Impact des recherches en cybersécurité sur la stratégie nationale en matière de souveraineté numérique

Laurent OLMEDO

Directeur du programme Sécurité globale Direction des applications militaires, CEA

Bruno CHARRAT

Responsable du programme cybersécurité Direction de la recherche technologique, CEA

Renforcer notre souveraineté numérique au plan national revêt un double enjeu, à savoir conserver notre liberté d'appréciation, de décision et d'action en cas de cyberattaque et préserver nos domaines de souveraineté traditionnels au regard des cybermenaces. Ceci passe par la disponibilité d'une filière industrielle nationale, voire européenne, forte et compétitive dans le domaine des produits et services de cybersécurité ainsi que d'une recherche d'excellence afin de préparer à l'avance les futurs outils de cybersécurité.

La crise sanitaire que notre pays traverse a pour conséquence indirecte de montrer l'importance des technologies digitales pour apporter une forme de résilience au plan de la continuité d'activité. Elle souligne également combien les vulnérabilités en matière de cybersécurité pouvaient surajouter du risque à la menace sanitaire. Ce premier retour d'expérience démontre qu'il est urgent de concrétiser les ambitions de la France en cybersécurité avec la mise en place d'une réelle capacité prenant en compte nos enjeux de souveraineté.

De nombreuses initiatives nationales

Le président de la République a lancé depuis près d'un an la démarche du pacte productif qui vise à dynamiser l'économie française. L'un des volets de cette initiative consiste à identifier les marchés clés prioritaires qui sont à soutenir et accélérer, afin d'en exploiter tout le potentiel économique. La cybersécurité a été identifiée comme l'un de ces secteurs clé, notamment afin de contribuer à garantir notre souveraineté numérique.

En complément, un rapport intitulé « Faire de la France une économie de rupture technologique[1] » a été remis par un collège d'experts aux Ministres de l'Économie et de L'Enseignement supérieur, de la Recherche et de l'Innovation mi-février. Ce document retient également la cybersécurité comme l'un des 10 marchés clés (cf. p.54 du rapport), ce qui signifie en pratique que la cybersécurité sera identifiée comme l'une des priorités claires du futur Programme d'investissements d'avenir (PIA 4).

Ce rapport demande pour ces secteurs clés une concentration des moyens de l'État, une meilleure coordination des initiatives de l'Administration, une intervention des pouvoirs publics sous forme

[1] https://cache.media.enseignementsup-recherche.gouv.fr/file/Mediatheque/41/1/Rapport_college_experts_06_02-2_1242411.pdf

notamment de « stratégies d'accélération » visant à soutenir les technologies diffusantes.

De façon plus large, l'État a déjà lancé plusieurs initiatives structurantes depuis 2018. Elles visent à accélérer autant que possible les stratégies en cours, définies en concertation avec les industriels, en particulier :

- La structuration d'une politique industrielle en matière numérique reposant sur la maîtrise de « technologies clés » qui est l'une des recommandations de la revue stratégique de cyberdéfense conduite par le SGDSN en février 2018, pour assurer la souveraineté numérique de la France ;
- L'action du Ministère des armées, avec la publication en Juillet 2019 du document d'orientation de l'innovation de défense (DOID) par l'Agence d'innovation de défense (AID) dans lequel l'objectif des travaux de recherche en cybersécurité répond au « double enjeu de défense des infrastructures critiques souveraines de l'État et de préservation de l'efficacité opérationnelle de nos forces » ;
- Le Comité stratégique de filière (CSF) « Industries de sécurité », dont le contrat a été signé le 29 janvier 2020, et son projet structurant « Cybersécurité et sécurité de l'IoT » ;
- La mission de préfiguration d'un campus cyber confiée à Michel Van Den Berghe, dont le rapport a été rendu public le 29 janvier 2020, et qui rentre dans sa phase d'opérationnalisation avec un objectif d'ouverture du campus au premier semestre 2021 ;
- Le lancement d'un Grand défi Automatisation de la cybersécurité dans le cadre du Conseil de l'Innovation.

Ce contexte général rend encore plus impérieux la nécessité de maintenir l'excellence de la recherche Française, à même de s'impliquer dans cette dynamique nationale et de répondre au besoin constant de disposer de nouveaux outils et technologies.

En effet, le domaine de la sécurité numérique est à la fois en forte croissance et face à un potentiel de crise majeure résultant de la professionnalisation et de la sophistication des attaques. Les **solutions technologiques matérielles et logicielles existantes ne suffisent parfois plus** à endiguer le flot des **fuites de données et des prises de contrôle de systèmes**, allant du bénin (pages personnelles) au **souverain** (infrastructures d'importance vitale, identité). Contrer ces menaces requiert de sécuriser l'ensemble des systèmes d'information qui supportent la souveraineté nationale et permettent la sécurité du citoyen. L'enjeu est de taille, et le succès d'une telle démarche permettra de créer les conditions pour une **confiance des citoyens dans le numérique, grâce à des filières industrielles et de services**.

