ma-
ni-
feste

Pour l'ANSSI des dix prochaines années

pour l'écosystème de la cybersécurité

En 2019, l'ANSSI a célébré dix années d'existence en s'entourant de celles et ceux qui font la cybersécurité en France.

Pour elle et pour cet écosystème, l'agence tout entière a profité de cette année symbolique pour entreprendre des travaux stratégiques et collaboratifs : ***ANSSI10+****.*

Directement issu de cette réflexion, le manifeste que vous tenez entre les mains est là pour rappeler d'où nous venons, ce que nous sommes et, surtout, où nous souhaitons aller, collectivement.

C'est presque devenu un poncif que d'évoquer l'impact des technologies numériques sur nos sociétés et nos économies, tant ces transformations sont désormais omniprésentes dans le fonctionnement de l'État, l'activité des entreprises et la vie quotidienne de nos concitoyens.

L'innovation est aujourd'hui sur toutes les lèvres ; le « cycle du *hype* » n'en finit pas de raccourcir et il est possible de lever plusieurs millions d'euros sur un simple *buzzword*. Ces phénomènes ne doivent cependant pas masquer certaines ruptures profondes. Pour ne citer que les progrès de l'apprentissage automatique et de l'intelligence artificielle, l'explosion de la virtualisation et les perspectives offertes par les réseaux 5G, tout porte à croire que nous sommes à l'aube de nouvelles révolutions.

Qu'elles soient en cours ou à venir, ces transformations sont avant tout synonymes de formidables opportunités. Mais fatalement — c'est bien le revers de la médaille — plus notre société se numérise, plus elle s'expose aux risques inhérents à ces technologies. Les attaques informatiques sont désormais susceptibles de porter gravement atteinte à notre économie, aux intérêts de notre défense et de notre sécurité nationale et à la vie même de nos concitoyens. Les scénarios du pire ne relèvent déjà plus de la fiction : sans même évoquer les menaces d'origine étatique, de simples groupes isolés ont potentiellement les moyens de provoquer de véritables catastrophes.

La sécurité est donc une condition fondamentale à la réalisation des promesses sociales, économiques, citoyennes et démocratiques du numérique. Pour chacun d'entre nous, elle est une condition de la confiance que nous pouvons accorder aux technologies. Pour les États, la sécurité du numérique est devenue une composante majeure de leur sécurité nationale. Presque une condition de survie.

Pour cause. Si les capacités de cyberdéfense développées par la France visaient historiquement à protéger les systèmes les plus critiques et contrer les acteurs les plus menaçants, les frontières tendent à se déplacer. À l'heure de l'entreprise étendue et de l'interconnexion croissante des organisations, la sécurité d'un acteur sensible dépend dorénavant des éléments les plus faibles de son écosystème. Et cet écosystème est parfois très vaste, d'une grande complexité. Cette donne n'a pas échappé aux attaquants, qui cherchent désormais à exploiter les relations de confiance entre les organisations et leurs partenaires à leur profit en s'en prenant aux prestataires et aux sous-traitants pour atteindre leurs cibles principales.

Partout dans le monde, la cybercriminalité est par ailleurs en pleine explosion. Touchant indifféremment les organisations et les particuliers, cette forme de criminalité est amenée à s'installer durablement dans la prochaine décennie. C'est qu'elle est particulièrement lucrative : sur les dernières années, le butin de certains groupes criminels avoisine ou dépasse le milliard d'euros.

Qu'il s'agisse de la complaisance de certains États avec des groupes criminels ou de l'impact d'une attaque indiscriminée affectant des milliers de cibles en France voire au-delà, la frontière entre la lutte contre la cybercriminalité et les considérations de sécurité nationale se fait ténue. Une attaque contre une petite ou moyenne entreprise serait naturellement appréhendée sous l'angle de la cybercriminalité. Mais quid, par exemple, d'un rançongiciel qui toucherait des milliers de PME sur l'ensemble du territoire ?

Dans ce contexte de menace croissante, la maîtrise du cyberespace devient l'une des clés de puissance dans le monde à venir. C'est déjà une priorité stratégique pour les grandes puissances mondiales, qui mobilisent tous les moyens techniques, opérationnels, diplomatiques et juridiques pour asseoir une forme de supériorité, voire de suprématie, dans ce nouvel espace. On assiste alors à la consolidation d'un premier cercle de cyberpuissances, condamnant l'ensemble des autres États à une forme de vassalité. Dans le même temps, les géants privés du numérique, dont la dernière décennie a marqué l'avènement fulgurant, ne sont pas en reste. En majorité chinois et américains, ceux que l'on surnomme « *Big Tech* » en raison d'une taille critique et d'une puissance financière sans précédents ambitionnent désormais de parler d'égal à égal avec les États. Voire de contester certains monopoles régaliens, qu'il s'agisse de fournir une identité, de battre monnaie ou d'assurer la sécurité des biens et des personnes.

