PREMIER
MINISTRE

Liberté
Égalité
Fraternité

Stratégie nationale de cybersécurité

*
* *

Rapporteur : IGA Bruno MARESCAUX

Secrétaire : M. Jonathan COLLAS

PREMIER MINISTRE
Liberté
Égalité
Fraternité

SOMMAIRE

PREMIER
MINISTRE
Liberté
Égalité
Fraternité

RESUME EXECUTIF

[TODO : une fois la stratégie validée en IM]

PREMIER MINISTRE
Liberté
Égalité
Fraternité

POURQUOI UNE NOUVELLE STRATEGIE NATIONALE DE CYBERSECURITE ?

L'évolution de l'environnement stratégique

L'avènement de l'ère numérique a profondément bouleversé les fondements de notre société, tissant une toile complexe d'interconnexions ainsi qu'une dépendance accrue à des infrastructures critiques dématérialisées, exposant ainsi des versants entiers de notre vie quotidienne et de notre économie à des cybermenaces d'une sophistication croissante.

Miroir des tensions géopolitiques et des compétitions internationales, le cyberespace est devenu un espace de compétition, de contestation et d'affrontement permanent et désinhibé.

La France est confrontée, comme ses partenaires internationaux, à une menace de cyberattaques[1] **particulièrement intense** et étendue à tous les pans de la société – qu'elles émanent d'Etats, de cybercriminels, d'activistes ou soient le résultat d'une prolifération non maitrisée de capacités commerciales d'intrusion.

Qu'elles soient motivées par des considérations économiques, politiques, militaires ou idéologiques, **ces menaces peuvent causer des dommages considérables**, perturbant le fonctionnement de nos sociétés, menaçant notre sécurité nationale. Ces attaques peuvent également avoir des répercussions économiques importantes, entraînant des pertes financières considérables et perturbant les chaînes d'approvisionnement.

Ces pressions s'exercent aussi sur des technologies critiques, piliers de notre économie et de notre défense, et accentuent les enjeux entourant la sécurité de nos données. En premier lieu, le cloud, qui concentre nos données les plus sensibles, soulève des questions majeures de protection. L'essor des systèmes d'intelligence artificielle, bien que prometteur, amplifie ce risque en concentrant les données sur des cibles de grande valeur dont l'exploitation n'est pas encore parfaitement maîtrisée.

*

La consolidation de la vision française

Face à ces défis majeurs, la France s'est engagée à résolument renforcer sa posture de cybersécurité. Ce domaine est, depuis plusieurs années, une des priorités nationales, et bénéficie d'un soutien et d'une coordination de la part des plus hautes autorités.

Depuis plus d'une dizaine d'années, la vision française de la cybersécurité s'est consolidée à force d'itérations stratégiques qui ont permis à la France de se doter d'une culture forte en la matière et d'élever progressivement son niveau de cybersécurité.

Les premières stratégies publiées en 2011[2] **et 2015**[3] **ont permis d'apporter une première réponse concrète pour mieux protéger la France contre les cyberattaques**. Dans le

[1] Panorama de la cybermenace 2023, ANSSI | lien
[2] Défense et sécurité des systèmes d'information : Stratégie de la France (2011) | lien
[3] Stratégie nationale pour la sécurité du numérique (2015) | lien

prolongement, la *Revue stratégique de cyberdéfense*[4] de 2018 a posé les bases d'un modèle national, solide et reconnu à l'international, séparant les missions offensives et défensives.

En 2021, l'Etat a de nouveau renforcé sa posture en consacrant un milliard d'euros dans le cadre de la *Stratégie nationale d'accélération pour la cybersécurité*[5] dans le cadre du plan d'investissement *FRANCE 2030*.

Cette dynamique permet à la France de disposer aujourd'hui dans le domaine cyber d'une ressource humaine qualifiée, de capacités de recherche de premier plan, d'une industrie de pointe, d'acteurs publics et privés collectivement engagés dans la cyber protection de la Nation, et de capacités défensives et offensives lui permettant d'assurer la préservation de ses intérêts et sa place dans l'ordre international.

Dans un contexte stratégique en constante mutation, la Revue nationale stratégique (RNS)[6] a fixé pour la France l'ambition d'une **résilience cyber de premier rang**.

La présente stratégie reprend cette ambition en développant une approche structurée autour de quatre piliers :

- **PILIER 1 | DEVELOPPER UNE CYBER-RESILIENCE COLLECTIVE**
- **PILIER 2 | INVESTIR DANS**
- **PILIER 3 | BATIR UNE CYBERDEFENSE OPERATIONNELLE**
- **PILIER 4 | S'AFFIRMER A L'INTERNATIONAL COMME UNE PUISSANCE CYBER RESPONSABLE, COOPERATIVE ET SOLIDAIRE**

*

* *

Déclinée en 12 objectifs stratégiques, cette stratégie définit 45 actions structurantes pour faire de la France UNE NATION CYBER DE PREMIER RANG.

[4] Revue stratégique de cyberdéfense (2018) | lien
[5] Cybersécurité : renforcement par le Gouvernement de la protection des citoyens, des administrations et des entreprises | lien
[6] Revue nationale stratégique, présentée le mercredi 9 novembre 2022 par le Président de la République | lien

PILIER 1 | DEVELOPPER UNE CYBER-RESILIENCE COLLECTIVE

> *Mettre en réseau les citoyens, les collectivités territoriales, les entreprises, les administrations, les acteurs de la recherche et de la société civile pour élever le niveau de résilience de la Nation.*

*

Depuis le Livre blanc sur la défense et la sécurité nationale de 2008, la résilience se définit comme la volonté et la capacité d'un pays, de la société et des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeures, puis à rétablir rapidement leur capacité de fonctionner normalement, ou à tout le moins dans un mode socialement acceptable. Elle concerne non seulement les pouvoirs publics, mais aussi les acteurs économiques et la société civile tout entière.

La nature des crises cyber susceptibles d'affecter la France dans les prochaines années appelle au développement d'une cyber-résilience collective de premier rang.

Au service de cette ambition, les talents constituent les atouts les plus stratégiques pour la Nation. Toutes les stratégies les mieux pensées n'étant rien sans les femmes et les hommes qui les mettent en œuvre, la France doit continuer de s'employer à disposer d'un large vivier de compétences en cybersécurité.

L'état de cyber-résilience collective de la Nation requiert ensuite le **développement d'une conscience collective du risque** cyber, qui impliquera de renforcer la **sensibilisation** de nos concitoyens dans le même temps que sera développée la **préparation** du tissu économique et social à répondre à des situations de crise à la suite d'une cyber attaque de grande envergure.

La cyber résilience collective reposera sur **une approche proportionnée,** dans laquelle les services et infrastructures les plus vitaux de la Nation, à commencer par ceux de l'Etat, seront portés à un niveau de sécurité très élevé, apte à résister aux menaces les plus avancées, dans le même temps que l'ensemble des entreprises, collectivités et associations, qui constituent le reste du tissu économique et social, seront incitées à élever leur niveau de sécurité à un niveau suffisant pour résister à des attaques de nature criminelle.

Pour rendre la cybersécurité plus accessible, un important effort sera consenti pour **simplifier** le cadre normatif, **accompagner** la montée en maturité cyber de l'ensemble des acteurs publics et privés, et **faciliter** le parcours d'assistance des victimes.

Objectif stratégique 1. Faire de la France le plus grand vivier de talents cyber d'Europe

Le rang de la France dans le cyber espace dépend en tout premier lieu de sa capacité à pouvoir s'appuyer sur une génération de femmes et d'hommes compétents et motivés.

Or, le secteur du numérique en général, et celui du cyber en particulier, connaissent des phénomènes de pénuries, accentués par les différentes sous-représentations sociales ou de genres, ce malgré le fait qu'ils connaissent une croissance importante et continue depuis plusieurs années, créant au passage de nombreux emplois qualifiés et rémunérateurs.

Au surplus, **les besoins en matière de cybersécurité augmentent plus rapidement que la capacité de l'écosystème à former** dans ce domaine, en raison d'un manque d'attractivité du secteur. Et toutes les projections disponibles indiquent que les tensions sur les métiers du numérique ne cesseront pas sans une politique **de ressources humaines ambitieuse et attractive, cohérente** vis-à-vis des métiers exercés dans le domaine cyber et des compétences nécessaires à leur exercice.

La **France doit continuer d'investir massivement dans les compétences nécessaires à l'exercice des métiers cybersécurité**[7], et ce en cohérence avec celles plus générales des différents domaines du numérique (logiciel, système, réseaux et télécommunications, etc.).

En association étroite avec le secteur privé, l'Etat déploiera donc une politique ambitieuse de ressources humaines qui visera à **faire de la France le plus grand vivier de talents cyber d'Europe.**

En plus de l'impact positif sur la posture de cybersécurité nationale et sur celle de l'Europe, cette ambition servira les objectifs plus globaux relatifs à la stimulation de la croissance économique et de l'innovation, ou encore à l'amélioration de l'inclusion sociale et de l'égalité des chances.

[7] Panorama des métiers de la cybersécurité | ANSSI | Lien

Action structurante 1. Développer, dès le plus jeune âge, une culture positive et inclusive de la cybersécurité

La jeunesse, identifiée par la Revue nationale stratégique de 2022 comme le "socle de la résilience collective" du pays, représente un vivier de talents potentiels pour la cybersécurité. Or, des préjugés tenaces - métier solitaire, exclusivement technique, réservé aux hommes et conditionné par des études supérieures - freinent l'accès à ce domaine porteur. Face à ce constat, la France déploie une stratégie ambitieuse pour briser ces barrières et ouvrir la voie à une nouvelle génération de cyber-experts.

Au cœur de cette stratégie, une campagne nationale visant à promouvoir l'inclusion sociale, la mixité et l'égalité des chances dans le domaine de la cybersécurité. L'objectif est de rendre accessible à tous, dans tous les territoires, les compétences et les opportunités offertes par ce secteur en pleine expansion.

La première étape consiste à démystifier la cybersécurité et à la rendre accessible dès le plus jeune âge. Pour cela, le ministère de l'Éducation nationale, de la Jeunesse et des Sports (MENJS), en collaboration avec les acteurs spécialisés de l'État, multiplie les initiatives. Intégration des compétences cyber dans le service public d'évaluation des compétences numériques PIX, interventions et conférences "parents-enfants" dans les écoles primaires par des acteurs territoriaux de la cybersécurité, sont des exemples d'actions à démultiplier pour sensibiliser les enfants et leur entourage aux enjeux de la sécurité informatique. Des enseignements d'exploration consacrés au cyber seront ainsi mis en place dans les collèges et lycées.

Des efforts seront entrepris pour **prolonger cet effort dans le champ culturel** (audiovisuel, cinématographique, littéraire,…) afin de présenter le domaine cyber au grand public sous un angle rompant avec des représentations stéréotypées du secteur.

L'accès à la formation en cybersécurité doit être facilité pour tous, en particulier pour les jeunes issus de milieux défavorisés. Des dispositifs d'aide financière spécifiques, tels que des bourses de pré-recrutement conditionnées par un engagement de service public, permettront de lever les obstacles financiers et d'attirer des talents prometteurs.

La sous-représentation des femmes dans les métiers de la cybersécurité et du numérique en général constitue un frein majeur à la diversification des talents. D'après l'observatoire des métiers de la cybersécurité, lancé par l'ANSSI en 2021, le domaine de la cybersécurité compte seulement autour de 10 % de femmes[8]. Pour augmenter de la représentation des femmes dans la cybersécurité, un programme de mentorat dédié sera mis en place, à l'image des « cadette de la cyber » du Pôle d'Excellence Cyber, permettant aux femmes de bénéficier de l'accompagnement et des conseils de professionnels expérimentés afin de développer leur carrière et briser ce « plafond de verre ».

L'attractivité des métiers de la cybersécurité passe également par l'enrichissement des ressources pédagogiques et le développement d'outils d'apprentissage innovants. Le programme CyberEnJeux, développé par l'ANSSI, le MENJS et le Campus Cyber, constitue un exemple concret de cette démarche. Des initiatives similaires seront encouragées pour rendre l'apprentissage de la cybersécurité ludique, stimulant et accessible à tous.

[8] L'attractivité et la représentation des métiers de la cybersécurité, enquête 2023 de l'Observatoire des métiers de la cybersécurité (ANSSI) | ici

Action structurante 2. Mobiliser les leviers de l'engagement civique

Les dispositifs d'engagement civique offrent des leviers adaptés pour susciter l'engagement des jeunes **dans le domaine de la cybersécurité.**

Pour rassembler les citoyens les plus jeunes autour des enjeux variés de la cybersécurité (géopolitiques, juridiques, techniques, etc.), et ainsi **développer une génération de talents mobilisée et compétente au service d'une société numérique plus sûre et plus résiliente**, l'Etat fera évoluer les dispositifs d'engagement civique afin **d'y renforcer la place de la cybersécurité.**

Au premier chef, le Service Civique et le Service National Universel (SNU) représentent deux vecteurs de sensibilisation des jeunes citoyens, mais aussi des leviers pour les inciter à s'engager concrètement dans la protection de notre espace numérique.

D'un côté, le Service Civique constitue une opportunité d'engagement citoyen et de découverte des métiers de la cybersécurité. Il permet aux jeunes de s'engager volontairement au service de l'intérêt général pendant une durée de 6 à 12 mois. Afin de renforcer l'attractivité des métiers de la cybersécurité, il est nécessaire d'inciter la multiplication de mission au caractère cyber.

De l'autre, le SNU doit être vu comme un tremplin pour sensibiliser les jeunes aux enjeux de la cybersécurité. Il vise à renforcer à grande échelle les valeurs de la République, développer le sens du devoir, favoriser le vivre-ensemble et préparer les jeunes à leur future vie de citoyen. Ce dispositif offre un cadre idéal pour attirer l'attention des plus jeunes citoyens sur un domaine crucial pour la sécurité nationale. Décliner une verticale cybersécurité du SNU permettra d'encourager les jeunes populations à s'engager sur les questions de cybersécurité.

Par ailleurs, d'autres programmes d'engagement civique, comme les *Cadets de la Gendarmerie*, représentent un vivier de talents potentiels et une opportunité de sensibiliser la jeunesse à l'importance de la protection du cyberespace. Ces programmes, en offrant aux jeunes une immersion dans le quotidien des métiers de la sécurité et la participation citoyenne, constituent également une opportunité pour susciter des vocations dans le domaine de la cybersécurité. La France fera effort pour inclure, dans ces programmes, des modules spécifiques sur la cybersécurité, permettant aux jeunes de découvrir les métiers de ce domaine.

Enfin, l'engagement des jeunes ne doit pas s'arrêter au terme de leur participation à ces dispositifs de sensibilisation à la cybersécurité. Pour pérenniser cet engagement et capitaliser sur les talents et les compétences acquis, il sera créé des passerelles vers les différentes réserves citoyennes et opérationnelles de cyberdéfense. Il s'agira de faciliter l'accès des jeunes ayant participé à des dispositifs d'engagement civique à ces réserves, en valorisant leur expérience et leurs compétences acquises.

Action structurante 3. Investir dans tous les pans de la formation

Pour garantir une orientation professionnelle juste et ouvrir ainsi les étudiants à de nouvelles perspectives d'évolution professionnelles, des efforts seront consentis pour faciliter la compréhension des liens entre les différents types de métiers, les compétences requises et les formations disponibles.

En première ligne, les relais de l'orientation scolaire et professionnelle **joueront un rôle crucial dans ce domaine** en fournissant des conseils et des informations aux élèves et demandeurs d'emploi sur les différentes voies d'accès aux métiers de la cybersécurité.

Pour offrir à ces publics des repères stables et communiquer avec un langage commun sur les compétences nécessaires à l'exercice des métiers du domaine cyber**, la France créera une plateforme nationale pour l'orientation vers les métiers de la cybersécurité.** Cette plateforme appuiera les actions entreprises conjointement par le ministère de l'Éducation nationale et de la Jeunesse et le Campus Cyber, à travers la campagne nationale DemainSpécialisteCyber, pour faire connaître et valoriser la cybersécurité et ses métiers auprès des collégiens et lycéens. Il s'agira notamment de faire converger les efforts entre cette initiative et le projet « TalCyb – Talents Cyber » porté par le Campus Cyber. Cette plateforme sera référencée sur le portail de la cybersécurité.

Les métiers de la cybersécurité sont en constante évolution, nécessitant une mise à jour régulière des compétences et des connaissances. La formation continue permet aux professionnels de se maintenir à la pointe des dernières techniques et outils de protection et de défense contre les cybermenaces, et de développer de nouvelles compétences adaptées aux besoins émergents.

La France soutiendra le développement de la formation continue des professionnels de la cybersécurité pour leur permettre de se maintenir à jour sur les dernières technologies et menaces, ou encore attirer de nouveaux professionnels dans une logique de parcours professionnel. Ce projet doit répondre à un enjeu de reconnaissance de la qualité de la formation. Il doit également permettre de d'orienter vers le domaine cyber un nombre accru de professionnels en reconversion, via des leviers comme le compte personnel de formation (CPF) et en favorisant et en soutenant les initiatives régionales s'appuyant sur des organismes ou associations locales.

