble des sujets liés à la cybersécurité aujourd'hui.

Mathieu Feuillet (2004)

Quels sont le rôle et les missions de l'ANSSI ?
L'ANSSI est l'autorité nationale en matière de cybersécurité et de cyberdéfense. Nous accompagnons et sécurisons le développement numérique en France pour que les citoyens et les entreprises puissent avoir confiance dans le numérique.
Nous avons un positionnement particulier au sein de l'État. Nous faisons partie des services du Premier ministre au sein du Secrétariat général de la sécurité et de la défense nationale. Notre rôle et nos missions sont exclusivement défensifs. Nous nous adressons à l'ensemble du tissu national afin de garantir la cybersécurité de tous et de trouver les solutions les plus adéquates pour les particuliers, les entreprises et les administrations. Nous accompagnons principalement deux types de bénéficiaires : les administrations et les opérateurs régulés (opérateurs d'importance vitale et les opérateurs de services essentiels), dont le statut est défini par la loi.
Avec ses 575 agents, l'ANSSI assure au quotidien une mission de :

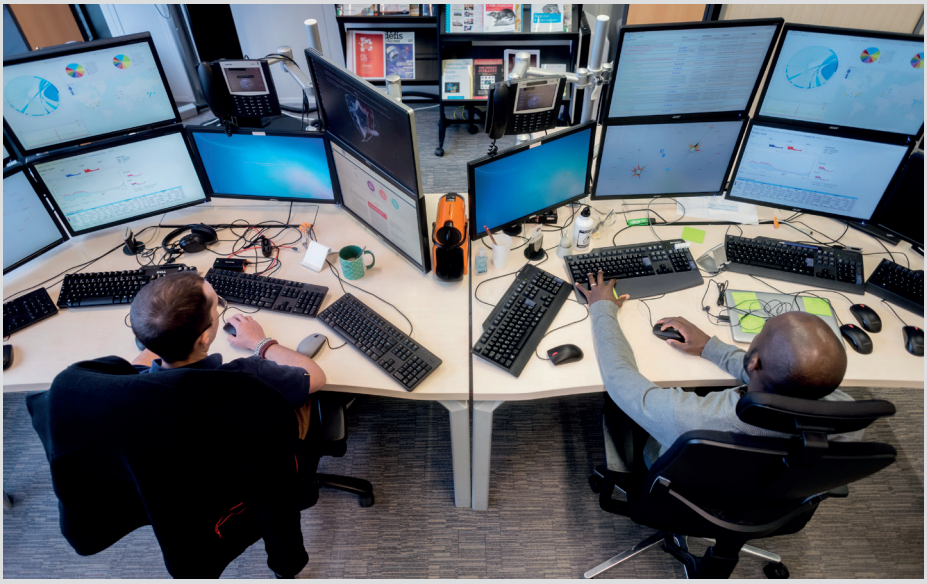
- Prévention : entraver les attaques informatiques en aidant les entreprises et administration à augmenter leur niveau de sécurité. Cela passe par différentes actions concrètes comme le conseil pour optimiser et augmenter le niveau de sécurité des systèmes d'informations. L'enjeu est de faire en sorte que, dans l'écosystème national, nous disposions de bons produits et services pour garantir la sécurité. Pour ce faire, nous menons un travail de qualification et de certification des produits et de prestataires qui reçoivent de la part de l'ANSSI un label, appelé visa, pour attester de leur bon niveau de sécurité ;
- Stratégie et négociation internationale : l'ANSSI développe une doctrine et assure le suivi de stratégie de cyberdéfense dans les composantes industrielles et économiques les plus stratégiques pour l'État. L'ANSSI est aussi en charge d'élaborer les positions et souvent conduire, pour la France, les négociations internationales en matière de cybersécurité. Elle est ainsi en première ligne au sein des instances européennes et des relations bi et multi-latérales.
- Information et de sensibilisation : l'ANSSI communique beaucoup en menant un important travail de pédagogie pour diffuser et promouvoir les bonnes pratiques. Ces actions visent le grand public, mais aussi des hauts cadres d'entreprises ou d'administrations afin qu'ils incluent le risque numérique dans leurs schémas de décision. Tous les ans, en octobre, pendant le Cybermois, en France et en Europe, nous menons diverses opérations. Sur le site de l'ANSSI, de nombreuses ressources sont consultables et téléchargeables (affiches, guides de bonnes pratiques…). Les visiteurs du site peuvent aussi compléter un MOOC pour tester et développer leurs connaissances sur ce sujet ;
- Intervention en cas d'incident : je suis, par ailleurs, en charge de ce volet au sein de l'ANSSI. Dans ce cadre, nos enjeux sont de mieux comprendre la menace qui cherche à porter atteinte aux intérêts français ; détecter les attaques, notamment celles visant l'État ; intervenir en cas d'incident pour y mettre fin, remettre le système d'information en état acceptable pour maintenir l'activité. Sur ce dernier point, nous pouvons fournir un soutien à distance, diriger vers des prestataires adaptés ou intervenir sur place avec le détachement d'une équipe dédiée si la situation est grave.

