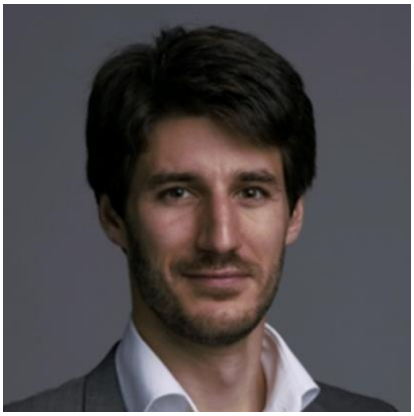
La Stratégie Nationale pour la Cybersécurité



William LECAT
Coordinateur Stratégie Nationale Cybersécurité
Secrétariat Général pour l'Investissement

Annoncée le 18 février par le Président de la République et financée dans cadre du plan France Relance et du 4e Programme d'investissements d'avenir, la Stratégie Nationale pour la Cybersécurité marque un tournant important du domaine. Les objectifs affichés, simples et concrets, sont très ambitieux. Les moyens conséquents mis en œuvre par les pouvoirs publics et le secteur privé pour les atteindre sont historiques. Pour la première fois en cybersécurité, des financements de taille sont débloqués pour le court, le moyen et le long termes avec des ambitions sociétales, économiques et technologiques à la hauteur des grands challenges que portent ces innovations technologiques plus que jamais nécessaires dans un monde ouvert et potentiellement vulnérable à des attaques cyber dont le nombre et la violence ne cesse de croître. Si le Grand Défi cybersécurité, lancé fin 2019, montrait déjà une volonté politique forte de prendre le sujet à bras le corps, cette Stratégie Nationale aux budgets allant deux ordres de magnitude plus loin ne laisse aucun doute sur la place prioritaire que le Gouvernement donne à la cybersécurité.

La cybersécurité est un secteur dont la croissance est structurellement liée à celle de la numérisation. Une numérisation croissante implique donc une importance grandissante de la cybersécurité. Si cet aspect semble évident, la prise de conscience et sa concrétisation impliquent souvent une étape supplémentaire : l'augmentation du nombre d'attaques et de leurs impacts. La pandémie mondiale que nous vivons depuis plus d'un an, épreuve inédite pour nos contemporains, a accéléré la numérisation de nos sociétés et de nos organisations exacerbant ainsi le niveau de maturité, probablement déjà insuffisant, en cybersécurité. Il est par ailleurs probable que la recrudescence des attaques lors de cette période corresponde seulement aux prémices de ce qui est à venir. Le parti pris d'accélérer fortement sur la cybersécurité est donc particulièrement nécessaire. C'est pourquoi l'Agence nationale de la sécurité des systèmes d'information (ANSSI) bénéficie d'un budget directement issu du plan France Relance pour sécuriser le socle numérique de l'Etat et des territoires. Ces 136 M€ visent un impact à court terme en finançant des états des lieux, des plans d'actions, des aides au déploiement et de l'achat d'équipements de sécurité déjà disponibles. Il s'agit d'un financement qui vient se rajouter aux différents budgets des bénéficiaires pour leur permettre d'accélérer leur sécurisation. L'objectif à moyen terme est également d'ancrer les bonnes pratiques dans les habitudes des usagers et des organisations que ce soient des entreprises ou des collectivités territoriales.

Mais l'ambition de la France n'est pas seulement de se « cybersécuriser » rapidement. Il s'agit également de maitriser cette sécurisation, d'en être non

seulement le consommateur mais également un fournisseur. Le besoin et la demande sont en forte croissance. Ce phénomène ayant vocation à s'amplifier et la Nature ayant communément horreur du vide, il est indispensable que les industriels français puissent se positionner rapidement et prennent une place de leader sur ce secteur prometteur. Cela passera naturellement par un effort marketing et commercial de leur part mais aussi par un investissement technologique majeur pour faire de l'innovation la source de notre compétitivité. C'est là que la nécessité de rapprocher la recherche et l'industrie devient essentielle. Sur le moyen et long termes, la pérennité de l'économie de la filière cyber passera par l'innovation qui ne peut être alimentée que par une cohérence profonde entre les différents niveaux de maturité de la recherche fondamentale à la recherche industrielle et ses applications pour répondre aux besoins d'aujourd'hui et de demain. Le 4e Programme d'investissements d'avenir (PIA4) nous permet de bénéficier de 360 M€ de financements publics pour soutenir tous les maillons de cette chaine de recherche et développement. Ce budget se décompose en 65 M€ pour la recherche fondamentale, 275 M€ pour les transferts technologiques et la R&D industrielle et 20 M€ pour des démonstrateurs territoriaux. L'objectif économique pour 2025 est d'atteindre les 25 milliards d'euros de chiffre d'affaires de la filière française, soit une multiplication par 3,5. Un objectif ambitieux mais à la hauteur du potentiel de la filière et réalisable grâce à la mobilisation de toutes les parties prenantes.

