

Cybersécurité, le défi du siècle

Datum 13.10.2026
Sujet Commissariat à l'énergie atomique
Region France
Kategorie IT, Science and research, Security

Alors que les cyberattaques n'épargnent désormais aucun aspect de notre vie quotidienne, la cybersécurité est devenue un impératif pour la souveraineté des États et la résilience de la Nation. Conscient de l'enjeu, le CEA s'appuie sur une stratégie développée de longue date et des moyens de recherche conséquents, pour soutenir une transformation numérique sans risque au service de ses propres activités mais aussi des citoyens, des entreprises et des institutions.

Pourquoi la cybersécurité est un enjeu stratégique pour la souveraineté numérique ?

Piratage de l'Education nationale et des Finances publiques après celui de l'Agence nationale des titres sécurisés, fuite de données de France Travail, cyberattaques d'hôpitaux et d'universités...

Depuis plusieurs mois, les attaques spectaculaires se multiplient et le débat s'enflamme. Plus que jamais, **la cybersécurité est au cœur des enjeux de souveraineté et de résilience des États**, avec une dimension économique, stratégique et politique qui va bien au-delà de la seule sécurité de l'ensemble de leurs systèmes d'information.

« Comme nos vies, qu'elles soient professionnelles, privées et même citoyennes, sont de plus en plus numériques, il s'agit avant tout d'être en cybersécurité au quotidien, souligne Vincent Cachard, responsable du programme Cybersécurité à la Direction de la recherche technologique du CEA. Plus qu'un domaine d'activité, la cybersécurité est donc avant tout un état à maintenir ».

Car si la nature des menaces reste la même qu'hier, c'est la fréquence et la complexité des attaques qui les rendent aujourd'hui plus prégnantes et préoccupantes.

« Le château fort n'existe pas, résume Philippe Mazabraud, directeur du programme transversal Sécurité globale à la Direction des applications militaires du CEA. La question n'est pas tant de savoir si nous serons attaqués mais quand cela se produira, comment s'y préparer et y répondre de façon à être les plus résilients possibles, dans un scénario central où nous ferions face à une augmentation massive d'ici 2030 des attaques dites hybrides ».

Cette accélération est par ailleurs nourrie par les progrès constants du numérique, notamment dans les domaines de l'IA et du quantique, et portée d'une part par des réseaux cybercriminels de plus en plus professionnels, d'autre part par les tensions géopolitiques mondiales actuelles qui déplacent les zones de conflit y compris dans le cyberspace.

L'impératif de la cybersécurité

Dès lors, comment s'organiser pour y faire face ? *« Pour renforcer le potentiel de défense, nous*

*jouons principalement sur deux tableaux, rappelle Vincent Cachard. D'une part, le CEA développe des outils pour mieux identifier les vulnérabilités des infrastructures critiques, de leurs composants et de leurs systèmes, d'autre part, il met au point les technologies permettant de les rendre plus robustes et résilients face aux nouveaux risques et aux nouvelles menaces ». **C'est précisément le champ d'action du CEA qui a fait de la cybersécurité un impératif, à la fois pour protéger ses activités dans des secteurs sensibles comme les énergies, la santé et la défense, et pour accompagner les industriels face aux risques et menaces.***

« Nous disposons d'une expertise en cyberdéfense développée depuis plus de 25 ans pour nos missions au service de la Défense nationale, souligne Philippe Mazabraud. Et de plateformes technologiques à l'état de l'art en cybersécurité permettant de développer et de tester des réponses innovantes aux défis de sécurisation du matériel, des logiciels et des données. L'ensemble fait du CEA un acteur de confiance reconnu tant en France qu'en Europe et capable de construire des écosystèmes réunissant les acteurs majeurs de la cyber ».

Pour renforcer sa « force de frappe », le CEA a regroupé dès 2019 ses activités de recherche et développement en cybersécurité dans un grand programme transversal qui mobilise aujourd'hui près de 200 ingénieurs-chercheurs répartis dans une quinzaine d'équipes. Celles-ci travaillent en lien étroit avec les services de l'État, notamment la Direction générale de l'armement et l'Agence nationale de la sécurité des systèmes d'information (Anssi), mais également en collaboration avec les acteurs académiques du domaine (CNRS, Inria, Mines-Telecom, universités...) ainsi qu'avec de nombreux industriels : opérateurs (EDF, IN Groupe), fournisseurs de composants logiciels ou électroniques (STMicroelectronics, Soitec, Sopra Steria), équipementiers (comme Schneider Electric) ou encore systémiers (Thalès, Naval Group, Airbus).