Au cours des dernières décennies, la cybersécurité est devenue un sujet central et stratégique. Quelles sont selon vous les évolutions qui ont marqué ce secteur ?
Aujourd'hui, le numérique est omniprésent. Il n'y a plus ou très peu d'organismes capables de fonctionner sans informatique. En parallèle, la donnée est de plus en plus importante. Au cœur du modèle économique des géants de l'information, les GAFAM, qui génèrent des chiffres d'affaires impressionnants, elle est devenue au cours des dernières décennies un bien précieux

très convoité. De plus en plus, elle représente un enjeu en matière de sécurité nationale. Les risques de déstabilisation augmentent et une criminalité spécifique se développe.

Dans le cyberespace, les règles du jeu sont différentes du monde réel. Contrairement aux conflits et à la criminalité traditionnels, nous sommes face à une quasi-instantanéité des actions menées. Une opération malveillante peut être menée de bout en bout en quelques secondes. À cela s'ajoute un affaiblissement des frontières et des espaces juridiques. En effet, il n'y a pas de frontières que l'on pourrait contrôler sur des réseaux comme Internet. Tout comme il est complexe de déterminer de quelle juridiction relève un incident. En outre, nous nous retrouvons très souvent face à l'anonymisation des actions. Il est très difficile de remonter jusqu'à l'auteur de faits malveillants et de mener les actions juridiques et diplomatiques nécessaires en fonction de l'attaquant. Enfin, c'est un combat asymétrique. Le défenseur d'un système d'information doit tout sécuriser de manière simultanée, alors qu'il suffit à l'adversaire de trouver un seul chemin d'attaque. Les opportunités d'attaques sont multiples et donc très attractives. Historiquement, l'espionnage stratégique et économique entre États ou entreprises représente le principal type d'incident. Avant le numérique, il s'agissait de corrompre un individu pour arriver à obtenir des informations, une action risquée avec un fort risque d'exposition. Avec le numérique, c'est-à-dire l'anonymisation des actions et la difficulté de remonter aux auteurs des faits, cela devient beaucoup plus attirant et le risque est plus faible. Ainsi, il y a de plus en plus d'opérations d'espionnage très sophistiquées et furtives que nous détectons malheureusement tardivement. Plus récemment, nous avons vu apparaître des attaques sur la chaîne d'approvisionnement. Les attaquants s'en prennent aux sous-traitants, aux fournisseurs de produits informatiques… pour atteindre leur cible finale. Tout le monde se souvient encore de l'attaque spectaculaire menée contre l'entreprise américaine SolarWinds révélée en décembre 2020. Les attaquants ont piégé un produit de l'entreprise qui leur aurait potentiellement permis de toucher plus 18 000 entités dans le monde qui avaient installé la version piégée du produit. Finalement, une cinquantaine d'entités aux États-Unis ont été attaquées. Ce genre d'incident a un effet démultiplicateur très impressionnant.

On assiste également au ciblage d'infrastructures critiques d'un pays à des fins de sabotage. En 2020 et 2021, Israël et l'Iran s'étaient mutuellement accusés de mener ce genre d'attaques contre des



usines de production d'eau potable avec des tentatives de modifier le taux de chlore afin de rendre l'eau impropre à la consommation. Certains états vont encore plus loin en menant des campagnes de prépositionnement qui s'étendent sur des mois, voire des années. L'idée est de se prépositionner dans des pays cibles pour être en capacité, si les enjeux politiques et géopolitiques le justifient, de mener des actions pouvant porter atteinte aux infrastructures critiques.