La demande est donc conséquente et en constante évolution. Malgré une très forte volonté de positionner l'écosystème français pour y répondre, ce secteur en très forte croissance se heurte à un frein majeur : le manque de personnes qualifiées. En réalité, le nombre d'experts cyber est important et croît rapidement, mais moins vite que la demande pour ces profils. La capacité de formation augmente également vite mais l'attractivité du secteur reste encore limitée pour le moment, rendant difficile de remplir toutes les formations. Il semblerait que le domaine et les métiers cyber pâtissent encore d'une image peu attractive incluant toutes formes de capuches et autres vies recluses dans des garages. Ce stéréotype est bien loin de la vérité. Il s'agit en fait de métiers aux compétences (techniques mais pas uniquement) de pointe avec des salaires au-dessus de la moyenne tous domaines confondus et surtout bénéficiant d'un dynamisme économique et technologique extrêmement important ce qui promet des perspectives variées et passionnantes. En résumé, des métiers d'avenir. Il est donc indispensable de penser et de mettre en œuvre une sensibilisation tournée vers l'attractivité de la filière. Un observatoire des besoins en compétences cyber devra permettre de quantifier et d'orienter précisément les efforts en formations. De forts besoins pour des formations « courtes » ont déjà été identifiés, l'essentiel des formations actuelles étant centré sur les niveaux bac+5 et bac+8. Il est aussi important de mettre l'accent sur la formation continue et les capacités de reconversion. La diversification de l'offre de formation en cohérence avec les besoins observés et anticipés, couplée à une sensibilisation à différents niveaux pour attirer et créer des vocations seront indissociables de l'atteinte des objectifs de la Stratégie qui vise à porter à 75 000 le nombre d'emplois dans le secteur en 2025.

La sensibilisation large spectre permettant une prise de conscience des enjeux et des dangers et conduisant à l'augmentation du niveau d'éveil cyber global est également très importante et doit être menée en parallèle. Une sensibilisation « grand public » semble particulièrement nécessaire. La sensibilisation des femmes et hommes, agents du public comme du privé, représentera « la brique de base » pour pouvoir ensuite présenter les solutions envisageables contre les différentes menaces. Les plans de continuité et de reprise d'activité face à la menace cyber sont particulièrement importants pour la résilience de notre société et représenteront un bon indicateur de l'impact organisationnel de la sensibilisation.

De manière générale, la « visibilité » des aspects de cybersécurité est aussi importante pour les différents secteurs utilisateurs que pour l'écosystème cyber lui-

même. En effet, ce dernier souffre d'une forte fragmentation qui nuit à son rayonnement. La création d'un lieu « totem », matérialisé par le Campus Cyber, permettant de rapprocher les différents acteurs cyber, de l'industrie, de l'administration et de la recherche tout en intégrant des clients finaux, sera donc un élément clé de la structuration de la cybersécurité française. La déclinaison de cet espace de référence au sein des territoires permettra une consolidation du secteur bénéficiant à tous les objectifs de la Stratégie Nationale. Ce projet, inspiré de plusieurs initiatives dans d'autres pays et de leurs enseignements, est une première mondiale dans son approche et ses objectifs. Le Campus Cyber devrait ouvrir ses portes en novembre 2021 à la Défense en région parisienne.

Dans cet effort de consolidation, un accent particulier sur la stimulation et le soutien à l'entreprenariat sera également mis. En effet, notre capital d'expertises techniques et d'excellences scientifiques devrait nous permettre d'accueillir un nombre croissant de startup dans les prochaines années. Il conviendra donc de faciliter leur création et d'accélérer leur développement en les accompagnant et en leur permettant d'accéder à des financements via une structure dédiée. Cela pose implicitement la question de notre capacité à financer les « scale-up » et les futures licornes françaises du domaine. Les différents rachats et départs de jeunes pousses prometteuses ne laissent pas d'ambiguïté sur la nécessité croissante d'adresser activement le sujet. Les réflexions entamées indiquent, sans grande surprise, que le bon niveau à terme se situe à l'échelle de l'Europe pour l'émergence de fonds d'investissement adressant cette problématique. Tout d'abord, les financements importants que permet l'échelon européen et le nombre relativement limité d'opportunités d'investissements de ce niveau laissent à penser que les thèses d'investissement de ce type de fonds devront dépasser les frontières de l'Hexagone. Cela semble d'autant plus vrai que beaucoup de startups en « hypercroissance » se tournent naturellement (avant tout rachat) vers le marché le plus important du monde dans le domaine, les Etats-Unis. La structuration d'un marché Européen (au sens de l'Union Européenne) offrirait donc le levier de croissance nécessaire pour permettre l'émergence de licornes et de fonds d'investissement pour les financer. Il se trouve en réalité que cet aspect résonne avec tous les objectifs de la Stratégie. La construction cyber en cours au niveau européen, autour du centre de compétence cyber européen et des déclinaisons nationales, représente donc une opportunité d'amplifier les impacts de la Stratégie Nationale Cybersécurité et d'accélérer son déploiement.