Pour toucher l'ensemble du tissu social, il sera également entrepris de **créer les conditions propices à l'auto-formation** aux enjeux de sécurité numérique. Les initiatives telles que le MOOC de sensibilisation SecNumAcadémie de l'ANSSI, visant à présenter des mesures simples et des bonnes pratiques, constituent un levier important pour élever le niveau de maturité cyber dans la société. Cette offre d'auto-formation sera renforcée et mise en visibilité sur le portail national de la cybersécurité.

Enfin, l'industrie technologique est en pleine effervescence, marquée par des tendances majeures telles que l'intelligence artificielle (IA), l'informatique quantique, l'Internet des objets (IoT) et la 6G. La cybersécurité s'inscrit pleinement dans cette dynamique et trouve de nouvelles opportunités de développement dans chacun de ces nouveaux domaines.

La convergence entre la cybersécurité et d'autres disciplines ouvre de nouveaux horizons pour l'innovation. Loin de diminuer l'attractivité du domaine, ces tendances en font un champ d'exploration passionnant pour les chercheurs, les étudiants et les professionnels. Les pôles

d'excellence français en matière de formation, de recherche et d'innovation en cybersécurité sont idéalement placés pour tirer parti de ces synergies.

Pour pérenniser la place centrale de la cybersécurité dans le paysage scientifique français, il est essentiel de mettre en place des "stratégies passerelles" entre les différentes disciplines. Ces passerelles permettront de favoriser les échanges, la collaboration et la fertilisation croisée des idées, renforçant ainsi globalement la position de la France dans ce domaine stratégique. La France doit continuer de soutenir financièrement des programmes de nature interdisciplinaires au sein des différents pôles académiques traitant de technologies, en y intégrant une dimension cybersécurité.

Action structurante 4. Augmenter l'attractivité des services de l'Etat

L'Etat offre dans le domaine de la cybersécurité et de la cyberdéfense la possibilité d'exercer des missions parfois singulières mais toujours variées, et porteuses de sens. Les femmes et les hommes qui, animés par des valeurs communes, choisissent dans ce cadre de mettre leurs compétences au service de l'intérêt général, participent très directement à la résilience cyber et à la souveraineté numérique de la Nation.

Dans un contexte de concurrence aigue pour les compétences clés du domaine, l'Etat mettra en œuvre dans le domaine cyber une politique ambitieuse en matière de ressources humaines, qui visera à :

- **mieux attirer les jeunes en quête d'un premier emploi dans le secteur**. L'État renforcera ses partenariats avec les écoles et mobilisera encore plus systématiquement les mêmes outils que les entreprises du secteur privé : stages, formations en alternance, bourses, promesses d'embauche ;
- **faciliter les parcours professionnels et inciter aux mobilités interministérielles**, ce qui suppose de créer de nouvelles formes de progression qui ne soient pas réservées aux seuls titulaires et aux profils managers, mais aussi au bénéfice des profils experts et des contractuels ;
- **développer une cartographie complète des compétences nécessaires à la cybersécurité,** en tenant compte des besoins évolutifs des différents services employeurs de compétences cyber au sein de l'Etat ;
- **mettre en place des programmes de formation et de développement professionnel sur mesure pour les agents publics évoluant dans le domaine de la cybersécurité**, en s'appuyant sur les dernières innovations technologiques et les meilleures pratiques internationales.

Cependant, une coordination accrue est nécessaire afin d'unifier les efforts produits sur ces différents axes par les services employeurs de compétences cyber au sein de l'Etat. Pour mettre en œuvre cette approche globale en capitalisant sur les investissements déjà consentis, **la compétence de la DINUM, en qualité de direction des ressources humaines interministérielle dans le domaine numérique, sera étendue à la dimension cyber.**

Chargée **d'animer et de fédérer le collectif des employeurs cyber de l'Etat**, elle veillera notamment à augmenter la capacité d'impact de l'Etat recruteur dans la relation avec les écoles et les universités, à piloter des parcours multi-employeurs, à apporter du conseil-mobilité aux agents et à gérer des viviers. La DINUM s'appuiera sur l'ANSSI pour exercer ces prérogatives nouvelles.

Action structurante 5. Etendre cette dynamique sur les ressources humaines au niveau européen

L'Europe s'est dotée d'une stratégie ambitieuse pour renforcer ses capacités en cybersécurité et s'imposer comme un leader mondial en la matière. Au cœur de cette stratégie, la mobilisation des ressources humaines est un enjeu prioritaire.

C'est dans ce contexte que l'Union européenne (UE) déploie une dynamique collective visant à harmoniser les standards, développer les compétences et favoriser la coopération entre les États membres.

L'Agence européenne pour la cybersécurité (ENISA) et le centre de compétences cyber européen (ECCC)[9] jouent un rôle central dans cette coordination.

L'ambition de la France pour l'UE est de doter le continent d'une main-d'œuvre de classe mondiale en cybersécurité. Au service de cette ambition, la France soutiendra :

- **l'émergence d'un socle commun de compétences au niveau européen :** l'harmonisation des standards et la définition de qualifications communes permettront de garantir un niveau de compétences homogène dans tous les États membres.
- **la mise en place des qualifications de formation cyber au niveau européen** : la création de cursus harmonisés facilitera la mobilité des professionnels du secteur et favorisera l'échange de bonnes pratiques.
- **l'organisation de parcours croisés entre autorités nationales de cybersécurité des États-membres** : les échanges d'expériences entre professionnels de différents pays permettront de mutualiser les connaissances et de renforcer la collaboration transfrontalière.
- **La multiplication des détachements des agents publics français au sein des agences et institutions européennes** : la mobilité des agents publics contribuera à diffuser l'expertise française et à renforcer la coopération internationale.

Cette politique publique concourt également à la construction d'une identité européenne commune en cybersécurité, et de manière indirecte, au renforcement de la réputation de l'Europe en tant que continent innovant et sûr.

[9] European Cybersecurity Competence Centre | lien

Objectif stratégique 2. Une Nation sensibilisée et préparée aux crises cyber

L'état de cyber-résilience collective de la Nation repose :

- sur le développement et le maintien dans la durée d'une conscience collective des risques que font poser sur la Nation les menaces cyber de toute nature, des plus crapuleuses aux plus stratégiques. Cet objectif repose sur un impératif de sensibilisation croissante de nos concitoyens aux questions de cybersécurité et de cyberdéfense ;
- sur la préparation du tissu économique et social à répondre à des situations dans lesquelles pourraient être mis en cause, à la suite d'une attaque perpétrée dans le cyberespace, la vie de la population ou le fonctionnement régulier de la vie économique, sociale ou institutionnelle du pays.

Il suppose le développement d'une synergie renforcée, à l'échelle territoriale, nationale et internationale, entre une population imprégnée de l'esprit de défense, des acteurs publics rompus à la planification et à la gestion de crise et l'ensemble du tissu économique et social.

Action structurante 6. Sensibilisation et prévention : faire de chaque citoyen un maillon de la chaîne de résilience numérique de la Nation

A l'instar des gestes barrières qui protègent notre santé, la prévention est essentielle pour faire du citoyen le premier maillon de la chaîne de résilience numérique de la Nation.

Une sensibilisation large et réussie de la Nation repose sur notre capacité à diversifier les moyens pour toucher le plus grand nombre, développer une conscience partagée des menaces et des risques, diffuser largement les bonnes pratiques et les bons réflexes. De nombreuses initiatives ont été lancées ce sens ces dernières années. Ces actions apparaissent cependant souvent dispersées, ce qui les rend difficilement lisibles, et peu évaluées.

La France mettra donc en œuvre une politique ambitieuse de sensibilisation et de prévention cyber.

Cette politique sera d'abord tournée vers les plus jeunes. Cet effort passera en premier lieu par une étroite collaboration avec le ministère de l'Education Nationale. Des modules de cybersécurité seront également intégrés dans toutes les formations d'enseignement supérieur (écoles d'ingénieurs, universités, etc.), y compris dans des parcours où le domaine d'enseignement n'est pas le numérique.

Cette politique sera ensuite tournée vers le tissu économique et social. Elle verra l'Etat adopter une posture d'exemplarité grâce à la mise en place d'une formation obligatoire à la cybersécurité pour tous les agents de la fonction publique, sur le modèle des formations à la transition écologique. L'Etat soutiendra la production d'un kit du type « Fresque du climat » à usage de ses propres services, des entreprises et des collectivités.

Elle sera enfin orientée vers le grand public. L'Etat veillera à promouvoir un meilleur niveau de transparence pour que les enjeux cyber puissent être mieux appréhendés dans le débat public, ce qui nécessitera un effort d'explication et de démystification tourné vers les relais d'opinion afin de leur donner les clés de compréhension utiles, par exemple à la suite de cyber attaques d'ampleur observées au niveau international.

L'Etat veillera par ailleurs, à l'instar de ce qui est pratiqué dans le domaine de la sécurité routière, à faire émerger **une marque nationale de prévention du risque numérique, connue du grand public**, en capitalisant sur le modèle du *cybermoi/s* européen. Le développement de cette marque sera confié au groupement d'intérêt public Action contre la cybermalveillance (GIP ACYMA), qui deviendra ainsi le maitre d'œuvre d'un programme ambitieux de prévention nationale en matière de cybersécurité.

Action structurante 7. Se préparer pour faire face : éprouver régulièrement le niveau de résilience numérique de la Nation

La France doit se préparer à des attaques cyber massives d'une ampleur qu'elle n'a jamais connue, et être capable d'y faire face le cas échéant en démontrant une pleine capacité à encaisser un tel choc, à continuer à assurer le bon fonctionnement de la Nation, fut-ce en mode dégradé, et à revenir le plus rapidement possible à un fonctionnement normal. Les cyber attaques perpétrées depuis 2014 contre les infrastructures critiques en Ukraine illustrent le type d'agressions face auxquelles la France doit être capable de démontrer un niveau de résilience cyber éprouvé.

Pour atteindre cette ambition, la France renforcera **sa préparation et sa capacité de réaction face** à une cyber attaque massive à l'origine d'une crise systémique. D'une part, elle consolidera sa **planification de gestion de crise**, afin d'être capable d'en traiter tant les causes que les effets. Elle veillera notamment à la généralisation des plans de continuité et de reprise d'activité en cas de crise. D'autre part, elle organisera une **mise en tension permanente des capacités de réaction** de la Nation à travers la diffusion d'une **culture de l'entrainement cyber accessible à tous**, permettant de préparer l'ensemble du tissu économique et social.

Cette stratégie se déclinera au niveau territorial, sectoriel, national et international. Elle visera à mobiliser plus fortement les professionnels du numérique au côté des professionnels de la cybersécurité et de la gestion de crise.

S'agissant de la planification de gestion de crise, le risque cyber sera pris en compte au niveau territorial dans les plans de prévention des risques technologiques (PPRT) et les plans communaux de sauvegarde (PCS), en particulier sur les volets de la continuité d'activité et de la reprise d'activité.

Au niveau sectoriel, les relais sectoriels de l'ANSSI dans chaque secteur professionnel entretiendront une dynamique visant tant le renforcement de la résilience opérationnelle des organisations que la résilience du secteur pris dans son ensemble. Cet objectif nécessitera de considérer l'ensemble de la chaîne de valeur sectorielle pour en identifier les dépendances les plus critiques.

Au niveau national, l'Etat poursuivra le déploiement du plan PIRANET maintenu par le SGDSN en veillant à la bonne articulation entre les capacités publiques et privées. Afin de prévenir tout risque de dépassement des capacités nationales de réponse, il planifiera, tant d'un point de vue opérationnel que juridique, le recours à des capacités complémentaires à celles disponibles au son sein, que celles-ci relèvent d'opérateurs privés ou de partenaires internationaux, notamment au titre de la solidarité entre les États membres de l'Union européenne ou du mécanisme d'assistance en vigueur au sein de l'OTAN.

S'agissant de l'entrainement à la gestion de crise, la politique mise en œuvre au sein de l'Etat a montré les effets positifs des exercices pour soutenir la préparation et diffuser une culture de la gestion de crise cyber. Un programme ambitieux d'exercice de crise cyber sera développé afin d'éprouver l'articulation et l'efficience de l'ensemble des capacités de réponse de l'Etat à Ce programme inclura des exercices cyber dédiés d'une part, et l'intégration systématique d'un volet cyber dans tous les autres exercices d'ampleur d'autre part.

Les premières expérimentations à l'échelle sectorielle ou massifiées ont permis d'initier la sensibilisation des acteurs aux enjeux et conséquences des crises d'origine cyber. Elles ont

démontré un véritable bénéfice pour les organisations participantes. Cette approche sera étendue à l'ensemble du territoire et du tissu économique et social.

A l'instar des exercices de réaction à une alerte incendie, **l'Etat soutiendra l'organisation, dans chaque entreprise, collectivité ou association, d'un exercice annuel** permettant aux plus grand nombre de citoyen d'être mis en contact avec les effets simulés d'une cyberattaque et de recevoir une acculturation ou un rappel de la conduite à tenir en cas de crise. Dans certain cas, cet exercice pourra prendre la forme d'une « journée sans numérique », mettant en relief les dépendances vis-à-vis du numérique et les éventuelles lacunes en matière de continuité d'activité et de résilience. A l'appui de cette ambition visant à inciter la participation de tous à des exercices de crise, l'Etat soutiendra la mise à disposition de communs de la gestion de crise à partir de ses ressources propres et de celles des communautés sectorielles.

Enfin, la France participera activement à des exercices avec ses partenaires internationaux afin de pouvoir organiser avec eux une réponse coordonnée aux crises. La France dispose d'une expertise reconnue en matière de planification et d'organisation d'exercice qui fait l'objet de partage régulier avec ses partenaires internationaux, en particulier à l'échelon de l'Union européenne. Le Ministère des armées participe régulièrement à des exercices de gestion de crise cyber organisé par des partenaires internationaux et par l'OTAN. Afin de continuer à opérationnaliser et renforcer l'efficacité d'une réponse collective en cas de crise majeure, la France proposera à ses partenaires de renforcer leur implication dans les exercices nationaux cyber.

PREMIER
MINISTRE
Liberté
Égalité
Fraternité

Objectif stratégique 3. Un rehaussement global le niveau de cyber-protection de la Nation

Un Etat exemplaire.

Une logique reposant sur l'obligation pour les opérateurs régulés :

- une approche centralisée et renforcée pour les OIV
- une approche sectorielle déconcentrée pour les entité essentielles (EE) et entité importantes (EI) ;

Une logique reposant sur l'incitation pour l'ensemble du tissu économique et social :

- une approche visant à démocratiser l'accès à la cybersécurité en mettant la cybersécurité à portée des acteurs les moins matures et leur permettant de s'inscrire dans un processus de montée en maturité progressif
- une approche complémentaire pour maitriser le risque cyber tout au long des chaines d'approvisionnement.

Action structurante 8. Faire de l'Etat une référence de la cybersécurité à l'état de l'art

Pour assurer ses missions et garantir la continuité des institutions de la République, y compris en cas d'attaque cyber massive, l'Etat doit investir pour fortement rehausser sa cyberprotection à un niveau cohérent avec celui de la menace qui pèse sur ses services numériques et ses données, et disposer d'une capacité robuste de cyberdéfense.

La priorité sera donnée à la mutualisation des investissements afin de consolider un socle numérique homogène et sécurisé. Ce socle numérique regroupe l'ensemble des ressources et des services numériques partagés par les différentes administrations, tels que les réseaux, les centres de données, les plateformes de communication et les applications métiers.

S'agissant des données non classifiées, les travaux relatifs à la sécurité et la résilience du réseau interministériel de l'Etat (RIE) verront leur priorité renforcée tandis que l'ANSSI et la DINUM développeront une offre de sécurité pour les services hébergés dans le cloud interministériel ainsi qu'une offre de terminaux sécurisés pour les agents de l'Etat.

S'agissant des données classifiées, des travaux seront conduits par l'OSIIC dans une perspective de généralisation des interconnexions entre réseaux de niveau SECRET ne nécessitant pas un isolement spécifique. En particulier, l'amélioration du partage d'informations opérationnelles au sein du centre de coordination des crises cyber (C4) passera par la mise en place d'un système d'interconnexions sécurisées reliant les systèmes d'information de l'ensemble de ses membres, dont le financement, l'homologation, la maintenance et l'administration seront confiés à l'OSIIC. Enfin, pour accélérer la transformation numérique des politiques publiques nécessitant la manipulation de données classifiées, un incubateur de start-ups d'Etat numériques sera développé.

Le développement de solutions avancées de cyberdéfense « automatisées », propres à anticiper ou entraver des cyberattaques, sera poursuivi. Ces solutions seront déployées par l'ANSSI sur le périmètre du socle numérique et au profit des ministères afin d'augmenter leur niveau de protection. Elles bénéficieront également d'une accélération du déploiement des solutions de détection des cyberattaques supervisées par l'ANSSI, alliée à une augmentation significative des capacités de détection, de traitement et d'analyse. Un centre interministériel de supervision, qui permettra aux équipes ministérielles et à l'ANSSI d'exploiter en commun les données et alertes produites par les différents capteurs, sera mis en place.

En complément de l'investissement consenti sur le périmètre du socle numérique, l'Etat accordera une priorité budgétaire élevée pour rehausser le niveau de sécurité des systèmes ministériels qui ne pourront pas relever d'une logique de mutualisation. Garante avec la DINUM de la cohérence de ces investissements, l'ANSSI émettra un avis sur les plans d'investissement numérique annuels de chaque ministère.