Au cours des dernières années, nous avons aussi assisté à l'explosion des campagnes d'influence et de déstabilisation. Ces incidents, à la frontière entre la cybersécurité et la manipulation d'informations (les fake news), visent à extraire des informations, les manipuler et les rediffuser pour déstabiliser une organisation, comme cela avait été le cas, en 2016, lors des élections américaines, avec le piratage des infrastructures du Parti démocrate.

Et bien évidemment, la cybercriminalité augmente toujours. Depuis quatre ans, il y a une recrudescence des attaques par rançongiciel. On peut notamment citer l'attaque, début 2021, contre l'entreprise Colonial Pipeline avec la mise à l'arrêt d'un oléoduc qui alimente la côte est des États-Unis. D'ailleurs, entre 2019 et 2020, à l'ANSSI, nous avons traité quatre fois plus d'attaques de ce type. États, administrations, collectivités, grands groupes, industries, PME sont tous exposés aux risques cyber et peuvent être la cible des cyberattaquants. Il est plus que jamais essentiel, voire vital, de prendre les mesures nécessaires pour se protéger au moins contre les menaces basiques. Pour cela, ils peuvent s'appuyer sur les ressources produites par l'ANSSI en commençant par notre *Guide d'hygiène informatique* qui liste les 42 mesures essentielles pour garantir la sécurité du système d'information et les moyens de les mettre en œuvre, outils pratiques à l'appui.

D'ailleurs, le Plan de Relance prévoit un volet cybersécurité. Que faut-il en retenir ? Et à quel niveau allez-vous intervenir ?

Le plan de relance, dont l'objectif est de redresser durablement l'économie, prévoit un volet cybersécurité que nous pilotons et qui dispose d'un budget de 136 millions d'euros pour la période 2021 et 2022. L'objectif est de renforcer la sécurité des administrations, des collectivités territoriales et des organismes qui ont un rôle de service public en dynamisant l'écosystème industriel de la cybersécurité. Dans ce cadre, nous subventionnons un grand nombre d'acteurs publics pour une sécurisation globale de leurs systèmes et l'acquisition de prestations, produits, sensibilisation et formation. Ainsi, plus de 600 entités (dont 70 % de collectivités territoriales, 20 % d'établissements de santé et 10 % d'établissements publics) vont bénéficier de ces aides pour former leurs agents, mais aussi pour déployer des solutions de sécurité.

ACTIVITÉ OPÉRATIONNELLE DE L'ANSSI EN 2020

- *2 287 signalements*
- *759 incidents*
- *7 incidents majeurs*
- *20 opérations de cyberdéfense*

En parallèle, nous développons les capacités cyber de l'État, mais également les nôtres, notamment en termes de détection des menaces pour agir le plus rapidement en cas d'incident. Pour accompagner en région, les PME, les ETI et les collectivités territoriales, nous avons récemment annoncé la signature avec sept régions d'une convention pour la création de centres régionaux de réponse aux incidents cyber (CSIRT : Computer Security Incident Response Team). Ces centres doivent soutenir le tissu économique et social de chaque territoire face aux cybermenaces, pour répondre de manière pertinente et efficace aux besoins identifiés.

Pour déployer en France et en Europe une stratégie de cybersécurité, quels sont les principaux enjeux selon vous ?

En février 2020, le Président de la République a présenté la stratégie de cybersécurité du pays. Au niveau européen, de nombreuses initiatives sont menées. Il y a plusieurs directives importantes et structurantes, comme la directive Network and Information System Security (NIS), dont la version 2 est en cours de négociation et qui vise à augmenter le niveau de sécurité du tissu économique européen de manière générale.

Par ailleurs, l'Europe s'est dotée de moyens de réponse si une agression extérieure survient, avec notamment la boîte à outils cyberdiplomatique, utilisable en cas d'atteinte aux intérêts européens, que soit touché un État ou une institution européenne. En parallèle, il s'agit aussi de réduire notre dépendance vis-à-vis du reste du monde et de mettre en place les moyens et les actions qui nous permettront de former les compétences et les talents dans ce domaine où il y a une très forte pénurie et compétition à une échelle mondiale.

Dans ce contexte, votre organisation et maillage national sur ce sujet ont vocation à évoluer. Qu'en est-il ?