Dans ce contexte de reconfiguration géopolitique profonde, la France jouit d'une position singulière. Sa stratégie audacieuse et ambitieuse l'a amenée à développer des capacités autonomes, lui permettant de demeurer l'une des rares nations encore capables de faire entendre une voix crédible, équilibrée, indépendante et forte à l'international. Elle est une puissance fédératrice dans la construction d'une Europe de la cybersécurité. Elle peut de plus compter sur une industrie performante, des startups prometteuses et un réseau académique de tout premier rang mondial. Ces forces tiennent pour beaucoup à nos valeurs, à notre histoire mais également à notre modèle.

Ce modèle est original. Il repose sur une vision globale et équilibrée de la cybersécurité portée par une agence placée sous l'autorité du Premier ministre, et une séparation stricte entre les missions de défense et de sécurité numériques, confiées en large partie à l'ANSSI, et les missions cyberoffensives.

Plus de dix années après l'intuition initiale, notre modèle confirme toute sa pertinence. Mieux, il continue de faire école : d'autres pays s'en inspirent explicitement pour construire ou adapter leurs propres architectures institutionnelles. C'est qu'il présente d'indéniables avantages. La vocation strictement défensive de l'Agence lui permet notamment d'afficher une posture claire et non ambiguë devant ses interlocuteurs — entreprises ou administrations victimes, assemblées parlementaires, chercheurs, médias, organisations non gouvernementales — pour jouer à plein un rôle de gardien et d'éclaireur dans les transformations numériques.

Ce modèle a en outre rendu possible la mise en œuvre de législations ambitieuses — souvent pionnières. Il en va ainsi du dispositif réglementaire de sécurisation des activités d'importance vitale qui a préfiguré un dispositif similaire de niveau européen et qui nous est envié en dehors de nos frontières. Les récentes évolutions législatives, qui ont permis d'accroître significativement les capacités de détection et de contrôle réglementaire de l'ANSSI, sont également rendues possibles par ce modèle protecteur.

Produit de la riche histoire cryptographique française, l'ANSSI est une agence fière de son ADN technique. Elle est avant tout une organisation humaine composée de plus de 600 femmes et hommes qui font la preuve chaque jour d'un engagement et d'un professionnalisme sans faille, dans un domaine où l'humilité doit rester la règle.

Forte de son rattachement à la Secrétaire générale de la défense et de la sécurité nationale, l'Agence a déjà su profondément évoluer dans sa nature. Si elle a bâti ses fondations sur une expertise résolument technique, elle est désormais reconnue dans sa capacité à sécuriser les systèmes d'information critiques, à répondre aux attaques les plus graves mais aussi à opérer les réseaux de communications interministériels sécurisés ou à conseiller le Gouvernement sur les politiques publiques de sécurité numérique, en lien avec les administrations concernées.

Notre légitimité et notre crédibilité, consolidées dans la dernière décennie, nous permettent aujourd'hui de faire autorité et d'asseoir une position singulière en interministériel, en Europe et à l'international. L'Agence est régulièrement cheffe de file dans le cadre de négociations internationales. Au sein de l'Union européenne, elle s'illustre par sa proactivité. Elle plaide pour une approche ambitieuse de la cybersécurité tournée vers l'économie et la société, et participe à modeler les législations européennes en la matière.

L'ANSSI est à l'origine de nombreux succès opérationnels. Des succès que nous continuerons, pour la plupart, à garder pour nous — la préservation de l'identité des victimes étant essentielle à leur protection — mais qui contribuent à nous rendre fiers de notre action.

La croissance consentie à l'ANSSI durant la dernière décennie, comme celle prévue pour les années à venir, traduisent la conscience élevée de nos autorités politiques face à l'ampleur du risque numérique. C'est également une marque de confiance importante. En ce sens, ces moyens nous obligent.