Face à ce défi, les acteurs nationaux de la recherche sont rassemblés au sein de l'alliance des sciences et technologies du numérique Allistene qui regroupe en tant que membres fondateurs la CDEFI, le CEA, le CNRS, la CPU, Inria et l'Institut Mines-Télécom.

Le CEA, un acteur singulier de la recherche en cybersécurité

De par ses activités dans le nucléaire, le Commissariat à l'Énergie atomique et aux énergies alternatives (CEA) est fortement concerné par ce sujet de la cybersécurité. D'une part, le CEA a des **problématiques propres de cybersécurité opérationnelle**, l'obligeant à exploiter ses systèmes d'information (SI) et opérer ses systèmes industriels (ICS), en cohérence avec le référentiel réglementaire édicté par l'ANSSI en ce qui concerne les activités civiles du CEA et par le Ministère des Armées pour les activités de défense.

Le CEA doit ainsi organiser **la protection au quotidien de 30.000 postes de travail, plus de 500 services ouverts sur internet avec 3 accès à très haut débit**. Cette cyberprotection du CEA sur l'ensemble de ses activités dans un périmètre étendu avec des systèmes d'information très diversifiés et une menace constante a nécessité de se doter **d'une très grande expertise opérationnelle**, afin de protéger des activités critiques telles que les infrastructures nucléaires, de calcul intensif, ou les activités en science du vivant.

D'autre part le CEA s'est doté d'une capacité de recherche technologique pour répondre à ses besoins propres et à ceux de ses partenaires en focalisant son action sur les deux grands axes d'activités suivants :

- **Recherche et développement de nouvelles technologies pour la sécurisation des systèmes** et leur transfert à des acteurs industriels. Selon les cas, le terme système peut recouvrir un circuit intégré, un système électronique – logiciels – réseaux – services connecté dans le cyberspace tels que des véhicules, équipements industriels, dispositifs médicaux…) ;

- **Recherche et développement de nouvelles méthodes de caractérisation et d'outils d'évaluation** de systèmes commerciaux ou en cours de développement par les industriels, afin d'en détecter les vulnérabilités.

Le CEA mène ses programmes d'innovation et de transfert technologique avec pour objectif d'accompagner le développement de la filière industrielle et de donner les moyens techniques aux services de l'État et à l'industrie d'assurer leur cyberprotection. Pour cela, **le CEA travaille en étroite collaboration avec ses partenaires de l'Alliance Allistene** avec pour objectif de créer des technologies et **des outils innovants**, et de fournir des preuves de concept concrètes, opérationnelles permettant aux industriels d'expérimenter et évaluer les briques technologiques. Ces activités d'intégration mobilisent donc de nombreuses compétences transverses (microélectronique, numérique), essentielles à la réalisation de ces démonstrateurs :

- **Une expertise reconnue internationalement** : sur certains sujets (par exemple la recherche de vulnérabilités), le CEA conduit des recherches au meilleur niveau national et international. En témoignent les travaux fondateurs conduits depuis 2015 avec **l'ANSSI**, sur l'utilisation de l'intelligence artificielle (IA) en attaque de composants électroniques ou encore la mise en open source d'outils logiciels de référence comme Frama-C (qualification de la sécurité des logiciels) ou Miasm (reverse engineering de codes malveillants) ;

- **La montée en maturité technique grâce à des plateformes technologiques** : maillon indispensable des recherches en cybersécurité le CEA a investi dans des plateformes qui permettent d'aller jusqu'à une démarche de prototypage. Certaines de ces plateformes constituent des moyens uniques au plan national.

Avec sa singularité, le CEA est reconnu par ses partenaires académiques, industriels et institutionnels comme un acteur de confiance de la filière cybersécurité française et européenne. Ainsi, dès 1999, le CEA a mis en place à la demande des pouvoirs publics, **un Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI)**, afin de répondre aux besoins des industriels français. Ce CESTI, agréé par l'ANSSI, fait ainsi partie du **schéma Français de certification des composants sécurisés et de micrologiciels**. Le CEA est également fortement sollicité par ses partenaires pour assurer la coordination globale d'actions collaboratives nationales et Européennes. C'est en particulier le cas du projet européen **SPARTA** qui est l'un des quatre pilotes retenus pour créer un « Réseau de compétences en cybersécurité » financé par la Commission Européenne. Son objectif est de ré-

imaginer la manière dont la recherche, l'innovation et la formation se pratiquent et se coordonnent au sein de l'Union européenne afin de participer au renforcement de l'autonomie stratégique européenne par la mutualisation des expertises. Ses travaux alimenteront également les réflexions préalables à l'établissement d'un centre de compétences européen en cybersécurité.