En effet ! Et cette démarche va se traduire au travers de deux projets essentiellement. Le premier est le Campus Cyber dont l'activité démarre cette année. Au sein de cette entité, nous allons installer une équipe afin d'être au contact des autres acteurs de l'écosystème national du cyber et être une des parties prenantes de ce campus. Et le second est la création d'une antenne de l'ANSSI à Rennes qui va accueillir près de 200 personnes à terme. Si le bâtiment dans lequel nous nous installerons est encore en cours de construction, nous avons déjà plusieurs personnes sur place qui préparent l'ouverture de cette antenne, prévue pour début 2023. Les centres régionaux de réponse à incident cyber, que j'ai mentionnés précédemment, sont destinés à toutes les entités du territoire touchées par la menace cyber. Nous accompagnons également des initiatives au niveau de certains secteurs d'activités : avec des autorités de régulation sectorielle, des associations, des industries, nous travaillons ensemble ainsi sur la création de capacité de traitement d'incident dans un secteur donné. Nous incitons aussi les grandes entreprises à se doter et à développer leur propre capacité d'intervention en interne.

L'ensemble de ces actions, qui visent à développer un maillage et un écosystème de la cybersécurité, a pour objectif de pouvoir réagir au plus vite et au mieux en cas d'incident et de limiter les dégâts ainsi qu'une éventuelle propagation de la menace.

Pour relever le défi de la cybersécurité, les compétences et expertises sont clés. Quelles sont celles que vous recherchez et qui vous intéressent plus particulièrement ?

La cybersécurité n'est pas uniquement un problème technique. C'est un enjeu stratégique, économique, politique… Pour y faire face, nous avons besoin de techniciens et d'ingénieurs, notamment en sécurité des systèmes d'information des logiciels ou des composants, en cryptologie, en data science et en machine learning… Mais nous avons aussi besoin d'experts en politique, en géopolitique, ainsi que des personnes capables de comprendre les conflictualités et les risques à l'international. Et pour sensibiliser la diversité des publics, nous recherchons des personnes qui maîtrisent les outils de la communication, du marketing.

Plus que jamais, nous avons besoin de femmes et d'hommes venant de tous les horizons.

Et au fil de la structuration de cet écosystème, nous avons besoin de pouvoir nous appuyer sur des cadres et des managers pour accompagner la montée en compétence de l'ensemble de ces talents. Des profils, comme les diplômés de Polytechnique notamment, pourront s'épanouir dans l'univers de la cybersécurité et plus particulièrement au sein de l'ANSSI, une entité transverse à la croisée de sujets techniques, économiques, humaines et politiques passionnants…

Et c'est l'ensemble de ces dimensions qui font la richesse du service public, ainsi que son attrait en aidant concrètement des victimes à éviter ou à se remettre d'une cyberattaque.

Quelles pistes de réflexion pourriez-vous partagez avec nos lecteurs ?

La cybersécurité est un écosystème en constante expansion qui est encore en pleine structuration aussi bien à l'échelle française et européenne que mondiale. Il y a encore beaucoup à faire en matière de régulation, de souveraineté numérique, de développement des capacités techniques et technologiques, de préservation des intérêts français et européens.

L'ère qui s'ouvre est porteuse d'une conflictualité encore grandissante : nous devons poursuivre et redoubler notre effort collectif de structuration pour y faire face et l'ANSSI est l'acteur majeur si ce n'est principal de cette dynamique. Il est certain que les talents qui vont opter pour une carrière dans ce secteur ne s'ennuieront pas dans les prochaines décennies !

FORMATION

Le constat est partagé depuis plusieurs années par l'ensemble de l'écosystème : il y a un cruel manque de candidats. La sécurité du numérique est pourtant une filière d'avenir ! La formation et l'attractivité des métiers de la cybersécurité est un enjeu essentiel pour les prochaines années.

En 2017, l'ANSSI a lancé un premier projet : la labellisation des formations initiales en cybersécurité de l'enseignement supérieur. L'objectif est d'aider les jeunes à choisir parmi les formations actuelles, avec les labels SecNumedu & Cyberedu. En 2020, on compte plus de 60 formations initiales labellisées SecNumedu, réparties sur tout le territoire. L'ANSSI a ensuite lancé SecNumedu Formation Continue, label pour les formations continues courtes. En 2020, on compte plus de 70 formations labellisées SecNumedu FC .

La formation est un processus continu : les actions de sensibilisation et de formation à la sécurité du numérique pour les décideurs, les agents publics, les acteurs économiques et les citoyens doivent se poursuivre.