Enfin, pour accompagner la migration des données de l'Etat dans le cloud et l'hybridation des capacités d'hébergement, l'Etat établira une doctrine nationale pour la mise en œuvre, par les administrations, d'une approche de cybersécurité centrée sur la valeur des données. Il développera une démarche progressive, réaliste aux plans techniques et calendaires, tenant compte des caractéristiques de chaque administration. Une priorité de premier rang sera notamment donnée au chantier de cartographie des données de l'Etat, préalable à la généralisation de telles nouvelles architectures de sécurité, ainsi qu'à la formation des agents publics afin de faciliter l'appropriation de cette nouvelle approche.

Au sein de l'Etat, le ministère des armées jouera un rôle précurseur en s'inscrivant dans la démarche dite « *data centric security* » déployée par l'OTAN.

Action structurante 9. Accorder un traitement particulier aux entités les plus critiques

Les infrastructures critiques sont aujourd'hui en France régulièrement la cible d'attaques physiques et cyber (incendies volontaires de pylônes de télécommunication, sabotages commis sur le réseau ferré, cyberattaques contre des hôpitaux etc.). Le retour des conflits de haute intensité sur le continent européen et à ses frontières a mis en lumière la vulnérabilité de ces infrastructures devenues des cibles prioritaires et stratégiques en cas de conflit. Leur destruction peut avoir de graves conséquences en France et dans les Etats voisins du fait des interdépendances structurelles de nos sociétés dans les secteurs critiques que ces infrastructures soutiennent.

Le volet cyber du dispositif de sécurité des activités d'importance vitale (SAIV) définie par la LPM de 2013 a montré toute sa pertinence dans la protection des intérêts fondamentaux de la Nation face à la menace étatique. Ce dispositif a globalement permis une prise de conscience du sujet cyber au plus haut niveau des entreprises concernées ainsi qu'une augmentation du niveau et de la maturité de ces entreprises en matière de cybersécurité.

Cela étant, la mise en œuvre du volet cyber du dispositif SAIV ne permet pas d'atteindre un niveau de sécurité adéquat pour les entités les plus critiques face aux menaces les plus avancées.

D'une part, un certain nombre d'opérateurs régulés ont inscrit leur action dans une logique de conformité réglementaire plutôt que dans une approche de maîtrise des risques. D'autre part, le suivi et le contrôle par l'Etat de cette mise en œuvre sont insuffisants, tandis que les exigences de sécurité n'ont pas été actualisées et tiennent de ce fait insuffisamment compte de l'évolution de la menace et des technologies et usages numériques.

Le volet cyber du dispositif SAIV sera donc révisé.

Cette révision sera menée par le SGDSN sur le fondement d'une analyse de risque sectorielle impliquant notamment :

- une réévaluation de la liste des opérateurs publics et privés devant entrer dans le champ du dispositif ;
- l'évaluation de l'opportunité de la mise en place d'un traitement particulier pour les OIV dont la défaillance est susceptible d'avoir des impacts systémiques en raison de leur rôle de fournisseur de services à d'autres OIV ;
- la mise à jour du corpus de mesures de sécurité techniques et organisationnelles, en cohérence avec les exigences de cyber-résilience prévues par la directive NIS 2.

En complément, une instance de partage et de dialogue sera mise en place par chaque ministère coordonnateur avec les OIV de son secteur afin de partager l'évaluation des menaces pesant sur les activités et co-construire avec eux des réponses grâce un dialogue public-privé reposant sur la confiance. Cette démarche sera soutenue par le déploiement de systèmes interministériels classifiés portés par l'OSIIC chez l'ensemble des OIV prêts à réaliser les investissements correspondants.

Action structurante 10. Mobiliser les secteurs professionnels au service du déploiement de NIS2

Avec la transposition de la première directive Network and Information Security (NIS) de l'Union européenne, la France a étendu au-delà des OIV le cercle des opérateurs soumis à des obligations en matière de cyber sécurité. Plusieurs centaines d'entreprises ont ainsi été désignées en France « opérateurs de services essentiels » (OSE).

Cette approche privilégiait jusqu'à présent un lien direct entre l'ANSSI et ces opérateurs, couvrant le soutien à l'implémentation du cadre réglementaire, l'assistance technique, la gestion des incidents de sécurité et la politique de contrôle. Si certains secteurs se sont structurés, avec l'apparition notamment de CERT sectoriels, la cyberdéfense des opérateurs critiques repose encore largement sur l'intervention directe de l'ANSSI auprès des opérateurs.

Or, la transposition de la directive NIS2 va considérablement augmenter le nombre d'opérateurs régulés en matière de cybersécurité. Cette expansion, qui ne permettra plus à l'ANSSI de maintenir un lien direct avec l'ensemble des opérateurs, requiert une évolution du modèle national pour permettre un changement d'échelle.

La directive Network Information System n°2 (NIS2)

Adoptée en janvier 2023, permet de renforcer la cybersécurité des opérateurs européens de services essentiels. Il s'agit d'entreprises des secteurs critiques pour notre économie, comme l'énergie, les transports ou encore l'eau. NIS 2 impose à ces sociétés de respecter des normes de cybersécurité exigeantes et de notifier aux autorités compétentes les cyberattaques dont elles seraient victimes. Elle accroit le périmètre des entités régulées au titre de la directive NIS1 de 2016 et s'applique par défaut à l'ensemble des systèmes d'information de l'entité.

Ce changement de modèle reposera sur une mobilisation accrue des secteurs professionnels, qui sont aux avant-gardes des enjeux de cybersécurité de notre pays, afin de positionner ceux-ci en relais de l'action de l'ANSSI et, ce faisant, de conforter le rôle de cheffe d'orchestre de celle-ci.

Cette évolution, déjà engagée dans les secteurs les plus matures, doit dorénavant s'accélérer et se structurer. En liaison avec les acteurs existants de la coordination du secteur, l'ANSSI pilotera un programme visant l'émergence et la montée en maturité, dans chacun des secteurs visés dans la transposition de la directive NIS2, de trois leviers forts :

- **un relais sectoriel**, qu'il s'agisse du ministère coordonnateur ou d'une autorité publique portant une mission de régulation sectorielle : investi d'une responsabilité sectorielle, il sera chargé de veiller avec l'ANSSI à bien articuler les exigences de cybersécurité avec les spécificités du secteur, notamment par le biais de stratégies sectorielles dédiées, et d'accompagner les opérateurs du secteur dans le renforcement de leur cybersécurité.
- **une communauté sectorielle réunissant acteurs publics et privés** : elle sera le lieu de la coordination publique-privée, qui permettra de co-construire les politiques publiques, programmes et outils cyber du secteur, et d'assurer le suivi de la mise en œuvre de la règlementation.
- **un CSIRT sectoriel** : dans une vision française de ce que sont chez nos partenaires les ISAC (*Information sharing and analysis center*), il sera le lieu du partage d'information, technique ou non, relatif à l'état de la menace du secteur, aux bonnes pratiques et au retour

d'expérience. Dans certain cas, il pourra également être le relais de l'ANSSI dans la réponse aux incidents affectant le secteur.

Avec le changement d'échelle lié à la mise en œuvre de la directive NIS2, l'autorité nationale fera de la mission de régulation un pilier de son action. La mission de contrôle, au travers de l'aspect dissuasif d'une éventuelle sanction, participera, en complément des missions d'accompagnement, de conseil et d'assistance historiquement assurées par l'ANSSI, de l'objectif de renforcement du niveau de cybersécurité en France.

[Non instruit : affecter le produit des amendes infligées par l'ANSSI au financement d'action d'intérêt cyber et de portée nationale – cf. régime bénéficiant à la Mission interministérielle de lutte contre les drogues et lesconduites addictives ou à l'Agence de gestion et de recouvrement des avoirs saisis et confisqués]

Action structurante 11. Inciter les plus vulnérables à élever leur niveau de cyberprotection

La cybersécurité des opérateurs économiques et des acteurs sociétaux non régulés, en particulier les plus petits d'entre eux comme les TPE et les PME, est encore aujourd'hui en France à un niveau trop faible. Cette situation expose à une menace de niveau technique parfois élémentaire ces acteurs qui, souvent par manque de compétences et de repères, ne savent pas par où commencer ni vers qui se tourner pour passer à l'action et prendre les mesures nécessaires pour se sécuriser.

Pour mettre fin à cette situation, **la France mettra en œuvre une politique visant à mettre la cybersécurité à la portée des acteurs les plus vulnérables**.

Cette ambition sera portée par le **développement, à l'échelle nationale, d'une offre de parcours de cybersécurité**. Inspiré du dispositif lancé initialement par l'ANSSI dans le cadre du plan FRANCE RELANCE au profit d'un millier de bénéficiaires du secteur public, ce dispositif, accessible à tous les acteurs économiques, régulés ou non, permettra aux entreprises et collectivités de s'inscrire dans une démarche progressive d'augmentation du niveau de protection et de défense de leur systèmes d'information contre les menaces cybercriminelles.

Le déploiement de cette offre sera piloté par l'ANSSI pour les entités publiques, et sera assuré par les relais sectoriels de l'ANSSI pour les opérateurs régulés. Pour les acteurs non régulés, le déploiement pourra être assuré à l'échelle territoriale. L'industrialisation de la démarche reposera dans tous les cas sur la mise à disposition par l'ANSSI de l'ensemble des outils et guides préalablement produits dans le cadre du plan France Relance.

Cette ambition verra également la **mise en place d'un mécanisme permettant à toute entreprise ou collectivité, à travers un indicateur [cyberscore] établi suivant un référentiel simple et lisible, d'attester de son niveau de cybersécurité**. Ce mécanisme permettra aux entreprises et collectivités, selon une logique incitative, de valoriser sur le marché, auprès de leurs clients, partenaires, investisseurs, leur engagement en matière de cybersécurité.

En fournissant une évaluation standardisée et reconnue du niveau de sécurité et de résilience d'une entreprise, ce mécanisme pourra notamment contribuer à la rationalisation des processus d'évaluation des risques auxquels sont soumis les entreprises, notamment dans les secteurs bancaires et assurantiels. Il pourra utilement contribuer à la structuration du marché de la cyber-assurance.

La compatibilité de ce dispositif avec le référentiel d'exigences réglementaires de sécurité sera assurée pour les acteurs régulés (OIV, opérateurs essentiels, etc.), dont la maturité sera attestée sans nécessité d'évaluation complémentaire.

L'ANSSI pilotera avec le GIP ACYMA la mise en place des ressources nécessaires à la mise en place de ce mécanisme de notation à l'échelle nationale et promouvra la mise en place de mécanismes de reconnaissance mutuelle au niveau international.

Action structurante 12. Sécuriser les chaînes d'approvisionnement

La compromission d'un fournisseur, d'un sous-traitant ou d'un prestataire d'une entreprise peut avoir des conséquences désastreuses pour cette dernière, allant du vol de données sensibles à l'arrêt total des activités. Or, le nombre d'attaques ciblant les chaînes d'approvisionnement a considérablement augmenté depuis 2018.

En matière d'espionnage, les attaquants recentrent en effet leurs efforts sur les acteurs les plus amont et les plus vulnérables des chaines d'approvisionnement, dans l'optique de pouvoir atteindre indirectement en aval des objectifs de plus haute valeur mais mieux protégés.

L'Etat ne dispose aujourd'hui que difficilement d'éléments relatifs à la maturité des entreprises critiques impliquées dans la chaine d'approvisionnement des organisations et des secteurs critiques. C'est pourquoi la déclinaison réglementaire de NIS2 imposera des obligations d'analyse de risque et de *due diligence* sur la chaîne d'approvisionnement de ces acteurs.

Ces obligations donneront notamment lieu à des contrôles qui pourront s'appliquer aux prestataires étrangers (UE et hors UE). Ce principe d'extraterritorialité, qui nécessitera un portage législatif, vise à la fois à la cohérence la maitrise du risque le long de la chaîne d'approvisionnement, mais aussi à éviter le contournement des mesures nationales.

S'agissant des acteurs non régulés, **l'introduction de la notation cyber [cyberscore] contribuera à sécuriser les chaînes d'approvisionnement** en permettant d'imposer en cascade des exigences de cybersécurité aux fournisseurs. Les clients, ou donneurs d'ordre, pourront ainsi exiger de leurs fournisseurs un **[cyberscore]** minimal en fonction de la sensibilité des contrats. Ce mécanisme permettra d'élever le niveau de sécurité numérique tout le long des chaînes de sous-traitance, et de donner une visibilité accrue aux clients sur la sécurité de leurs fournisseurs.

L'objectif est ainsi de faire monter en maturité l'ensemble de l'écosystème économique, en apportant une réponse concrète et pragmatique à la tendance préoccupante à l'augmentation des attaques cyber par supply chain.

L'État recourra systématiquement à des exigences de cette nature dans le cadre de la commande publique, en imposant progressivement un **[cyberscore]** minimal à l'ensemble de ses fournisseurs.

Objectif stratégique 4. Accompagner cette cyber-protection

Action structurante 13. Simplifier les règles du jeu

Depuis 2018, le corpus normatif cyber, tant français qu'européen, s'est enrichi avec un foisonnement de nouveaux textes ou la mise à jour de dispositifs existants couvrant différents champs liés à la cybersécurité ou connexes, notamment : Directive NIS2, IGI 1300, II 901, IGI 1337, eIDAS, Cyber Resilience Act, OSE, OIV, sous-traitant BITD, etc.

De ce fait, le cadre normatif en matière de cybersécurité est rendu insuffisamment lisible générant ainsi un effet d'empilement d'exigences :

- des exigences de cybersécurité, pourtant globalement similaires, se retrouvent dans plusieurs textes avec des niveaux de détail et de profondeur différents ;
- l'architecture réglementaire n'est pas pilotée dans son ensemble afin d'en garantir la cohérence.

Au niveau européen et international, la multiplication des réglementations nationales non-harmonisées est de nature à générer des distorsions de compétitivité pour les industriels multinationaux ou dans le cadre de projets en coopération, lorsque les règlementations et normes étrangères sont plus simples et moins coûteuses à appliquer que leur équivalent français.

L'enjeu pour l'Etat est donc de faire réduire les coûts, les délais et les difficultés liés à compréhension de la règlementation pour les entreprises et pour les administrations publiques. Une simplification des règles de sécurité des systèmes d'information en France sera ainsi recherchée.

Cette simplification visera notamment à :

- faire des exigences de sécurité définies dans le cadre de la transposition de la directive NIS2 le socle commun applicable au plus grand nombre pour protéger nos organisations contre la menace cybercriminelle ;
- mettre en cohérence avec ce socle commun les exigences de sécurité supplémentaires du dispositif SAIV destinées à protéger nos organisations les plus sensibles contre la menace étatique ;
- traiter les besoins réglementaires spécifiques, notamment sectoriels et thématiques en veillant à leur cohérence avec le bloc d'exigences NIS2/SAIV.

Ce travail impliquera d'une part, de mettre en place au niveau national, puis au niveau européen, des démarches d'équivalence et de reconnaissance croisée de référentiels entre différents secteurs d'activité. D'autre part, une démarche similaire sera nécessaire au niveau international afin d'éviter la duplication de normes et de limiter les risques d'ingérences normatives.

Une commission mixte, associant les acteurs privés et les autorités sectorielles compétentes, sera installée autour de l'ANSSI pour accompagner celle-ci dans la conception et le déploiement de cette approche réglementaire rénovée.

Action structurante 14. Accompagner la montée en maturité cyber de la Nation

Qu'ils soient portés par des initiatives publiques ou privées, nationaux, sectoriels ou territoriaux, les dispositifs permettant aux particuliers, associations, entreprises et collectivités territoriales de poser un diagnostic sur leur niveau de cyber résilience, de bénéficier d'un accompagnement pour élever celui-ci, voire d'accéder à cette fin à des aides financières, sont aujourd'hui nombreux et insuffisamment lisibles.

Pour répondre aux besoins d'accompagner la montée en maturité de ces acteurs, une **plateforme nationale d'information et d'orientation sera créée pour donner aux différents publics une information claire, les aiguiller vers les dispositifs à leur disposition et les accompagner dans leurs démarches relatives à la cybersécurité.**

Sur le modèle de la plateforme France Numérique, cette plateforme unique, porte d'entrée pour la cybersécurité, répondra au besoin d'identification d'une figure de proue de la cybersécurité du quotidien, permettant de recenser les dispositifs existants et de répondre aux interrogations des citoyens afin qu'ils puissent mieux appréhender le risque cyber, et ainsi mieux s'en prémunir. Elle sera en capacité d'orienter vers les dispositifs et acteurs pertinents en matière de prévention, de signalement et d'assistance. Elle recensera ainsi notamment les aides disponibles, les contenus de sensibilisation, et tout autre support utile pour aider le grand public dans ses démarches en lien avec la cybersécurité.

En tant que portail d'information, elle valorisera **l'offre de formation cyber initiale et continue et** les initiatives entreprises par l'Etat, les collectivités et les acteurs privés, notamment le Campus Cyber national, sur le sujet de l'attractivité des métiers de la cybersécurité. Elle permettra enfin de s**implifier le parcours d'assistance aux victimes de cyber malveillance en améliorant sa lisibilité.**

Le développement et l'exploitation de ce portail sera confié au GIP ACYMA, qui fédère les acteurs de la cybersécurité, qu'ils soient publics ou privés, offreurs ou utilisateurs, autour d'une même mission d'intérêt général. La plateforme cybermalveillance.gouv.fr, qu'il opère aujourd'hui, sera intégrée au portail.