Enfin, le CEA s'est doté d'un programme spécifique de recherche en **Sécurité globale** qui a permis de créer une interaction forte avec les pouvoirs publics (DGA, ANSSI, Ministères des Armées et de l'Intérieur) en apportant une expertise scientifique et technique et en positionnant les projets de recherche dans une dimension régalienne. Cette capacité a également démontré son utilité dans la crise liée au CoVID-19.

Quelles actions à engager pour renforcer la souveraineté numérique de la France ?

Le propos liminaire du DOID[2] dresse ce constat : « Innover est plus que jamais une nécessité opérationnelle et stratégique, c'est même un enjeu de souveraineté nationale ». Toutefois cette démarche se doit d'être faite dans un cadre structurant et fédérateur des initiatives afin d'en tirer le meilleur bénéfice au plan national.

Pour réussir, il est indispensable, comme le dit l'ANSSI dans son manifeste 2020, de structurer « l'écosystème de cybersécurité ». À ce titre, l'initiative du Campus cyber Parisien devrait devenir une pierre angulaire au plan national dans sa capacité à rassembler des acteurs, en vue de la création de « communs en cybersécurité » et à faire émerger d'autres campus sur le territoire national, fonctionnant en réseau, afin de tirer parti au mieux des expertises disponibles localement.

Cette démarche bénéficiera d'un contexte où la cybersécurité est l'archétype des recherches dites « duales », tant du point de vue de l'irrigation conjointe et respective des deux domaines civil et défense, que de celui des forts enjeux de criticité (parfois différents) qui y sont associés pour chacun d'entre eux.

À ce titre, l'initiative du Ministère des armées avec la création récente du Cyberdéfense factory au sein du pôle Rennais est un bon exemple de création d'outils innovants indispensables permettant de renforcer les interactions entre les différents acteurs.

L'autre enjeu sera de renforcer la coordination des actions de recherche et innovation afin d'éviter tout risque de travail en silo et d'éparpillement des moyens. Le développement de nouveaux outils de cybersécurité est en effet intrinsèquement interdisciplinaire (hardware, software, mathématiques, sciences sociales…) et il est indispensable de pouvoir faire travailler ensemble des experts d'horizons divers, sur des plateformes technologiques à l'état de l'art et en étroite interaction avec les acteurs industriels et étatiques, afin de garantir la performance, la pertinence et la légalité des outils. Des initiatives comme le Grenoble Alpes Cybersecurity Institute, fondé en 2018 et rassemblant des experts de 16 laboratoires pour conduire des travaux interdisciplinaires sont des exemples à suivre et répliquer.

Il ne peut en effet y avoir de projets de recherche structurants sans connexion avec une analyse fine de la menace actuelle et de sa projection dans un futur court et moyen terme. Il ne peut y avoir également de projets de recherche à visée stratégique sans une analyse fine des enjeux liés aux grandes évolutions en cours ou à venir, comme en témoigne le domaine de la cryptographie post-quantique.

[2] Document d'Orientation de l'Innovation de Défense. Lien : https://www.defense.gouv.fr/aid/actualites/le-document-d-orientation-de-l-innovation-de-defense-doid

Dans cette perspective, on peut souligner le travail effectué par le SGDSN dans sa revue stratégique en matière d'identification de technologies critiques destinées à assurer notre souveraineté numérique.

Il reste désormais à construire la feuille de route nationale en matière de projets de recherche, dans une dimension interdisciplinaire qui tire le meilleur des technologies numériques pour développer de nouveaux composants de confiance ou encore de nouveaux outils d'analyse de la sécurité en soutien des analystes

Tout le succès des programmes de recherche qui vont se mettre en place reposera en définitive sur une démarche « coordonnée » : connaissance partagée des enjeux, des réalités de chaque acteur, ainsi que sur la construction de feuilles de route conjointes. Les initiatives lancées au plan national ne trouveront pleinement leur sens que dans cette logique et pourront alors renforcer la souveraineté numérique de la France et sa place dans un espace européen et international fortement compétitif.

Au plan européen, beaucoup reste encore à faire pour que se concrétisent les objectifs que se donne également la nouvelle Commission européenne au plan de la souveraineté numérique. L'importance de cette dimension européenne a conduit le CSF « Industries de sécurité » à l'inscrire dans sa feuille de route.

Tout semble réuni pour que notre pays tire pleinement parti des capacités existantes pour renforcer sa souveraineté numérique. Le CEA a de son côté l'intention d'apporter sa contribution à cet effort national, notamment en participant au Campus cyber, et en poursuivant son engagement européen dans la coordination de réseaux d'acteurs à l'instar de ce qui a déjà été engagé avec SPARTA et son implication dans ECSO.