Une expertise au service de la confiance numérique

Comment se décline concrètement ce programme ? Il s'appuie sur les diverses expertises du CEA appliquées à la sécurité, notamment autour : de l'évaluation de composants, d'équipements et de systèmes dans le cadre du Centre d'évaluation des technologies de l'information (Cesti) qu'héberge le CEA depuis plus de 25 ans sous l'égide de l'Anssi, du développement d'outils à base de méthodes dites formelles pour garantir l'absence de défauts logiciels susceptibles de générer une erreur lors de l'exécution d'un programme informatique ou permettre des actions malveillantes comme Frama-C pour le code source, Binsec pour le code binaire ou Pyrat pour l'IA ; de la sécurisation des composants électroniques ou des systèmes dès leur conception (Secure by technology), ou enfin grâce à des approches innovantes en réponse aux défis des technologies quantiques, de la confiance décentralisée avec le simulateur MAX ou encore de la supervision/détection/réaction intelligente des réseaux avec SIGMO-IDS ou Adviz. *« La confiance numérique est un pilier central, conclut Philippe Mazabraud. Dans le domaine civil bien sûr mais plus encore dans celui de la défense où la maîtrise des systèmes d'information est au cœur de ce qu'on appelle la guerre hybride ».*

L'ensemble des recherches du CEA se nourrissent et s'inscrivent dans le cadre de la réglementation européenne, et de ses déclinaisons nationales, pour limiter les vulnérabilités des systèmes numériques : après le Cybersecurity Act en 2019, la directive NIS2 sur la sécurité des réseaux et des systèmes d'information en 2022, le Cyber Resilience Act (CRA), qui entre en vigueur au début de l'année prochaine, vise à aller encore plus loin dans la sécurisation du marché numérique européen.

« La régulation est une nécessité pour se protéger des acteurs malveillants, note Vincent Cachard.

Le CRA introduit ainsi des exigences de sécurité obligatoires pour les fabricants, importateurs et distributeurs de produits matériels et logiciels, avec des impératifs de surveillance, de transparence et de mise à jour tout au long du cycle de vie des produits que nous devons intégrer dans nos travaux ».

Structurer et animer la filière cyber

Des travaux et des compétences qui permettent au CEA de jouer un rôle de premier plan dans la structuration et l'animation des filières cybersécurité en France et en Europe qu'il irrigue par ses transferts de technologie et la création de plusieurs start-up.

Au niveau national, dans le cadre du programme France 2030, le CEA s'est ainsi vu confier la responsabilité du copilotage du programme de recherche de la stratégie nationale pour la cybersécurité et le copilotage de tous les PEPR sur les technologies numériques. Membre fondateur du Campus Cyber à Paris et membre de l'Alliance pour la confiance numérique, il a récemment intégré le pôle d'excellence cyber (PEC) créé sous l'égide du ministère des Armées et de la Région Bretagne.

Depuis 2024, il copilote le projet structurant « Innovation et technologies clés » du Comité stratégique de la filière des industries de sécurité, qui vise à élaborer une feuille de route en vue d'assurer la maîtrise des technologies-clés d'avenir et des technologies critiques. Enfin, avec l'agence de programme Asic, le CEA travaille à lancer un programme national sur l'évaluation sécuritaire regroupant l'ensemble de la filière. Et en Europe, où il est partie prenante de différents projets d'ampleur, le CEA a activement participé à la création de l'European Cyber Security Organisation (ECSO), qui fédère aujourd'hui plus de 300 acteurs à travers 28 pays dans l'objectif de renforcer les communautés et capacités en matière de recherche, de technologie et de politique industrielle en cybersécurité au niveau de l'Union européenne.

Et demain ? « *Il nous faut continuer à amplifier la dynamique mise en place pour assurer un continuum de sécurité sur l'ensemble de la chaîne numérique* », expliquent Philippe Mazabraud et Vincent Cachard. Un véritable défi à l'heure de l'IA et du quantique.

Evaluer des dispositifs à haut niveau de sécurité

Le Centre d'évaluation de la sécurité des technologies de l'information (Cesti) du CEA-Leti est un laboratoire d'évaluation sécuritaire agréé par l'Agence nationale de la sécurité des systèmes d'information (Anssi) depuis 2000 et accrédité par le Cofrac. Dans ce cadre, il conduit des évaluations de composants sécurisés, d'équipements matériels avec boîtier sécurisé et de systèmes, selon les Critères Communs*, jusqu'au niveau EAL7. Il est également habilité à réaliser des évaluations en vue de certifications CSPN**.

Premier Cesti à recevoir l'agrément de l'Anssi pour évaluer des composants ou systèmes utilisant la cryptographie post-quantique, celui du CEA dispose de compétences spécialisées dans les domaines des semiconducteurs, de l'électronique, de la cryptographie et des technologies de l'information. Il conçoit et développe également ses propres moyens de test et d'attaque, matériels et logiciels. Il bénéficie aussi des expertises des plateformes technologiques du CEA-Leti ainsi que d'une compétence unique du CEA-List en outils logiciels d'analyse de la sécurité à base de méthodes formelles tels FRAMA-C. La combinaison de ces moyens expérimentaux et de ces compétences spécialisées contribue au maintien de son haut niveau d'expertise au service des secteurs de la Défense, de la banque, de l'identité numérique, de l'automobile, et de l'énergie.

* Les Critères Communs (Common Criteria) sont un standard international d'évaluation de la sécurité des produits et systèmes des technologies de l'information.

** La Certification de sécurité de premier niveau (CSPN) est délivrée par l'Anssi pour différents types de produits, notamment logiciels et matériels. Alternative aux évaluations Critères Communs, elle vise à établir un premier niveau de robustesse du produit.

<https://www.cea.fr/presse/Pages/actualites-communiques/ntic/cybersecurite-defi-siecle.aspx>