▸ Le groupement d'intérêt public Action contre la Cybermalveillance (GIP ACYMA)

Incubé au sein de l'ANSSI à partir de 2017 et présidé par le directeur général de l'ANSSI, le GIP ACYMA opère la plateforme Cybermalveillance.gouv.fr qui vise à sensibiliser, prévenir et assister le plus grand nombre d'acteurs en France et est progressivement devenu l'un des acteurs majeurs de la prévention et de l'assistance cyber en France.

Par ailleurs, la transposition en droit français de la directive NIS2 va générer une demande croissante en matière de services de cybersécurité. Pour accompagner les collectivités et entreprises dans leur montée en maturité, une action sera entreprise pour **développer un réseau maillé d'acteurs compétents et spécifiquement formés**. Ce réseau, dont la densité devra être singulièrement accrue, sera développé sur les bases jetées par :

- **l'initiative FRANCE NUM,** qui vise à fédérer tous les acteurs de terrain au soutien de la numérisation des PME, et devra faire de la cybersécurité l'une de ses priorités majeures pour les années à venir ;
- le GIP ACYMA, qui référence avec **le label EXPERT CYBER** les prestataires à même d'assister les entreprises, notamment dans le traitement des incidents cyber.

Ce développement s'inscrit dans une logique de collaboration étroite avec les réseaux d'accompagnement économiques existants, tels que les services économiques en région, les chambres de commerce et d'industrie, et les pôles de compétitivité**.** L'objectif est de faire converger les enjeux de cybersécurité et de développement économique, en renforçant la résilience numérique des territoires et en stimulant la compétitivité des entreprises.

Enfin, l'Etat poursuivra son action en faveur de la disponibilité d'une offre de produits et de services de cybersécurité lisible et adaptée aux besoins du tissu économique, proportionnée au niveau de menace auxquels les acteurs sont exposés. Cetteoffre pourra être valorisé par les relais sectoriels et territoriaux de l'action publique cyber (CSIRT régionaux, Campus Cyber régionaux, …)

L'ANSSI développera une offre de services qui sera mise progressivement à disposition des entités régulées, et qui les aidera à concevoir, organiser et mettre en conformité leurs systèmes d'information pour atteindre progressivement un niveau de protection renforcé.

L'État soutiendra le développement d'une offre "packagée" de solutions de cybersécurité pour les TPE et PME. L'ANSSI engagera auprès des opérateurs de cloud et des opérateurs de services numériques managés (MSP) une démarche visant à faire émerger des offres dont la sécurité sera attestée par la puissance publique et sera valorisable dans la démarche de notation cyber.

Enfin, au sein de chaque secteur professionnel, les grands donneurs d'ordre seront incités à mettre en place, au profit de leur sous-traitant, un dispositif de mentorat permettant à une grande entreprise d'aider une PME pour un soutien général (organisation, finances, marketing) mais aussi pour de l'ingénierie ou des sujets techniques.

Action structurante 15. Faciliter le parcours d'assistance aux victimes de cyberattaques

L'ANSSI, en tant qu'autorité nationale de défense et de sécurité des systèmes d'information, a consolidé son rôle de cheffe de file nationale de la réponse à incidents cyber, au travers notamment de son centre de réponse à incidents gouvernemental, le CERT-FR, qui a vu son offre de services s'accroitre ces dernières années à l'attention de ses bénéficiaires, essentiellement les opérateurs régulés.

Le groupement d'intérêt public ACYMA est progressivement devenu l'un des acteurs majeurs de l'accompagnement des victimes en France, en particulier concernant le grand public (professionnels et particuliers). Il offre notamment une plateforme d'autodiagnostic afin d'orienter les victimes vers des prestataires cyber labellisés ou les acteurs publics de l'accompagnement des victimes.

L'Etat, au travers de l'ANSSI, a par ailleurs encouragé le développement de l'écosystème français des centres de réponses à incident (CSIRT – computer security incident response team) en accompagnant l'émergence et la structuration de CSIRT relais (sectoriels, ministériels, territoriaux), qui participent à renforcer les actions de prévention et d'assistance des victimes cyber dans leurs secteurs respectifs et en soutenant une association, l'InterCERT France, créée pour mettre en réseau ces centres.

Les services de police et de justice ont également renforcé leurs capacités nationales et territoriales d'enquête et de répression des actes de cybermalveillance. On peut citer à ce titre le renforcement du Parquet J3 et la création récente du COMCYBER-MI.

L'action publique en matière d'accompagnement des victimes cyber s'est grandement étoffée, au risque de manquer de lisibilité. La multiplication des plateformes de signalement complexifie en effet le parcours des victimes, ces dernières ne sachant pas toujours où s'adresser.

L'Etat engagera donc une action visant à **instaurer un parcours d'accompagnement fluide, lisible et adapté au statut de chaque victime** (entreprise, particulier, entité régulée …), en permettant à celle-ci d'obtenir les services adaptés à ses besoins dans les plus courts délais.

Cette action sera pilotée par l'Etat en y associant les acteurs de l'accompagnement aux victimes au niveau national et dans les territoires. Au-delà de la lisibilité des interlocuteurs, la simplification des parcours pour les victimes passera par un meilleur partage d'information entre les acteurs de l'accompagnement aux victimes, afin notamment d'éviter les sollicitations redondantes.

S'agissant des entités régulées, le guichet d'accompagnement par défaut sera celui du CERT-FR de l'ANSSI, qui s'appuiera, dans le contexte de la très forte augmentation du nombre d'entités régulées découlant de la directive NIS2 sur un réseau de centres de réponse à incidents relais auxquels elle délivrera un agrément. Cet agrément permettra de donner à ces centres de réponse, quel que soit leur statut (structure publique ou privée, GIP, association), une légitimité pour accompagner des entités régulées, tout en conservant à l'autorité nationale son rôle de coordination globale. Il donnera par ailleurs une visibilité à toute victime de la qualité des services offerts par ces centres de réponse à incidents cyber et représentera donc une marque de confiance.

S'agissant des publics non régulés, la plateforme 17Cyber, lancée à l'été 2024, a vocation à être le guichet connu du grand public. Elle proposera un diagnostic permettant d'orienter la victime vers l'acteur le plus pertinent pour l'aider (prestataire privé, CSIRT régional, gendarmerie /

police, justice, ANSSI). Cette plateforme offrira une meilleure lisibilité du parcours victime, garantira son suivi, et facilitera le dépôt de plainte et autres démarches administratives associées pour le grand public. Elle sera directement intégrée au portail de la cybersécurité.

PILIER 2 | INVESTIR DANS LA SECURITE DES TECNOLOGIES ET DANS LES TECHNOLOGIES DE SECURITE

> *Une économie des produits de sécurité forte et souveraine, au service d'une économie numérique sûre.*

*

Notre société repose sur un ensemble de technologies numériques essentielles, telles que les réseaux de communication, le *cloud computing* et les applications logicielles. Ces fondations numériques sous-tendent l'économie française et européenne et sont indispensables au bon fonctionnement de nombreux secteurs d'activité.

Toutefois, ces technologies sont également vulnérables aux cyberattaques, qui peuvent avoir des conséquences graves et durables. Une attaque d'envergure sur ces infrastructures critiques pourrait paralyser des services essentiels, causer des dommages financiers importants, voire nuire à la sécurité nationale.

Pour faire face à ces menaces, il est crucial d'investir massivement dans la cybersécurité de ces composants clés. Cela implique de développer des technologies de protection robustes, de former des experts qualifiés et de mettre en place des stratégies de réponse efficaces.

La France doit jouer un rôle de premier plan dans la construction d'une cyberdéfense européenne forte. Cela implique de coopérer avec les partenaires européens pour développer des solutions communes, de partager les connaissances et les meilleures pratiques, et de soutenir la recherche et l'innovation dans le domaine de la cybersécurité.

En outre, la France doit développer sa propre souveraineté numérique en s'assurant de disposer des compétences et des technologies nécessaires pour protéger ses intérêts nationaux. Cela implique de pouvoir évaluer les risques cyber, de protéger les communications sensibles, de détecter et de répondre aux cyberattaques, et de développer des technologies numériques de manière sécurisée.

L'effort national en matière de cybersécurité doit être pérenne et s'adapter aux menaces en constante évolution. Il est essentiel de mettre en place une approche cohérente et coordonnée, en tirant parti des dispositifs européens existants et en encourageant la collaboration entre les secteurs public et privé.

Les acteurs de la R&D, public et privés, renforceront leurs échanges, ceci afin de détecter au plus tôt les innovations techniques dans le domaine de la cybersécurité, les nouvelles technologies de vie numérique à protéger. Ceci devra permettre d'adapter régulièrement la politique d'investissement de l'état, dans une logique de concentration de l'effort sur les éléments les plus critiques.

Objectif stratégique 5. Sécuriser les fondements numériques de notre société

Le paysage numérique européen se trouve, à l'heure de profonds bouleversements, marqués par l'avènement de technologies innovantes et l'imbrication croissante du numérique dans tous les aspects de la vie quotidienne. Cette évolution, si porteuse d'opportunités, s'accompagne de risques accrus en matière de cybersécurité.

L'avènement de technologies innovantes comme l'intelligence artificielle (IA), le *cloud computing*, l'identité numérique, l'internet des objets (IoT) et les systèmes opérationnels technologiques (OT) s'accompagne d'une double réalité : ces produits numériques sont à la fois vecteurs d'innovation et de vulnérabilités potentielles. Cette nature duale renforce d'autant plus la nécessité d'adopter une approche proactive et résolue pour protéger les fondements numériques de l'Europe, d'autant plus à l'aube d'une ère où la sécurité des produits et des services numériques sera portée par le règlement européen sur la cyber-résilience (CRA).

Le CRA constitue un jalon essentiel dans cette démarche, en établissant un cadre juridique harmonisé pour renforcer la sécurité des produits numériques. Néanmoins, pour aller au-delà de cette réglementation et forger un socle numérique de confiance, la France, fortement intégrée au marché unique européen et, doit développer une stratégie nationale ambitieuse bâtie sur l'idée d'une autonomie stratégique européenne.

Cette souveraineté sera acquise au travers d'investissements majeurs dans la cybersécurité, notamment dans recherche et l'innovation, à l'instar du plan de relance Européen qui a financé des programmes tels qu'Horizon 2020 et Horizon Europe qui soutiennent des projets de recherche sur la cybersécurité et favorise la collaboration entre les acteurs publics et privés.

Cette nécessité s'inscrit dans la perspective de préserver une autonomie stratégique européenne dans des domaines clés en capitalisant sur les atouts du marché unique européen pour structurer notre filière industrielle. Le marché unique, avec ses 450 millions de citoyens et ses entreprises dynamiques, constitue un terreau fertile pour l'innovation et la croissance dans ce domaine.

Action structurante 16. Accompagner les fournisseurs de produits et de services numériques national dans l'implémentation du règlement européen sur la cyber-résilience (CRA)

Les attaques majeures dites WannaCry et NotPetya perpétrées en 2017 ont mis en lumière la responsabilité des éditeurs de solutions logicielles dans la vulnérabilité de notre société. La prochaine mise en œuvre du règlement européen dit *Cyber Resilience Act* (CRA) constituera un levier structurant pour le passage à l'échelle de notre résilience cyber.

> **Règlement européen sur la cyber-résilience (2022/0272)**
>
> Déclinaison de la stratégie de cybersécurité de l'UE de 2020, le Cyber Resilience Act (CRA), est un règlement européen qui vise à renforcer la cybersécurité des produits numériques mis sur le marché européen en imposant des exigences strictes à l'ensemble des fournisseurs de produits et de services numériques. Il complètera ainsi la directive NIS2, tournée pour sa part vers les entités utilisatrices du numérique, et permettra une juste répartition de l'effort nécessaire en matière de cybersécurité entre les fournisseurs de solutions numériques et leurs utilisateurs.

Le CRA permettra de généraliser à l'ensemble des produits numériques les caractéristiques indispensables à l'exigence d'hygiène numérique, en particulier la prise en compte systématique de la cybersécurité dans la conception des produits (« *security by design* ») et la fourniture de produits dans une configuration sécurisée par défaut, sans action nécessaire de leur utilisateur (« *security by default* »).

Le CRA devra également conduire à la systématisation des bonnes pratiques en matière de gestion de la sécurité tout au long du cycle de vie d'un produit, notamment en fixant les obligations des fournisseurs de ces produits en ce qui concerne la gestion responsable et coordonnée des vulnérabilités, ou de l'obsolescence de leurs produits. Pour accompagner cet objectif, et dans le cadre plus général du renforcement de la politique nationale de gestion coordonnée des vulnérabilités, **l'ANSSI participera à l'animation de la communauté nationale des chercheurs éthiques et professionnels de vulnérabilités**.

Sur le plan de la menace, une meilleure gestion des vulnérabilités et de l'obsolescence réduira structurellement la capacité pour des acteurs malveillants de détourner des équipements informatiques à des fins malveillantes. Avec les obligations de déclaration de vulnérabilités, l'ANSSI sera en mesure d'accroitre sa capacité d'anticipation d'attaque sur les systèmes d'information vulnérables, réduisant ainsi les opportunités pour les attaquants.

Compte-tenu de son champ d'application très vaste, la conformité au CRA reposera principalement sur une logique d'auto-attestation par les fournisseurs de produits numériques, adossée à une supervision renforcée par les pouvoirs publics. Elle devra néanmoins s'adosser, pour les produits présentant un besoin de sécurité particulier, à des référentiels d'exigences spécifiques, et s'articuler dans ce cas avec les schémas déjà existant de certification de la cybersécurité par des tiers de confiance.

L'ANSSI accompagnera l'amélioration des pratiques de développement logiciel en France en publiant des guides et en soutenant les travaux de conception de méthodologies et d'outils permettant d'auto-évaluer la conformité au regard des référentiels et exigences en vigueur. Elle engagera avec la DINUM une action visant l'élévation du niveau de sécurité des briques logicielles développées au sein de l'Etat.

Enfin, sur les logiciels libres :

- la **France investira dans la recherche** afin de faire émerger des mécanismes permettant de garantir et d'attester l'intégrité et la provenance de ces briques logicielles libres, à l'image du soutien qu'elle apporte au projet *SWHeritage-Sec*.

> **Le projet SWHeritage-Sec**
>
> Software Heritage est une initiative lancée il y a environ six ans par l'INRIA en partenariat avec l'UNESCO consistant à rassembler dans une seule base l'ensemble des codes source publiquement disponibles. L'archive contient déjà plus de 12 milliards de fichiers sources uniques issus de plus de 180 millions de projets logiciels d'origines différentes, avec tout l'historique de leur développement. Le projet SWHeritage-Sec consiste à extraire de cette ressource sans précédent les informations pertinentes pour la sécurité, comme les dépendances entre composants logiciels et les liens avec les vulnérabilités connues. L'objectif est de pouvoir tracer l'origine et l'impact des vulnérabilités, et permettre la détection et la correction automatique des composants logiciels vulnérables.

- **La France soutiendra les actions en faveur de la sécurité des produits *open source***, auxquels ont de plus en plus recours les produits commerciaux. Les fondations *open source*, qui orchestrent une communauté de contributeurs et maintiennent souvent la feuille de route de développement et de correction des failles, tiennent un rôle clé dans l'ensemble de la chaine d'approvisionnement.

Action structurante 17. Faire de la cybersécurité de l'IA une priorité nationale

L'intelligence artificielle est particulièrement prometteuse pour améliorer l'efficacité des dispositifs de cybersécurité et de cyberdéfense. Dans le même temps, l'utilisation malveillante de l'IA, qui permet de faciliter le développement de code malveillant et l'introduction de vulnérabilités dans les codes informatiques, accroit la pression qui pèse sur notre cybersécurité.

Cela étant, alors que l'intelligence artificielle diffuse à très grande vitesse dans toute la société, **la cybersécurité de l'IA doit constituer une priorité absolue**, du point de vue de la sécurité des données, comme de celle des modèles et des systèmes d'information sur lesquels ceux-ci sont entrainés et déployés.

Les menaces contre les systèmes à base d'IA et les contre-mesures associées sont un sujet de recherche en plein essor. Les attaques peuvent ainsi par exemple viser à reconstituer de manière illégitime le corpus des données utilisées à l'entraînement. Elles peuvent également intervenir dès la phase de conception et d'entrainement des modèles afin d'en altérer le fonctionnement.

Dans ce contexte, **il convient de doter la France des conditions et moyens favorables à la conception de protocoles d'évaluation de la sécurité des systèmes d'IA.** Cette action sera conduite par l'agence de programme numérique opérée par INRIA, en coordination avec les acteurs étatiques pertinents tels que l'ANSSI, l'AMIAD, le PEReN, le LNE, les organismes de recherche etc. et supervisée par une gouvernance interministérielle dont la coordination serait assurée par le SGDSN, **articulée avec le réseau international des instituts pour la sécurité et la sûreté de l'IA**[10].