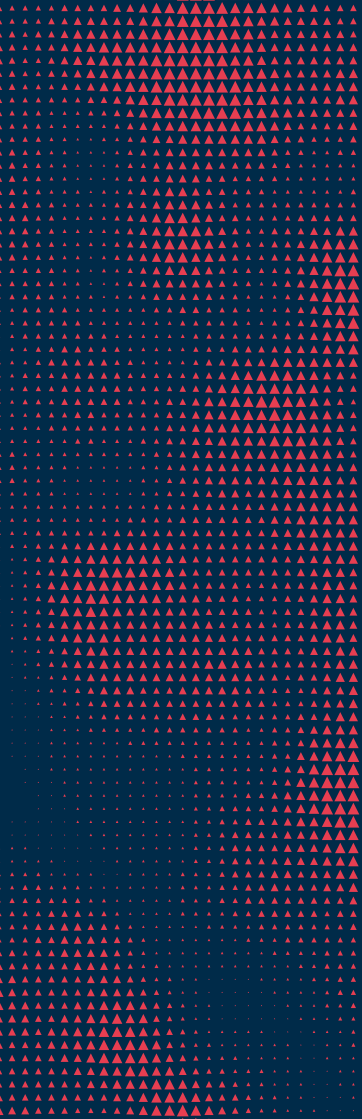
Après une première décennie de développement qui nous a permis d'occuper un rôle central dans la compréhension, la prévention et la réponse au risque numérique, l'ANSSI doit tirer le meilleur parti de cette croissance en cours et à venir. D'ici 2025, elle sera implantée sur au moins trois sites en France, avec l'ouverture dans les prochaines années d'une implantation à Rennes.

Cette évolution ne peut être homothétique. Ces moyens supplémentaires ne doivent pas seulement nous conduire à faire plus, en simple proportion, mais nous amener à parfois faire différemment. À explorer des partenariats moins naturels pour nous enrichir de visions différentes. Le contexte profondément incertain dans lequel s'inscrit notre action nous oblige à réorienter nos priorités lorsque c'est nécessaire, à toujours et encore rechercher de nouveaux relais et effets démultiplicateurs.

En effet, face au dynamisme et aux volontés hégémoniques de certaines puissances mondiales, l'écosystème français doit faire front ; l'ANSSI prendra part à cet effort collectif. Car si les capacités et l'engagement des acteurs régaliens sont essentiels (et doivent le demeurer !), ceux-ci ne pourront assumer seuls l'objectif de confiance et de sécurité numériques. Plus que jamais, les acteurs publics doivent montrer la voie, susciter l'adhésion, fédérer, accompagner la prise en compte progressive de ces enjeux.

Tel un « village d'Astérix 4.0 », l'écosystème français de cybersécurité est petit en comparaison de certains géants mondiaux. Il est cependant composé d'acteurs qui, s'il leur arrive d'en découdre, s'apprécient, se soutiennent mutuellement et continuent de résister encore et toujours à l'envahisseur. Mieux, cette communauté continue à se structurer, ce qui donne déjà lieu à de belles réalisations.

Il ne s'agit bien sûr pas de remettre en question notre cœur régalien et notre capacité à protéger le secret garant de notre efficacité opérationnelle et de la confiance que nous accordent nos partenaires. Mais bien de faire évoluer notre approche, notre action comme nos modes d'intervention pour davantage tirer parti de cet écosystème en construction et grandir collectivement.



La compétence,
l'ouverture et l'agilité
sont les trois valeurs
centrales de l'ANSSI.
Elles constituent
le socle de notre
stratégie.

Valeur centrale de l'Agence, la compétence constitue le premier pilier de notre stratégie.

1.

Nous devons d'abord jouer à plein notre rôle d'éclaireur des transformations numériques.

Dans ce contexte d'accélération technologique et dans la continuité de la création d'un conseil scientifique, il s'agit de renforcer notre capacité à anticiper les ruptures technologiques et les révolutions d'usages, à discerner les signaux faibles, annonciateurs des mutations profondes pour le monde numérique. Nous devons pouvoir accompagner ces transformations, en acquérant les compétences nécessaires pour toujours mieux éclairer notre écosystème et les politiques publiques numériques. Nous devons également davantage développer notre vision stratégique de ces défis numériques, en consacrant le temps nécessaire à l'élaboration de cette vision et en diffusant au sein de l'Agence une culture de la mise en perspective.

2.

Nous devons sans cesse renforcer notre efficacité opérationnelle face à des menaces profondément changeantes, notamment face à la recrudescence des menaces de masse.

Les évolutions législatives de ces dernières années confient à l'ANSSI un accès à des volumes croissants de données techniques de cybersécurité, d'une valeur exceptionnelle. Il y a là une responsabilité importante, mais aussi une grande opportunité de renforcer notre capacité à détecter et répondre aux attaques. Pour cela, nous devons être en mesure de faire fructifier cette donnée pour renforcer la cybersécurité d'aujourd'hui et inventer les moyens de la cybersécurité de demain.

3.

Nous devons davantage mettre cette compétence au service de la formation en cybersécurité.