Enfin, l'hébergement constitue également un enjeu clé pour la sécurisation des systèmes d'IA et de leur déploiement, en particulier, leur entrainement et leur hébergement dans des infrastructures. Si la France s'est dotée d'une doctrine *cloud*, elle doit chercher à l'adapter en particulier aux déploiements de systèmes d'IA et favoriser l'émergence d'une offre concurrentielle. Au-delà du cloud, la France doit chercher à développer d'autres leviers pour garantir la confidentialité des données et la maîtrise de la chaine d'approvisionnement de l'IA.

[10] *AI safety institute*

Action structurante 18. Faire du *cloud* un instrument de protection des données

La transformation numérique de notre société repose aujourd'hui sur un recours massif aux technologies et services d'informatique « *nuagique* », connue également sous le nom de *cloud computing*. Avec le développement du télétravail et l'utilisation de moyens personnels pour accéder à des données professionnelles, ce recours peut réduire le contrôle que les entités exercent sur leurs systèmes d'information et sur leurs données.

Ce mouvement représente un enjeu majeur pour la sécurité des données, dans un contexte où les conditions dans lesquelles il est pertinent de recourir aux services de cloud sont encore insuffisamment comprises et maitrisées par les clients de ces services, qu'ils soient publics ou privés. La menace que fait peser sur la sécurité de nos données la soumission de certains fournisseurs de services cloud à des lois à portée extraterritoriale n'est notamment pas appréhendée de manière homogène par l'ensemble des acteurs économiques.

Il est dès lors primordial d'investir dans le renforcement de la protection de nos données les plus sensibles hébergées dans le *cloud*.

Ce renforcement passera d'abord par le maintien et le partage par l'ANSSI de standards et d'exigences techniques, organisationnelles et juridiques pour l'hébergement des données sensibles dans le cloud, tenant compte de l'évolution de la menace. Ces exigences, essentielles pour la protection des données sensibles françaises et européennes, sont aujourd'hui présentes dans le référentiel *SecNumCloud,* élaboré par l'ANSSI, permettant de qualifier des offres de confiance.

▸ **SecNumCloud**

Ceci requiert de l'ANSSI un investissement pour maintenir en permanence un haut niveau de connaissance des technologies cloud, en composant avec la très forte dynamique d'évolution de celle-ci.

Ce renforcement passera ensuite par un meilleur accompagnement des secteurs privé et public dans la migration de leurs données et systèmes d'information vers le cloud. Ceci conduira à refondre la doctrine cloud de la France pour acculturer les sphères publiques et privées aux enjeux relatifs à l'hébergement de données sensibles. **L'Etat clarifiera ainsi les usages possibles en fonction des différents types d'offre de cloud, de la nature des systèmes d'information, du niveau de sensibilité des données.**

Cette doctrine sera promue au niveau européen afin de d'établir au sein du marché européen les conditions d'émergence d'une offre de confiance et d'une montée homogène du niveau de sécurité des données européennes les plus sensibles.

Dans le même temps, l'Etat poursuivra son action en faveur de l'émergence d'une offre de cloud de confiance, notamment par la poursuite du dispositif d'accompagnement auprès des PME.

Action structurante 19. Mettre à la disposition de tous une identité numérique de confiance

En permettant de diminuer le risque de fraude dans l'espace numérique, l'identité numérique est un levier majeur dans la lutte contre la cybercriminalité de masse.

Le déploiement en cours d'une offre de moyens d'identification numérique, publics (France Identité Numérique, FranceConnect) ou privés, permettra à terme d'offrir une protection adaptée à un large éventail d'usages numériques, selon leur criticité.

La confiance en ces moyens repose sur des garanties robustes en matière de cybersécurité, portées par la démarche de certification de l'ANSSI, en tant qu'autorité nationale de la cybersécurité. La démarche de la France s'inscrit dans une ambition européenne forte, incarnée par le règlement sur l'identification électronique et les services de confiance (eIDAS).

> **Le règlement européen règlement sur l'identification électronique et les services de confiance « eIDAS » (910/2014)**
>
> Le règlement « eIDAS » a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur. Il établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques. Sa mise en œuvre permettra aux citoyens d'utiliser leur identité numérique pour accéder à des services en ligne dans toute l'Europe, de manière simple et sécurisée.

Au service de cette ambition, l'action de l'Etat sera orientée vers la promotion à large échelle de l'utilisation de moyens d'identification numérique sécurisés et vers le maintien de la confiance dans ces moyens au travers d'une politique de cybersécurité forte.

A l'échelle nationale, cette action passera par :

- **la systématisation de l'emploi d'identités numériques sécurisées dans les services publics** en ligne et par l'accélération du déploiement de l'identité numérique régalienne.
- **une gouvernance renforcée au sein de l'Etat, associant acteurs du numérique et du cyber**, fournisseurs et utilisateurs des moyens d'identification numérique, acteurs publics et privés. L'intégration des enjeux de cybersécurité au cœur de cette gouvernance sera le vecteur de confiance et le garant de l'adoption dans la durée de ces moyens d'identification.
- **a l'appui de cette coordination, la création d'un centre national d'expertise technique pour coordonner les compétences nationales** (DINUM, ANSSI, MIOM, DGE, etc.) **sur la sécurité de l'identité numérique**. Ce centre développera des coopérations avec les autres Etats membres, à commencer par l'Allemagne qui dispose d'un centre équivalent[11].

A l'échelle européenne, la France participera activement aux travaux découlant de la révision du règlement eIDAS, qui appelle la conception et la sécurisation d'un futur portefeuille européen d'identités numériques (*wallet*). Ces travaux portent un enjeu d'harmonisation des exigences minimum de sécurité au sein du marché unique européen. La France sera attentive à ce que les futurs schémas de certification s'appuient sur des normes exigeantes de cybersécurité et préservent les intérêts nationaux pour les usages régaliens.

[11] Biometrics Evaluation Center (BEZ)

Action structurante 20. Renforcer la prise en compte de la cyber sécurité dans l'ensemble des filières industrielles.

La France dispose d'un tissu dynamique d'acteurs industriels regroupés au sein du comité stratégique de filière des industries de sécurité et couvrant une large partie de la chaîne de valeur des produits et services cyber.

Le comité stratégique de filière (CSF)

Les comités stratégiques de filière (CSF) sont un élément central de la démarche inhérente au Conseil national de l'industrie (CNI). Il s'agit de plateformes de dialogue et de concertation entre l'État, les entreprises et les représentants des salariés afin de définir, sur 19 thèmes, les projets structurants pour chaque filière. Ces engagements sont matérialisés par des contrats de filière.

Pour autant et paradoxalement, les liens entre cette filière et les autres filières industrielles (santé, aéronautique, etc.) sont restées ponctuels et souvent trop limités. Le renforcement de la coopération autour de projets de sécurité concrets au bénéfice de l'ensemble des acteurs de ces filières utilisatrices est ainsi d'ores et déjà identifié comme l'un des axes majeurs du prochain contrat de filière du CSF industrie de sécurité pour les années 2024 à 2027.

La création du comité stratégique de filière « numérique de confiance » regroupant notamment les technologies d'intelligence artificielle et de cloud computing, et auquel le comité de filière des industries de sécurité sera étroitement associé, sera l'occasion pour les acteurs de la cybersécurité de contribuer au renforcement de la sécurité des maillons essentiels de la chaîne de valeur que sont les produits et services d'IA ou de *cloud*.

Une dynamique de même nature sera mise en œuvre par l'Etat en liaison avec le conseil national de l'industrie pour l'ensemble des autres filières industrielles afin d'intégrer la cybersécurité dès la conception des produits et services et d'en garantir le maintien tout au long de leur cycle de vie.

En particulier, une priorité élevée sera mise pour limiter les conséquences physiques des menaces informatiques. En etffet, le développement exponentiel des objets connectés à Internet (IoT) et des systèmes opérationnels industriels (OT) a révolutionné de nombreux secteurs, de la santé à l'énergie, en passant par les transports. Mais dans le même temps, l**a connectivité croissante de ces systèmes cyber-physiques les rend plus vulnérables aux cyberattaques.** Ces attaques peuvent avoir des conséquences physiques graves, menaçant la sécurité des personnes, des biens et de l'environnement. En effet, les systèmes embarqués contrôlent souvent des infrastructures critiques comme les réseaux électriques, les installations industrielles et les véhicules autonomes. **La Guerre en Ukraine, dont** les réseaux électriques, les installations industrielles et les systèmes de transport, ont été la cible de cyberattaques, **a mis en lumière l'importance de renforcer la sécurité de ces systèmes.**

France 2030

France 2030 est un plan d'investissement de 54Md€, qui transforme l'économie et la société françaises en les accompagnant dans les grandes transitions écologiques, économiques et sociales auxquelles elles sont confrontées. Il intervient sur l'ensemble du cycle de l'innovation, de la recherche à l'industrialisation, et sur les dimensions supportant ce cycle – comme les

sujets de formation, de soutien à l'entreprenariat, de mise en place de communs, ou de sensibilisation – avec pour objectif de positionner la France en leader du monde de demain.

Enfin, un dispositif, visant à conditionner les aides perçues à des efforts de cybersécurité minimums, sera mise en œuvre dans le cadre du plan d'investissement France 2030 :

- **pour les verticales faisant émerger des produits contenant du numérique**, afin de réduire le risque cyber porté par ces derniers et de garantir leur conformité au titre du CRA **;**
- **pour l'ensemble de ses lauréats**, qui bénéficieront d'un parcours pour l'obtention d'une cyber notation.

Ces entreprises représentent en effet des cibles de choix pour la propriété intellectuelle qu'elles produisent ou parce qu'elles offrent à l'attaquant une possibilité de rebond vers d'autres cibles. L'Etat mobilisera les moyens financiers afin d'accompagner ces sociétés dans un parcours visant l'élévation de leur niveau de cybersécurité.

Une même approche sera promue à l'échelle européenne.

Objectif stratégique 6. Faire de la France un moteur de la structuration d'un marché européen des produits et services de cybersécurité

L'Europe s'est dotée d'une stratégie ambitieuse pour renforcer ses capacités en cybersécurité et s'imposer comme un leader mondial en la matière. Elle déploie une dynamique collective visant à harmoniser les standards, développer les compétences et favoriser la coopération entre les États membres. Depuis 2018, elle s'est dotée d'instruments variés lui permettant de garantir sa propre sécurité et de mieux affronter les crises.

Elle mène d'abord une politique de recherche et d'innovation dans le domaine cyber articulée autour de centres de compétences et de plateformes sur le territoire national, et formalisée avec l'adoption du règlement du Centre européen de compétences en cybersécurité (CECC) installé à Bucarest, dont l'objectif vise à favoriser le développement de l'expertise, de la recherche et des capacités industrielles en matière de cybersécurité au niveau européen. L'ANSSI assume pour la France la responsabilité de centre de coordination national (NCC-FR).

Ensuite, le cadre visant à relever le niveau de sécurité du tissu économique et sociétal européen s'est vu renouvelé et renforcé grâce à l'adoption de la directive NIS2 et du règlement relatif au renforcement de la cybersécurité des institutions, agences, offices et organes européens (EUIBAs). De plus, un premier schéma de certification de cybersécurité des produits a été adopté cinq ans après la formalisation du cadre européen de certification de sécurité, auquel viendra s'ajouter le Cyber Resilience Act (CRA), en vertu duquel les produits numériques placés sur le marché européen devront respecter un minimum d'exigences de cybersécurité. La révision du règlement eIDAS s'inscrit dans la même logique.

L'enjeu pour l'Union de se doter d'un cadre de solidarité dans le domaine cyber figure désormais à l'agenda européen. Il se traduit par l'adoption à venir du Cybersolidarity Act et prévoit l'extension de la certification aux prestataires de services de cybersécurité.

La France contribue à cette dynamique et se veut être un des moteurs de l'autonomie stratégique européenne dans le domaine de la cybersécurité. Elle jouera un rôle de premier plan dans la poursuite de la structuration de l'écosystème européen en matière d'innovation et soutiendra les efforts visant à faire émerger des capacités industrielles européennes de premier rang, en recherchant des synergies entre les domaines civil et militaire.

Dans cette optique, elle maintiendra à un niveau élevé ses investissements dans le domaine cyber et favorisera l'émergence et la consolidation d'acteurs industriels de premier rang mondial, à même de contribuer de manière proactive au développement capacitaire de l'Union européenne et, dans une logique de pleine complémentarité, de l'Alliance atlantique.

En particulier, elle développera des capacités de recherche dans le domaine de l'IA pour la cybersécurité, permettant à la France de se maintenir au meilleur niveau international pour anticiper les évolutions à venir dans ce domaine très dynamique, accroitre nos compétences et faciliter l'usage de l'IA dans les différents volets de la cybersécurité.

Action structurante 21. Consolider le tissu industriel national et favoriser l'émergence de champions européens

La France dispose d'un tissu dynamique d'acteurs industriels couvrant une large partie de la chaîne de valeur des produits et services de cybersécurité et de cyberdéfense. Au côté d'acteurs de premier plan occupant une place de référence sur le marché international figure un très grand nombre de PME, qui constituent la plus grande part de la filière « industries de sécurité ». **Ce tissu industriel, pour performant qu'il soit, reste aujourd'hui relativement fragile** et il convient d'actionner l'ensemble des outils de politique industrielle pour maintenir son niveau de compétences, garantir sa pérennité et son développement à long terme.

Les évolutions rapides des technologies nécessitent d'avoir un écosystème de recherche au meilleur niveau international, ayant la capacité d'attirer les talents et d'anticiper les futures potentielles menaces et vulnérabilités, de les détecter, de mieux les attribuer et d'imaginer des solutions innovantes de prévention et de remédiation. C'est le rôle des pôles d'excellence français en matière de recherche et d'innovation en cybersécurité, dont les synergies avec le monde industriel seront développées.

Afin de renforcer les dynamiques collectives de la recherche française en appui de l'État dans le domaine de la cybersécurité, les agences de programmes « numérique, logiciel et algorithmes » et « du composant aux systèmes et infrastructures numériques » sont chargées dans leurs domaines respectifs de proposer des orientations stratégiques et de faciliter l'implication de leurs écosystèmes pour répondre aux enjeux d'aujourd'hui et de demain.

L'un des leviers d'action les plus pertinents pour soutenir le développement de cette industrie est la commande publique qui offre aux industriels de la filière une référence de poids dans un contexte de concurrence internationale où le fait d'avoir l'Etat dans ses clients est la norme. Dans la suite directe du programme « Je Choisis la French Tech », l'Etat doit recourir plus systématiquement à la commande publique et notamment à l'achat public innovant à destination des acteurs de la cybersécurité.

Dans le contexte favorable d'une dynamique forte de croissance du marché intérieur européen des produits et services de sécurité, la commande publique devra notamment permettre de susciter et d'accompagner une **consolidation du secteur** aujourd'hui caractérisé par une forte fragmentation, qui rend les entreprises françaises vulnérables face à la concurrence étrangère. En prenant le relais du levier que constitue le soutien à l'innovation via l'octroi de subventions publiques, elle visera à **faire émerger des offres commerciales intégrées portées par des entreprises de taille intermédiaire** capables de répondre aux attentes du marché européen et, plus largement, mondial.

Ensuite, comme pour d'autres secteurs, les industriels de la cybersécurité peinent à trouver des investisseurs qui considèrent, à tort, ces investissements comme complexes ou trop risqués. L'Etat poursuivra son analyse des freins au développement et son soutien actif au développement de fonds d'investissement privés ou publics/privés, en particulier investissant entre *l'early stage* et le *late stage*.

L'Etat veillera également à ce que la puissance normative de l'Union européenne s'exprime pleinement en installant, conjointement avec le comité stratégique de filière Industrie de sécurité, un cadre stratégique pour organiser et renforcer la présence française dans les instances et groupes de travail en matière de normalisation et d'évaluation de la conformité en lien avec les sujets de sécurité.

En lien avec le Campus Cyber, l'Etat poursuivra son action pour lever les freins à l'accès aux données **et aux conditions d'emploi réelles des solutions**, essentiel pour permettre aux industriels du secteur d'améliorer leurs solutions.

Enfin, l'Etat accompagnera les champions nationaux sur les marchés internationaux en mobilisant davantage l'ensemble des leviers de diplomatie économique.

Il renforcera la sensibilisation des entreprises aux opportunités liées aux initiatives internationales soutenues par la France, au premier rang desquelles la Réserve cyber de l'UE et le mécanisme VCISC de l'OTAN. Il appuiera les entreprises françaises qui souhaiteraient participer à la mise en œuvre de ces instruments. Il clarifiera les conditions d'engagement des entreprises privées françaises pour répondre à des demandes d'assistance internationale et adaptera le cadre juridique afin d'assouplir le déploiement de nos entreprises à l'étranger, possiblement dans des contextes de crise, et pour intervenir sur des réseaux civils comme militaires.

L'Etat accompagnera les entreprises dans l'élaboration des réponses à des programmes complexes et multidisciplinaires, en particulier ceux donnant accès à des financements par le Fonds européens de défense.

Il soutiendra, notamment dans le cadre du plan gouvernemental « Osez l'export », la visibilité et l'exportation du savoir-faire et des solutions cyber françaises. Ce plan sera décliné en un volet export du dispositif France 2030, qui permettra d'accompagnera financièrement les entreprises lauréates.

- Le Campus cyber établira à une nouvelle feuille de route internationale afin de continuer à mettre en valeur l'écosystème cyber national tout en organisant un meilleur partage de l'information relative aux grandes initiatives en cours au niveau international.

Action structurante 22. Contribuer à porter au meilleur niveau mondial l'offre européenne de services en matière de cyber défense.

Ainsi que le démontre le théâtre ukrainien, les prestataires de services jouent aujourd'hui un rôle essentiel pour répondre à l'ampleur des besoins dans le domaine de la cyber défense, tant en matière de connaissance et d'anticipation des menaces, de détection que de reprise de contrôle après une attaque.

Être en mesure de détecter des menaces émanant de l'ensemble de nos compétiteurs ou être capable de remettre rapidement un système attaqué en état de marche représentent des enjeux de souveraineté et de résilience en cas de crise majeure.

La France considère que l'échelle européenne est l'échelle appropriée pour bâtir une offre de services compétitive en matière de cyber défense, portée par un réseau de prestataires privés de confiance et entrainé pour des opérations d'assistance susceptibles d'être requises dans le cadre de la solidarité européenne (réserve européenne), ou au bénéfice de partenaires bilatéraux qui solliciteraient un appui opérationnel.

A ce jour, la France dispose d'une base de prestataires de détection et de réponse à incident, complétée de services d'accompagnement à la gestion de crise. Cette base souffre cependant d'une interopérabilité limitée des moyens de détection et d'une faible centralisation des remontées techniques, conséquence d'un tissu industriel éclaté, dans un contexte où la masse de données acquises par les sociétés étrangères les rend incontournables. Elle souffre également d'un manque de compétences dans le rétablissement de systèmes d'information gravement compromis, domaine maitrisé par l'ANSSI mais dans lequel aucune offre privée n'existe à l'échelle nationale ou européenne.

En mobilisant l'ensemble des leviers de politique industrielle, la France mettre en œuvre un plan visant à faire émerger une offre nationale de service en matière de :

- **connaissance, anticipation et détection des menaces**, en capitalisant sur les investissements consentis dans le cadre du programme d'investissement d'avenir France 2030 et en orientant la commande publique afin de créer les conditions d'une consolidation de l'offre nationale à partir des solutions aujourd'hui proposées par les principales PME du secteur ;
  [OCE et CTI]
- remédiation de grande envergure, en accompagnant la montée en compétence du secteur privé grâce à un programme de transfert de compétences de l'ANSSI.

‣ Compte tenu de l'ampleur des attaques visant le piégeage de téléphone mobile à des fins de captation de données, une priorité sera mise sur la détection et l'investigation sur les terminaux mobiles.

Cette offre nationale constituera la contribution de la France à l'émergence d'une offre européenne de services de cyber défense, dont la structuration sera soutenue par l'amendement prévu au *Cyber Security Act* (CSA) pose les bases réglementaires pour la création de futurs schémas de certification pour ces métiers.

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Objectif stratégique 7. Maitriser nos dépendances technologiques pour assurer à la France son autonomie d'appréciation et sa liberté d'action

La protection des systèmes d'information critiques (en particulier ceux des opérateurs d'importance vitale et de l'Etat) et plus largement la protection des valeurs, du patrimoine ou des intérêts économiques de la Nation reposent sur un ensemble de fonctions clés dont la défaillance ou la compromission aurait des conséquences d'une telle ampleur qu'il convient d'avoir recours à des technologies maîtrisées.

Or, dans une économie mondialisée, le développement de solutions numériques dépend souvent de fournisseurs extra-européens pour lesquels il peut être difficile d'obtenir des garanties de sécurité.

Afin de conserver son autonomie d'appréciation et sa liberté d'action, la France se fixe dans ce contexte une ambition claire :

- conserver la maitrise complète des technologies critiques clés dans le domaine de la cryptographie et des produits de sécurité à usage gouvernemental ;
- développer les compétences nécessaires à la maitrise des architectures, à l'identification des dépendances dans les chaines d'approvisionnement en recherchant systématiquement une double source d'approvisionnement technologique, et en portant au meilleur niveau mondial la capacité nationale d'évaluation de sécurité des produits et services numériques.

Action structurante 23. Une démarche d'anticipation stratégique pour orienter nos investissements et les dispositifs de sécurité économique

La très forte dynamique d'évolution des technologies et usages numériques d'une part, de la menace d'autre part, requiert que la France structure une **démarche d'anticipation stratégique dans le domaine cyber**.

Cette démarche devra permettre d'assurer une meilleure prise en compte des mutations rapides de notre environnement et des menaces sous toutes leurs formes, afin de préparer l'avenir et éviter toute surprise stratégique. En se projetant dans le temps long et en reposant sur une capacité d'analyse multidimensionnelle, elle visera à détecter et caractériser les facteurs de risques associés à ces évolutions et contribuera à orienter dynamiquement les investissements nécessaires pour les prévenir.

Cette démarche reposera sur une enceinte interministérielle, qui sera notamment chargée d'établir, et de maintenir dans la durée, une vision des technologies et compétences du numérique essentielles pour notre sécurité et notre autonomie stratégique. Ces travaux alimenteront l'orientation de la politique de soutien à l'innovation et la politique industrielle menée par l'Etat en matière de cybersécurité. Ils orienteront également les travaux interministériels relatifs à la sécurité économique des entreprises françaises clés identifiées.

Le secteur de la recherche, coordonné par les agences de programme numérique et des systèmes, ainsi que le conseil national de l'industrie, au travers des comités stratégiques de filière compétents, seront étroitement associés à la démarche et le Campus Cyber jouera un rôle de premier plan pour associer à celle-ci l'ensemble des acteurs volontaires.

- Installer, dans une logique public-privée, des travaux d'anticipation stratégiques ayant vocation à éclairer le pilotage des politiques publiques

Action structurante 24. Maintenir la France au premier rang des nations référentes en cryptographie

Le socle de sécurité permettant d'assurer la confidentialité et l'intégrité des communications comme du stockage des données ne peut plus se concevoir sans chiffrement tant pour des usages régaliens que privés. Par ailleurs, la généralisation des échanges et des systèmes centrés sur la donnée crée des besoins nouveaux que les solutions de sécurité actuelles ne permettent pas de couvrir.

Enfin, les progrès dans la compréhension et la maîtrise des phénomènes de nature quantique sont en passe d'introduire de nouvelles révolutions technologiques, présentant à la fois des opportunités et des menaces critiques dans le champ de la cryptographie.

Or, il apparaît aujourd'hui que ces risques sont insuffisamment pris en compte, y compris au sein de la sphère publique, et que l'offre de marché permettant d'y répondre reste insuffisante et trop dépendante de solutions étrangères ou de quelques entreprises critiques, en raison notamment d'un manque de maturité des technologies en cours de développement.

Dans ce contexte, l'ANSSI, en coordination avec les agences de programme du numérique et des systèmes, établira un plan national de transition vers la cryptographie post-quantique et pilotera la participation de la France aux travaux européens visant à établir une feuille de route pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique dans l'ensemble de l'Union européenne.

Ce plan s'appuiera sur une programmation pluriannuelle de financements permettant de garantir la transition des applications souveraines vers la cryptographie quantique et l'adaptation de l'offre privée, notamment dans le domaine des cartes à puces. Cette programmation dédiée complètera les investissements prévus par la loi de programmation militaire, lesquels permettront la mise à niveau progressive de l'ensemble des moyens de chiffrement souverain de l'Etat et le maintien de capacités industrielles souveraines de premier plan.

- Etablir un plan national de transition vers la cryptographie post-quantique

En complément, des travaux de recherche et d'innovation seront conduits pour soutenir l'émergence de briques technologiques de protection de donnée, sur l'ensemble de son cycle de vie.

Les développements seront notamment attendus dans le domaine de la **protection des données dans le cloud,** à la croisée du *confidential computing*, de la cryptologie de nouvelle génération, de la détection d'altération, de l'anonymisation et de la privacité différentielle. De nouvelles solutions de chiffrement répondant aux enjeux particuliers des objets connectés (IoT) (chiffrement « à bas coût ») feront également l'objet d'un effort de recherches prioritaire.

Action structurante 25. Investir sur la durée dans une gamme élargie de produits aptes à contrer les menaces les plus avancées

L'Etat et les entreprises ont besoin de recourir à des solutions de confiance pour traiter et échanger les données les plus sensibles. Cela concerne en premier lieu les informations protégées par le secret de la défense nationale, échangées par les plus hautes autorités de l'Etat, les ministères ou les OIV. Cela concerne plus largement toutes les informations de nature stratégique manipulées par les services de l'Etat et les entreprises à leur contact, et celles échangés avec nos partenaires et alliés.

Complexes par les moyens cryptologiques qu'elles embarquent et par le niveau de menaces qu'elles visent à contrer, ces solutions nécessitent des phases de recherche et développement longues et un écosystème industriel d'excellence incluant une filière de production maitrisée. L'évolution rapide des usages et des technologies dans le domaine du numérique exige par ailleurs une accélération des cycles de développement et un investissement continu.

Pour répondre à ses propres besoins de sécurité nationale, comme aux besoins d'interopérabilité avec ses partenaires et alliés au sein de l'Europe et de l'OTAN, la France maintiendra à un niveau élevé ses investissements dans le domaine des produits de sécurité aptes à contrer les menaces les plus avancées, en se positionnant comme une nation capable d'offrir à l'Europe des solutions de sécurité au meilleur niveau, aptes à résister aux menaces les plus avancées.

Au service de cette ambition, elle relancera une dynamique interministérielle ambitieuse pour le développement de produits de sécurité à usage gouvernemental, en mettant en place une planification budgétaire interministérielle, pluriannuelle dédiée au développement de ces produits, ainsi qu'une gouvernance interministérielle chargée d'élaborer une feuille de route stratégique et d'en piloter la réalisation grâce à une maîtrise d'ouvrage clarifiée.

Action structurante 26. Accroitre la maitrise de la chaine d'approvisionnement logicielle

Les pratiques en vigueur en matière de développement de produit logiciel voient la plupart du temps les éditeurs réutiliser des briques logicielles de natures diverses, sans toujours être capables d'en tracer la provenance ou de développer une connaissance fine de ces dépendances à des composants externes.

Or, en dépit de la dynamique positive attendue avec l'entrée en vigueur du CRA, des vulnérabilités continueront d'être découvertes dans ces composants logiciels à différents moments de leur cycle de vie.

Cette situation nuit à la maitrise du risque cyber puisqu'elle ne permet ni aux éditeurs, ni *a fortiori* aux utilisateurs, de produits logiciels de connaitre l'état de vulnérabilité de ceux-ci, faute de pouvoir vérifier qu'aucun de ces composants externes n'est affecté par une faille de sécurité connue.

Pour corriger cette situation, l'Etat introduira progressivement dans la commande publique des exigences en matière de sécurisation de sa chaîne d'approvisionnement logicielle. Celles-ci permettront d'exiger la mise à disposition de la nomenclature logicielle des produits numériques dont il fait l'acquisition.

Cette démarche concernera dans un premier temps aux éditeurs de solutions visant le niveau DR et les niveaux classifiés de défense. Elle pourra ensuite être étendue à toutes les entreprises fournissant des solutions qualifiées et de confiance pour l'administration et à terme à l'ensemble des entreprises fournissant des logiciels aux services de l'Etat.

Action structurante 27. Porter la capacité nationale d'évaluation de sécurité au meilleur niveau mondial

La France dispose historiquement d'une filière d'évaluation de sécurité, constituée de laboratoires d'évaluation de sécurité pour permettre la certification ou l'agrément de produits. Cette filière dispose de compétences publiques et privées en matière d'audit logiciel et d'audit matériel. Aussi, de centres d'évaluation de services qui mènent des audits de prestations et de prestataires. En complément de quoi, des centres de certification délivrent des certificats de sécurité sur la base d'évaluations faites par les organismes précités.

Dans cet écosystème, l'ANSSI joue un rôle central en assurant dans de nombreux cas, en particulier pour le niveau élevé, le rôle de centre de certification. Elle agrée également les centres d'évaluation de produits ou de services et assurera, par application du *Cyber Security Act*, le rôle d'autorité nationale de certification de cybersécurité pour la certification européenne. Le Ministère des Armées joue par ailleurs un rôle central pour l'évaluation de produits et systèmes classifiés de défense visant des agréments ou une homologation.

L'évolution rapide des usages et des technologies du numérique impose une adaptation constante de cette filière en faisant évoluer les capacités d'évaluation en réponse aux attentes du marché : expertises, connaissance de l'état de l'art, suffisance de ressources humaines, etc.

Parmi les évolutions technologiques appelant aujourd'hui une adaptation des domaines d'expertise figurent notamment : la migration vers la cryptographie post-quantique ; le recours à des systèmes d'intelligence artificielle pour assurer des fonctions de sécurité dans certains produits (détection, filtrage, reconnaissance d'identité, etc.) ; l'utilisation de l'intelligence artificielle pour évaluer les produits de sécurité ; l'innovation en matière de protection de la donnée en exécution (chiffrement et calcul multipartite, exécution en enclaves matérielles, informatique confidentielle) ;la migration des fonctions de sécurité des cartes à puces vers d'autres composants matériels comme les Systems-on-Chips.

Par ailleurs, l'harmonisation à l'œuvre en Europe des pratiques d'audit et de délivrance de certificats de sécurité dans le contexte du Cyber Security Act (CSA) et du Cyber Resilience Act (CRA) expose la filière à des exigences de capacité et de compétitivité nouvelles.

Dans ce contexte, la France investira pour développer sa capacité d'évaluation de sécurité et la porter au meilleur niveau mondial. Elle veillera au développement d'une offre privée apte à évaluer des produits et services selon les normes françaises, européennes ou internationales et Le modèle économique du schéma français sera confronté à celui adoptés par d'autres filières européennes dans le but d'identifier les freins à la compétitivité. Dans le même temps, elle renforcera les moyens de l'ANSSI et ceux du ministère des armées.

Des partenariats seront créés avec les acteurs académiques de la formation et de la recherche en cybersécurité tandis que des coopérations seront mises en place entre centres d'évaluation de différents Etats-membres afin de mettre en commun des compétences.

▸ Mettre en place un programme de transfert de compétences des acteurs publics vers les acteurs privés.

PILIER 3 | BATIR UNE CYBERDEFENSE OPERATIONNELLE

> *Renforcer la réponse gouvernementale face au développement de la menace et décourager les adversaires potentiels de la France de mener des cyberattaques sur ses infrastructures ou celles de ses partenaires.*

*

En dépit des mesures de protection et de défense robustes qu'elle met en œuvre, la France est confrontée à une cybermenace débridée qui porte atteinte à ses intérêts.

D'un côté, elle a vu apparaitre, sur des secteurs jusqu'alors préservés, des modes d'action d'une intensité croissante opérés par des attaquants qui n'hésitent plus, souvent à des fins criminelles, à paralyser des infrastructures critiques pour la Nation, comme des hôpitaux. De l'autre, elle observe une élévation de l'intensité et du niveau de sophistication d'opérations clandestine d'espionnage et de pré-positionnement visant des intérêts fondamentaux de la Nation. Ces attaques représentent pour la France un préjudice considérable.

La France ne vit pas cette tendance comme une fatalité et est déterminée à entraver la dynamique d'expansion de la menace cyber. Elle s'emploiera **à mobiliser, de manière coordonnée, l'ensemble des leviers d'action à sa disposition pour** augmenter significativement le coût et les risques pour ceux qui nuisent à notre économie, à la stabilité de nos démocraties, à la sécurité de nos concitoyens, les décourageant ainsi de s'en prendre à la France.

Objectif stratégique 8. Renforcer les leviers institutionnels

Action structurante 28. Renforcer le cœur de la cyberdéfense nationale

Pour répondre aux agressions qui visent les intérêts fondamentaux de la Nation dans le cyber espace, la France dispose du Centre de coordination des crises cyber (C4). Il réunit autour du SGDSN les administrations de l'Etat en mesure de (i) développer une connaissance et une analyse approfondies de la menace, (ii) détecter, caractériser et imputer les attaques, (iii) contribuer à la réponse de l'État aux cyberattaques.

A la différence de la cellule interministérielle de crise (CIC), qui pilote la gestion des effets d'une crise, le C4 situe son action sur le plan de la gestion des causes. Son rôle est de d'élaborer et de soumettre à la validation de l'autorité politique les stratégies appropriées de réponse aux cyberattaques. Chaque stratégie de réponse, proposée par le C4 à l'autorité politique, est établie en fonction notamment de la gravité de l'attaque, de son origine et de la disponibilité, des coûts et bénéfices associés à chaque levier qui peuvent par ailleurs se cumuler.

Parmi les principales mesures que la France se réserve le droit d'utiliser en réponse à une attaque figurent des leviers techniques (diffusion d'informations sur la menace, perturbation ou neutralisation des activités de l'attaquant par des actions informatiques), **diplomatiques** (condamnation publique, mise en œuvre de mesures de rétorsion, ou *a contrario* activation d'un canal de dialogue, développement de mesures de confiance), **judiciaires, politico-médiatiques, économiques et militaires**. En fonction des objectifs recherchés, elle peut également décider de mobiliser des leviers de réponse en lien avec ses partenaires étrangers et dans le cadre de l'UE et de l'OTAN.