Dans un contexte de compétition internationale acharnée sur les talents, nous devons renforcer notre engagement dans la formation initiale et continue pour intégrer plus avant ces thématiques dans les formations en informatique. Dans un monde où les compétences numériques deviennent des fondamentaux, la cybersécurité doit également être renforcée dans les enseignements scolaires, notamment pour susciter les vocations dès le plus jeune âge. C'est le sens des efforts très concrets entrepris avec le ministère de l'Éducation et de la Jeunesse et le Service national universel, en plus des efforts engagés depuis longtemps dans la formation supérieure et continue. La formation accrue des décideurs, des agents publics, des acteurs économiques et des citoyens sera également un axe essentiel de cet effort.

L'ouverture, à nos partenaires traditionnels ainsi qu'à des partenaires nouveaux, constitue le deuxième point d'appui de cette stratégie.

4.

Nous devons continuer à développer les synergies opérationnelles avec nos partenaires institutionnels nationaux.

C'est notamment le sens de la future implantation de l'Agence à Rennes, qui vise à la rapprocher des acteurs institutionnels majeurs de la sphère du ministère des Armées, à commencer par le COMCYBER. En effet si les dix dernières années ont permis de consolider notre modèle et d'organiser la séparation du glaive et du bouclier, les dix prochaines devront permettre de renforcer la coordination des différentes chaînes opérationnelles, dans le sillage de la création du centre de coordination des crises cyber (C4) présidé par la secrétaire générale de la défense et de la sécurité nationale. Le tout sans mélange des genres, en préservant les forces de notre modèle, les responsabilités et les missions de chacun.

5.

Nous devons accompagner la structuration de l'écosystème de cybersécurité.

Cette ouverture se traduira notamment par un partage renforcé de l'expertise de l'Agence, de ses outils et de ses données, notamment au profit des plus petits acteurs. L'objectif ? Stimuler l'innovation publique et privée au bénéfice de l'ensemble de la communauté. Il s'agira également de s'engager dans la réussite du prometteur projet industriel de Campus Cyber, souhaité par le président de la République et qui participe précisément de cette nécessité de fédérer et structurer l'écosystème. En construction, le premier partenariat entre l'ANSSI et INRIA constitue par ailleurs le terreau idéal pour renforcer et développer nos liens avec le monde académique. Plus largement, le recours à l'expertise académique, y compris aux sciences humaines et sociales, doit nous permettre de renforcer nos messages et d'élargir nos capacités d'influence.

6.

Nous devons renforcer notre engagement européen

pour accélérer la construction d'une Europe de la cybersécurité, en complémentarité avec l'échelon national. « *Europe first* » : l'ANSSI continuera à mettre à profit ses métiers et compétences pour contribuer à la sécurité et de la souveraineté de plus de 500 millions d'Européens. Il s'agit également de consolider la position singulière de la France, de promouvoir et défendre le modèle français de cybersécurité et sa vision en matière de sécurité et de stabilité du cyberespace.

L'agilité, enfin, constitue le troisième pilier de cette stratégie.

7.

Nous devons encore plus être une « administration orientée bénéficiaires »

pour toujours mieux comprendre les besoins, les attentes mais également les contraintes des bénéficiaires de notre action. Il s'agit notamment d'adapter nos prestations et de développer notre offre de services en nous appuyant sur une exploitation accrue des données dont nous disposons, tout en tenant mieux compte du niveau de maturité de chaque acteur. Cela implique également de refuser la tentation — naturelle pour le défenseur — de la « surqualité » pour viser un niveau de sécurité toujours adapté aux enjeux. Enfin, il convient d'explorer la possibilité de développer une plateforme hébergée par l'agence, où des services seraient développés par d'autres au profit de nos bénéficiaires, en valorisant les données dont nous disposons.

8.

Nous devons également renforcer notre culture interne de l'expérimentation et amplifier notre capacité d'innovation.

L'agilité suppose de se donner la possibilité de pivoter et d'expérimenter dans un contexte profondément changeant et incertain, où les cycles d'innovation ne cessent de se raccourcir. Cela passera notamment par le lancement d'une démarche d'innovation et un accompagnement plus resserré des projets de nos agents, y compris d'éventuels projets entrepreneuriaux.

9.

Nous devons enfin renforcer l'accompagnement de nos agents.

Parce que l'ANSSI est avant tout une organisation humaine, un effort important sera mis en œuvre pour offrir aux agents les meilleures conditions pour mener à bien leurs missions. En phase avec les aspirations de nos agents, il s'agit là de renforcer les fonctions de soutien et d'améliorer l'outillage pour permettre à chacun de se concentrer sur l'essentiel. Il est également question de réussir le défi d'un fonctionnement multi-sites. En un mot, de faire de l'Agence un endroit où il fait bon vivre et travailler au profit de l'intérêt général.

Premier ministre