Selon les cas, la France pourra décider d'*attribuer* l'attaque en en choisissant les modalités : attribution publique (désignation publique du commanditaire ou de l'exécutant d'une attaque), **attribution privée** (de façon confidentielle et bilatérale, soit auprès d'un Etat tiers, soit directement auprès de l'Etat incriminé), **attribution coordonnée** (publiquement, de façon concertée et coordonnée avec d'autres Etats ou sous l'égide d'une organisation internationale).

Pour enrayer la dynamique de développement de la menace et imposer un coût accru aux agresseurs :

- **le C4 se saisira de manière désormais plus systématique de l'ensemble des leviers à sa disposition pour répondre aux cyberattaques.** Cette orientation visera notamment à améliorer la mobilisation du levier des sanctions et de la capacité d'entrave offerte par la capacité nationale cyberoffensive. Elle visera également à renforcer la coordination de l'action des services de l'Etat avec l'action judiciaire. Cette coordination accrue s'appuiera notamment sur la mise en œuvre des dispositions prévues à l'article 706-105-1 du code de procédure pénale, qui constitue un instrument de nature à faciliter ces échanges d'informations entre les autorités judiciaires et administratives dans le cadre d'enquêtes sur la cybercriminalité. Il a déjà permis aux procureurs de transmettre des informations pertinentes pour les enquêtes en cours auprès des services spécialisés désignés.
- **le C4 orientera son action vers l'anticipation opérationnelle des activités malveillantes susceptibles de viser la France.** A cette fin, un centre d'échange et de coordination sera

créé afin de réunir, sur des plateaux de nature technico-opérationnelle, l'ensemble des compétences étatiques disponibles au sein de l'ANSSI, la DGSE, la DGSI, la DGA et le COMCYBER du ministère des armées.

Action structurante 29. Renforcer l'action judiciaire en matière de lutte contre la cybercriminalité

Face à l'escalade des cybermenaces et à la sophistication croissante des cybercrimes, le renforcement des capacités judiciaires françaises en matière de lutte contre la cybercriminalité est une nécessité impérieuse.

L'enjeu crucial pour la France est double : améliorer l'efficacité des investigations judiciaires pour identifier et traduire en justice les cybercriminels et **renforcer ses capacités à décourager toute forme de cybercriminalité** en envoyant le message clair et la preuve par les faits que la cybercriminalité ne sera pas impunie.

Pour atteindre ces objectifs, un plan d'action structuré et multidimensionnel sera mis en œuvre, comprenant en ligne de fond le développement d'une double expertise juridique et cybernétique au sein des différents échelons judiciaires.

Les capacités d'investigation spécialisées des services compétents seront renforcées. Cela implique d'une part de doter le parquet spécialisé de Paris, compétent au niveau national, des ressources nécessaires pour mener des enquêtes complexes et aboutir à des condamnations. D'autre part, de développer des compétences cyber au sein des juridictions inter-régionales et locales afin de leur permettre de traiter efficacement les cybercrimes sur leur territoire.

Le cadre légal judiciaire, en particulier le code de procédure pénale (CPP), devra également évoluer pour tenir compte des spécificités de la cybercriminalité. En effet, les cybermenaces d'aujourd'hui ne correspondent pas toujours aux infractions prévues dans les textes actuels, ce qui limite la capacité des autorités à poursuivre les cybercriminels et à obtenir justice pour les victimes. Parmi les adaptations nécessaires, on peut citer :

- **la création d'un cadre pour conduire des opérations de démantèlement et de désinfection à distance** des supports informatiques utilisés par des cybercriminels à l'insu de leurs propriétaires légitimes, afin de faire cesser l'infraction ;
- **la création d'une infraction spécifique de fraude informatique.** Cette infraction permettrait de sanctionner plus efficacement les actes de piratage informatique, d'intrusion dans des systèmes informatiques et de vol de données ;
- **la modification de l'infraction de plateforme en ligne.** Cette infraction, actuellement limitée à la diffusion de contenus illicites, devrait être élargie pour couvrir d'autres types d'infractions commises sur les plateformes en ligne, comme la cybercriminalité.

Enfin, les coopérations internationales seront intensifiées. En la matière, la France pilote ou participe déjà activement à des opérations internationales de lutte contre la cybercriminalité, conduite principalement par le paquet de Paris. Cette coopération inter-services et inter-Etats doit à présent se développer et être partagée par un plus grand nombre d'acteurs judiciaires afin de permettre un meilleur partage des informations, une coordination des enquêtes plus efficiente et des possibilités accrues de recours aux procédures d'extradition.

Action structurante 30. Renforcer l'action administrative en matière de lutte contre la cybercriminalité

La cybercriminalité, en pleine expansion, menace désormais les individus, les entreprises et les États. Face à cette menace croissante, il est impératif de mettre en œuvre des mesures fortes et efficaces pour protéger nos citoyens et nos intérêts nationaux.

Aujourd'hui, les sanctions financières apparaissent comme un instrument potentiellement efficace dans la lutte contre l'impunité des cybercriminels Elles sont complémentaires des saisies judiciaires et privent les cybercriminels de leurs avoirs, notamment numériques.

▸ **Mesures de gel des avoirs**

Le registre national des gels, tenu par la direction générale du Trésor, recense toutes les personnes, entités et navires faisant l'objet de mesures de gel d'avoirs en France. Ces mesures, prises en application de dispositions nationales, européennes et internationales (ONU), visent à empêcher les personnes et entités visées de réaliser des opérations financières.

L'extension du régime national de gel des avoirs aux cybercriminels s'inscrit dans une démarche globale de lutte résolue contre la cybercriminalité. En prévenant la dissipation des avoirs du cybercriminel, y compris ceux n'ayant pu être identifiés et saisis judiciairement, cette mesure s'appuie sur une approche pragmatique et efficiente pour s'attaquer au cœur du problème : les motivations financières des cybercriminels.

Ce dispositif de gel constituera un instrument supplémentaire qui devra être :

- **proportionné :** ne s'appliquer qu'aux personnes soupçonnées de cybercriminalité et qu'il est soumis à des garanties strictes pour protéger les droits individuels ;
- **efficace** : permettre d'interdire rapidement l'accès de la cible du gel à toutes ses ressources financières et immobilières.

Ce levier sera complémentaire du régime de saisies judiciaires qui nécessite une identification préalable des avoirs. Toute action visant alors à contourner la mesure de gel, qu'elle soit directe (celle du mis en cause) ou indirecte (action d'un complice) sera criminalisée. Compte tenu de l'efficacité opérationnelle de l'articulation entre saisies judiciaires et sanctions financières, il apparaîtrait opportun de pouvoir disposer d'un tel levier d'action similaire à l'échelle nationale pour le contentieux de la cybercriminalité.

Action structurante 31. Renforcer la crédibilité de la posture cyber de l'UE en contribuant davantage à la mise en œuvre de la boîte à outils cyberdiplomatique de l'UE

▸ Mobiliser davantage le régime de sanctions cyber de l'Union européenne et en élargir le périmètre, notamment aux cybercriminels

La réponse aux incidents de cybersécurité demeure une prérogative souveraine. Pour autant, alors que la menace cyber pèse sur l'ensemble de l'Union européenne et compte tenu du poids d'une réponse conjointe de l'UE et ses Etats membres, l'Union a développé une boite à outils cyberdiplomatiques en 2017. Ce dispositif fournit une cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillances. Il permet de faire pleinement usage des mesures relevant de la politique étrangère et de sécurité commune, y compris, si nécessaire, des mesures restrictives. Cette réponse conjointe est proportionnée à la portée, l'échelle, la durée, l'intensité, la complexité, la sophistication et l'incidence de l'attaque.

La France apporte un fort soutien à la mise en œuvre de ces outils européens, y compris s'agissant de la réponse aux cyberattaques, dans le respect des prérogatives nationales et du droit international. Depuis 2022, l'Union européenne a réalisé deux attributions publiques de cyberattaques qui ont témoigné d'une plus grande convergence entre les Etats membres sur la nécessité d'affermir la réponse européenne et sur la capacité de l'Union à parler d'une seule voix. Des travaux sont également en cours pour décliner la boîte à outils en stratégies spécifiques en fonction de la menace.

A la suite des cyberattaques conduites contre l'Organisation pour l'interdiction des armes chimiques (OIAC), les dirigeants européens ont appelé à renforcer les capacités de dissuasion, résilience et réaction de l'UE. Parmi les outils disponibles, le règlement 2019/796 a mis en place un régime de sanctions européen consacré aux cyberattaques.

▸ **Règlement européen (2019/796)**

L'UE peut ainsi imposer des mesures restrictives ciblées à l'encontre de personnes ou d'entités impliquées dans des cyberattaques qui ont des répercussions importantes et constituent une menace extérieure pour l'UE, ses Etats membres ou des Etats ou organisations internationales tiers lorsque ces mesures sont jugées nécessaires pour réaliser les objectifs de politique étrangère et de sécurité commune.

Le régime de sanction est transversal (portée mondiale) et consiste, pour les individus visés, en des restrictions de déplacement sur le territoire de l'UE et de gels des avoirs pour les individus et entités. Les désignations doivent s'appuyer sur des éléments de preuves disponibles en sources ouvertes et sont susceptibles de recours devant les juridictions européennes.

La France soutient activement la mise en œuvre de la boite à outils cyberdiplomatiques et l'opérationnalisation des différents leviers qui concourent à renforcer la posture cyber de l'UE. Sans préjudice de la réponse à titre nationale, elle cherchera à associer ses partenaires européens aux stratégies de réponse aux incidents qui s'y prêtent et montrera sa solidarité en contribuant à la réponse européenne lorsque l'UE ou d'autres Etats membres sont visés.

La France portera son effort pour identifier les individus ou entités à désigner et soutenir la construction de dossiers de preuve. Une fois constitués, ces dossiers devraient pouvoir être

transmis à l'UE et aux autres Etats membres pour contribuer à nourrir les désignations. Ces dernières faisant l'objet d'un renouvellement régulier, il conviendra de pouvoir les alimenter pour justifier de la menace et du maintien de la mesure.

Enfin, la désignation de cybercriminels dans le cadre du régime est possible à droit constant. Le recours à ce régime permettra d'avoir un impact plus important sur le terrain compte tenu des effets des mesures sur les groupes cybercriminels dont la motivation est financière.

Action structurante 32. Mobiliser la capacité nationale cyberoffensive au service de l'entrave des actions cybermalveillantes

Rédaction réservée.

Objectif stratégique 9. Mobiliser les acteurs privés dans la cyberdéfense de la Nation

Action structurante 33. Mobiliser les acteurs privés de l'Internet dans la lutte contre les cybermenaces

Le réseau Internet repose sur un certain nombre d'acteurs structurants, en particulier les opérateurs de communications électroniques (OCE), les hébergeurs, les gestionnaires de nom de domaine et les réseaux de diffusion de contenu. Du fait de leur positionnement, ils disposent d'une capacité à avoir une vision large sur les activités des attaquants, et bloquer leurs actions quand cela est jugé nécessaire.

De ce fait, ces acteurs sont appelés à jouer un rôle important dans la cyberdéfense de la Nation. Il s'agira donc, sur la base de partenariats public-privé, de mettre en place un ensemble de mesures de protection pour détecter et caractériser au plus tôt les attaques avant qu'elles n'atteignent les utilisateurs, et éventuellement les bloquer.

▸ Les dispositifs légaux pour observer ou bloquer des activités malveillantes

En matière d'observation, l'ANSSI peut recueillir certaines données utiles à la cyberdéfense[12], et peut fournir préalablement des marqueurs techniques aux OCE[13] pour les accompagner dans cet effort de détection.

En matière de blocage ciblé, des dispositifs sont prévus, notamment sur le DNS, pour exiger une des OCE une neutralisation des menaces portant atteinte à la sécurité nationale[14].

Contre la menace de masse ciblant les consommateurs, la mise en place d'un filtre anti-arnaque[15] vise à filtrer de manière préventive les adresses internet qui correspondent à des sites malveillants, aussi bien sur ordinateur que sur smartphone.

Pour les serveurs d'attaquants hébergés sur le territoire national, l'autorité judiciaire peut intervenir pour faire saisir ces serveurs et faire cesser l'infraction.

Les dispositifs légaux existants, complétés par la loi de programmation militaire pour 2024-2030, offrent donc un large panel de leviers d'action aux services de l'Etat. Il s'agira désormais :

- **de consolider leur mise en œuvre**, notamment en assurant le financement, pour les OCE et les hébergeurs, des capacités nécessaires à leur mise en œuvre effective ;
- **de mettre en place un système permettant la transmission plus rapide et plus simple à traiter** pour les OCE et principaux hébergeurs des différentes sollicitations aux titre des différents dispositifs légaux. La capacité judiciaire pourra en bénéficier ;
- **pour le dispositif issu de la loi SREN**, de l'alimenter par différents acteurs publics comme privés pour augmenter son efficacité. L'effet communautaire de ce dispositif sera un garde-fou comme un formidable vecteur de circulation de l'information à grande échelle.
- **pour les services de l'Etat et les opérateurs d'importance vitale (OIV), de mettre en place un centre de « nettoyage » de trafic internet (*scrubbing center*), qui permettra à l'ANSSI**

[12] article L2321-2-1 et L2321-3-1 du Code de la défense
[13] article L33-14 du Code des postes et des communications électroniques – CPCE
[14] article L2321-2-3 du Code de la défense
[15] porté par la loi visant à sécuriser et réguler l'espace numérique (SREN) promulguée en 2024

de rerouter le trafic réseau d'une entité victime d'une telle attaque, et de le filtrer afin d'en limiter les impacts et la durée. Ces centres spécialisés, déployés à des points névralgiques du réseau internet national, joueront un rôle essentiel dans le blocage des flux malveillants.

Action structurante 34. Faire du partage de l'information un levier de cyberdéfense

Le partage d'informations techniques sur les menaces est la clé de voute de notre cyberdéfense collective. Il conditionne notre capacité à mieux détecter et contribue à la prévention et à l'entrave des cyberattaques.

Les acteurs privés jouent dans ce domaine un rôle essentiel en ce sens qu'ils consomment et produisent des informations techniques qu'ils doivent pouvoir échanger par ailleurs. Or, il leur est parfois difficile de partager ces informations. Les difficultés rencontrées tiennent à la qualification, la normalisation et la gestion du cycle de vie des informations techniques et leur adaptation à un contexte donné. De plus, les entités privées ont des niveaux de maturité hétérogènes en matière de cybersécurité, ce qui a un impact sur les capacités de traitement des informations et sur l'aptitude à garantir la confidentialité de ces dernières.

Le modèle français du partage d'informations relatives à la menace repose sur une mise en réseau et un dialogue public-privé, incarnés par l'InterCERT France.

InterCERT France

Association professionnelle créée en 2021, l'InterCERT France constitue la première communauté d'équipes de réponse aux incidents de sécurité informatique (CSIRTs) en France. Elle rassemble plus d'une centaine de CSIRT appartenant à différents secteurs économiques et prestataires de services mais aussi des émanations d'acteurs du secteur public, dont le CERT-FR de l'ANSSI, CSIRT national et gouvernemental. Son existence est fondée sur deux objectifs principaux : le partage de données actionnables et l'accueil de nouvelles structures publiques comme privées pour les accompagner vers un meilleur niveau de maturité cyber.

Acteur central de l'écosystème, l'InterCERT France sera accompagnée dans une nouvelle étape de l'échange d'informations entre acteurs cyber. A la fois communauté nationale et somme de communautés sectorielles, l'InterCERT France pourra ainsi accélérer sa montée en puissance et continuer à se structurer en communautés sectorielles.

Pour accroitre les capacités de l'InterCERT France, l'Etat accompagnera l'organisation dans le renfort de ses moyens ainsi que dans sa reconnaissance en tant qu'association d'utilité publique. Il s'agira notamment de mettre en œuvre un outillage commun, de partager des analyses de la menace et des vulnérabilités par secteur, de mutualiser avis sur des produits de sécurité et leur pertinence dans un secteur d'activité donné, d'organiser le retour d'expérience sur des incidents et d'accompagner la montée en maturité des CSIRT les moins avancés, mentorés par les CSIRT les plus expérimentés.

Aussi, l'InterCERT France, en s'inscrivant dans le schéma européen promu par l'ENISA, jouera un rôle crucial dans l'intégration des communautés sectorielles aux réseaux européens de cybersécurité. Ce faisant, il facilitera le partage d'informations spécifiques à chaque secteur, prenant en compte les menaces, les technologies et les vulnérabilités propres à chacun.

Pour favoriser ce partage ciblé, l'État accompagnera l'émergence de structures les plus adaptées, telles que des CSIRT sectoriels ou des communautés d'échanges au sein de l'InterCERT France.

Il appartiendra à l'Etat et à l'ANSSI, en tant qu'autorité nationale, d'accompagner cet élan vers un plus grand partage d'informations, notamment par la diffusion de ses connaissances dans les communautés appropriés et par l'accompagnement et l'outillage de l'écosystème.

PILIER 4 | S'AFFIRMER A L'INTERNATIONAL COMME UNE PUISSANCE CYBER RESPONSABLE, COOPERATIVE ET SOLIDAIRE

> *La résilience de la France dépend de celle de ses partenaires européens et internationaux ainsi que de la sécurité et de la stabilité du cyberespace dans son ensemble.*

Facteur clé de la résilience cyber des nations et de la stabilité du cyberespace dans son ensemble, la coopération internationale fait face aujourd'hui à de nombreux défis : cyber-conflictualité croissante, y compris dans le cadre de stratégies hybrides, remise en question du multilatéralisme et des mécanismes de régulation onusiens, promotion d'une vision autoritaire de l'espace numérique par certains Etats, prolifération et ruptures technologiques susceptibles d'abaisser le seuil d'accès à l'arme cyber, rôle croissant joué par des acteurs non-étatiques, y compris au sein du secteur privé, etc.

Dans ce contexte, la France cherchera à maximiser les effets de son action internationale en inscrivant celle-ci dans le respect de plusieurs principes clés.

La France promeut une approche fondée sur les valeurs démocratiques, tels que le juste équilibre entre liberté et sécurité, notamment en matière de lutte contre la cybercriminalité, l'opposition aux modèles autoritaires de gouvernance du cyberespace, la promotion de l'État de droit et l'application du droit international dans le cyberespace. La France est attachée à un cyberespace libre, ouvert, sûr et non-fragmenté.

La France agit comme un moteur au niveau européen, et soutient le renforcement de l'autonomie stratégique de l'UE dans le domaine cyber. L'action européenne repose sur un modèle robuste de cyber-résilience – dans la construction duquel la France joue un rôle de premier plan – conjugué à un recours à des leviers d'action multiples sur les plans règlementaire, industriel, judiciaire, diplomatique ou encore militaire. Ce faisant, la France contribue au renforcement de la sécurité euro-atlantique et au pilier européen de l'OTAN.

La France est attachée à une gouvernance internationale agile, fondée sur un équilibre entre une gouvernance multilatérale (comprenant les organisations internationales et leurs Etats Membres) et une gouvernance multi-acteurs (comprenant États, secteur privé, organismes de recherche, société civile), qui fasse clairement apparaître les droits et responsabilités pour chaque partie prenante. En particulier, la France est attachée au caractère multi-acteurs de la gouvernance de l'Internet.

La France est une puissance d'initiative, dotée d'une diplomatie proactive (ex : Appel de Paris, Programme d'action de l'ONU, Processus de Pall Mall) et pragmatique, recherchant l'équilibre et le consensus. Elle rejette la logique de blocs géopolitiques, qu'elle considère comme un facteur d'instabilité et de fragmentation du cyberespace.

La France est attachée à sa liberté d'action dans le cyberespace, et dispose à ce titre de capacités de lutte informatique défensive, offensive, et d'influence. Ces capacités sont mises en œuvre de manière autonome ou combinée, dans le respect du droit international. Dans ce domaine, la France recherche la construction de partenariats militaires et l'action en commun avec ses alliés.

Sur la base de ces principes, la France mettra en œuvre trois axes d'effort :

(1) **agir en « puissance responsable » en faveur de la sécurité et la stabilité du cyberespace** : la France agit dans le cyberespace sur la base d'une grammaire stratégique cyber propre et dans le respect du droit international. Elle promeut un cadre normatif international

définissant des obligations de bonne conduite pour les Etats – ainsi que pour d'autres acteurs au comportement potentiellement déstabilisant (ex : secteur privé) – et permettant une coopération efficace contre des menaces communes (ex : lutte contre la cybercriminalité)

(2) **agir en « puissance coopérative » à l'échelle de l'UE, de l'OTAN et dans le cadre de partenariats formant une communauté d'intérêt :** la France agit et coopère en allié et partenaire fiable dans le cyberespace, en jouant un rôle moteur au service de l'autonomie stratégique de l'UE – concourant ainsi au développement de l'ensemble de ses leviers politique, normatif, industriel, diplomatique et défense – et au sein de l'OTAN, en tant qu'alliance militaire. Dans l'ensemble de ses partenariats, la France promeut avec ses pairs une approche pragmatique afin d'augmenter le niveau global de sécurité.

(3) **agir en « puissance solidaire » en faveur du renforcement du niveau de cybersécurité à l'échelle internationale :** la France entend se doter des moyens d'aider les partenaires qui en expriment le besoin, compte tenu de ce que sa résilience dépend aussi de celle de ses partenaires. Cet appui, qui a vocation à promouvoir l'approche française en matière de résilience, peut prendre une forme structurelle (promotion de bonnes pratiques, programmes de renforcement capacitaire) ou opérationnelle, y compris sur le plan militaire (« Partenariat cyber agile » ou « *Tailored Cyber Partnership* »).

Objectif stratégique 10. Être une puissance cyber responsable et promouvoir un cadre et une gouvernance internationale garantissant la sécurité et la stabilité du cyberespace

Le cyberespace n'est pas un espace de non-droit. La France prend ses responsabilités pour en faire un espace libre, ouvert, sûr, non-fragmenté, stable, accessible et pacifique et contrarier les tentatives de certains de ses compétiteurs et adversaires d'en faire un instrument de pouvoir autocratique ou un champ privilégié pour la conduite de campagnes hybrides à des fins de renseignement, de déstabilisation, de perturbation, voire de destruction.

En tant que puissance responsable agissant dans le cadre du droit international, la France s'attache à inscrire le plus largement possible son action dans un cadre multilatéral afin de promouvoir un cadre normatif à même de garantir la sécurité et la stabilité du cyberespace. Elle développe à cet égard au sein de l'organisation des Nations unies une approche pragmatique en faveur de l'élévation du niveau de cybersécurité à l'échelle mondiale.

La France est par ailleurs engagée en première ligne pour associer à cette ambition les entreprises privées, qui possèdent la quasi-totalité des infrastructures de l'Internet et opèrent la plus large partie des services numériques sur lesquels reposent aujourd'hui le fonctionnement de nos sociétés.

La France est engagée en faveur de la non-prolifération des armes numériques et porte des propositions permettant d'encadrer le commerce et l'usage irresponsable de capacités cyber-intrusives disponibles sur le marché.

En tant que puissance responsable, la France fait du principe de transparence un élément clé de sa posture.

Action structurante 35. Mettre en œuvre et approfondir le cadre normatif multilatéral en matière de sécurité du cyberespace

La régulation de l'usage des technologies de l'information et de la communication (TIC) dans un contexte de sécurité internationale fait l'objet de négociations entre Etats depuis déjà un quart de siècle. Au sein de l'Organisation des Nations unies (ONU), cette discussion a permis de définir un consensus sur un cadre de comportement responsable, reposant notamment sur le droit international existant et comportant, de manière additionnelle, onze engagements de bonne conduite à caractère volontaire spécifiques au domaine cyber. Ces engagements adoptés en 2015 prévoient, par exemple, que les Etats doivent s'abstenir d'endommager les infrastructures essentielles d'un autre pays ou qu'ils sont tenus à coopérer entre eux dans la gestion des incidents informatiques.

▸ La diligence requise (due diligence)

C'est un principe général du droit international, consacré par la pratique des Etats et la jurisprudence internationale. En 2015 à l'ONU, les contours de cette obligation appliquée au cyberespace ont été précisés sous forme de norme de comportement responsable volontaire et non contraignante. Il s'agit ainsi pour les Etats de ne pas « permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications ».

Cet ensemble de règles s'appliquent aux activités conduites dans le cyberespace, que ce soit à des fins offensives ou défensives, en temps de paix comme en temps de guerre. Dans un contexte de très forte polarisation des discussions aux Nations unies, la France poursuivra la promotion de son initiative de réforme de la gouvernance de l'ONU en matière de cybersécurité, via l'établissement d'un Programme d'Action (PoA) des Nations unies à l'horizon 2026. Cette initiative aura notamment vocation à faciliter la mise en œuvre – aujourd'hui lacunaire - du cadre normatif agréé.

▸ Le programme d'action des Nations unies sur la cybersécurité

Les négociations à l'ONU visant à consolider un cadre de comportement responsable pour les Etats dans le cyberespace ont jusqu'à ce jour été traitées par des groupes de travail mis en place pour une durée limitée, et qui se concurrençaient parfois entre eux. Afin de stabiliser ce processus, la France a été à l'initiative d'une proposition de Programme d'action (PoA) des Nations unies sur la cybersécurité, dont l'Assemblée générale des Nations unies a décidé qu'il serait mis en place d'ici 2026. Conçue aux côtés d'un groupe d'Etats de toutes les régions du globe, la proposition de PoA a vocation à offrir une plateforme permanente et tournée vers l'action accessible à l'ensemble des Etats, ainsi qu'aux autres parties prenantes (industrie, recherche, société civile). L'objectif du PoA est 1/ d'offrir un cadre pour poursuivre les discussions et la coordination aux Nations unies sur les enjeux de cybersécurité et 2/ de soutenir les efforts des Etats dans la mise en œuvre du cadre normatif existant, notamment à travers des projets concrets en faveur de l'élévation du niveau de cybersécurité à l'échelle mondiale, contribuant ainsi à réduire la fracture numérique dans ce domaine.

Enfin, la France continuera de promouvoir la mise en œuvre de « mesures de confiance » appliquées à la conduite des Etats dans le cyberespace (répertoire de points de contact, échange sur les doctrines, mécanismes de désescalade, etc.), telles qu'elles sont aujourd'hui conçues dans un cadre régional (OSCE) ou onusien.

- Consolider le rôle de chef de file constructif et inclusif de la France dans les négociations internationales sur la sécurité du cyberespace en faisant aboutir la création du programme d'action cyber à l'ONU.

Action structurante 36. Expliciter publiquement la posture de la France en matière de comportement responsable dans le cyberespace

La France reconnait que le droit international, et notamment la Charte des Nations unies et le droit international humanitaire, s'applique pleinement au cyberespace et qu'il est suffisant pour encadrer les activités en temps de paix et en contexte de conflit armé.

Cet effort de transparence sera poursuivi dans le prolongement des efforts engagés par le ministère des armées, qui a d'ores et déjà publié son analyse de l'application du droit international aux opérations cyber ainsi que des éléments de doctrine en matière de lutte informatique offensive (LIO).

La publication d'un tel corpus doctrinal contribuera à une pluralité d'objectifs - prévention, signalement et communication sur nos intentions, réduction des risques d'incompréhension ou d'escalade non maîtrisée – visant tous à renforcer la stabilité du cyberespace. Outre les modalités d'application du droit international, seront notamment explicités :

- **les principes qui régissent l'élaboration de stratégies gouvernementales de réponse aux cyber-attaques**, qui reposent sur quatre principes structurants : la souveraineté (préserver la liberté d'appréciation, de décision et d'action de la France), la légitimité (garantir la liberté d'action de la France, la maîtrise de l'engagement et le respect du droit international), la proportionnalité (accorder la primauté à la désescalade et au règlement pacifique des différends) et la stabilité (promouvoir l'approche française visant à renforcer la stabilité et la pacification du cyberespace) ;
- **les principes qui guident le processus d'attribution d'une attaque**, lequel consiste, pour l'autorité politique, à reconnaitre la responsabilité du commanditaire d'une cyberattaque et à agir en conséquence. L'attribution porte sur des cyberattaques qui visent essentiellement, mais non exclusivement, des victimes françaises. La France peut agir sur une base purement nationale ou de concert avec ses partenaires. Elle étudiera par ailleurs les sollicitations de ses partenaires et les possibilités en matière attribution coordonnée.
- **l'engagement de la France en matière de gestion coopérative des incidents cyber au niveau international**, et notamment les modalités de la mise en œuvre de la diligence requise (*due diligence*) dans le cyberespace ;
- **les modalités d'usage responsable de capacités cyber-offensives détenues par la France.**

Les travaux doctrinaux se poursuivront au niveau national sous l'autorité du SGDSN afin de d'élaborer de nouvelles normes, notamment s'agissant de la régulation des acteurs privés.

Enfin, la France soutiendra l'élaboration d'une posture européenne sur l'application du droit international dans le cyberespace.

▸ Expliciter publiquement les paramètres qui font de la France une puissance cyber responsable

Action structurante 37. Renforcer la régulation « multi-acteurs » du cyberespace

L'Appel de Paris pour la confiance et la sécurité dans le cyberespace

Lancé le 12 novembre 2018 par le président de la République, fédère plus de 1200 acteurs autour de neuf principes fondateurs pour promouvoir un cyberespace ouvert, sûr, stable, accessible et pacifique. Le Forum de Paris sur la Paix, qui assure depuis 2022 le Secrétariat de l'Appel de Paris, anime aujourd'hui la communauté d'acteurs membres de l'Appel. Cette plateforme d'échange et de réflexion alimente et interagit avec les négociations internationales visant à faciliter l'émergence d'un cadre de comportement responsable au service de la paix et la sécurité dans le cyberespace. En particulier, l'Appel de Paris a joué un rôle pionnier dans l'élaboration d'une régulation autour de sécurité des produits numériques ou encore du phénomène de « cyber mercenariat ».

Avec l'Appel de Paris en 2018, la France a été pionnière dans la régulation « multi-acteurs » du cyberespace, le texte mettant en lumière les responsabilités croisées entre Etats/entreprises. La France poursuivra l'animation de l'Appel de Paris, et soutiendra les initiatives internationales connexes visant à mettre en œuvre les neufs principes de cette initiative, à l'instar du Processus de Pall (cf. infra) .

Par ailleurs, la France continuera à s'investir à l'OCDE qui constitue une enceinte prénormative efficace pour définir des approches concertées sur les responsabilités des acteurs privés dans la stabilité du cyberspace.

Action structurante 38. Lutter contre la prolifération et l'usage irresponsable de capacités cyber-intrusives commerciales

Ces capacités, dont le marché est aujourd'hui en plein essor, sont susceptibles de présenter une menace pour les droits de l'Homme, notre sécurité nationale et la stabilité globale du cyberespace.

La généralisation de l'usage de telles capacités vient abaisser le seuil d'accès à l'arme cyber pour un nombre croissant d'acteurs étatiques comme non-étatiques, tout en complexifiant encore le travail d'imputation et d'attribution des cyber-attaques. Aujourd'hui largement centrées sur un objectif de surveillance, rien n'exclut que de telles capacités soient à l'avenir mobilisées dans le but de perturber ou d'endommager des systèmes d'information critiques. Enfin, l'on peut anticiper dans le futur proche une sophistication croissante de l'offre industrielle disponible, grâce notamment aux progrès effectués dans le domaine de l'intelligence artificielle.

Dans le même temps, le développement et l'usage de telles capacités permettent de couvrir certains besoins nationaux légitimes dans le champ de la sécurité nationale, comme par exemple en matière de lutte contre le terrorisme ; le développement d'une offre responsable constitue à ce titre un enjeu légitime de développement pour notre base industrielle, y compris à l'export.

▸ Le processus de *Pall Mall*

Fruit d'une initiative franco-britannique lors du Sommet bilatéral du 10 mars 2023, a été officiellement lancé lors d'une conférence co-organisée par la France et le Royaume-Uni à Lancaster House à Londres les 6-7 février 2024.

Format de concertation multi-acteurs (Etats, industrie, société civile), le processus de Pall Mall a vocation à déboucher sur des recommandations concrètes (ex : Code de conduite) à destination des Etats et de l'industrie visant à lutter contre la prolifération et l'usage irresponsable des capacités cyber-intrusives disponibles sur le marché : vulnérabilité & exploits, spyware, hacker-for-hire, etc.

Il s'agira au bilan, dans la lignée de l'Appel de Paris et sur la base d'une doctrine nationale dédiée, de s'employer au travers d'une initiative diplomatique dédiée (le Processus de Pall Mall) à clarifier au niveau international la notion de développement et d'usage responsable de ces capacités commerciales, avec pour objectif l'adoption d'un Code de conduite visant à encadrer le phénomène.

▸ Via un Code de conduite, clarifier au niveau international la notion de développement et d'usage responsable de capacités cyber-intrusives commerciales.

Action structurante 39. Promouvoir un régime efficace de coopération en matière de lutte contre la cybercriminalité dans le respect des droits humains et de la souveraineté des Etats

Dans le domaine de la lutte contre la cybercriminalité, la Convention de Budapest sur la Cybercriminalité fournit depuis 2001 un cadre complet et cohérent pour tout pays souhaitant élaborer une législation nationale solide en matière de lutte contre la cybercriminalité ; elle permet par ailleurs une coopération internationale protectrice des libertés fondamentales.

Si cette convention a été élaborée par le Conseil de l'Europe, elle est toutefois ouverte à l'adhésion de pays de toutes les régions du monde et a été ratifiée à ce jour par 66 Etats parties.

Depuis plusieurs années, un processus de négociation est en cours à l'initiative de la Russie pour élaborer une nouvelle Convention internationale contre la cybercriminalité, cette fois dans le cadre des Nations unies. Ces travaux devraient se conclure courant 2024.

La France participe à cette négociation de manière constructive afin de promouvoir les avancées réalisées dans le cadre de la Conventions de Budapest au sein du futur texte international et en veillant à la protection des droits de l'Homme et des libertés fondamentales.

‣ Veiller à ce que les négociations à l'ONU à la suite de l'initiative russe ne conduisent pas à fragiliser les bases solides jetées pas la Convention de Budapest en matière de lutte contre la cybercriminalité.

‣ **Counter Ransomware Initiative (CRI)**

En octobre 2021, les Etats-Unis ont lancé une initiative de lutte contre les rançongiciels visant à renforcer la coopération internationale en ce domaine, à travers des échanges de bonnes pratiques et la diffusion de standards internationaux. Une cinquantaine d'Etats y participent.

L'objectif est d'améliorer la lutte contre les rançongiciels par (i) le renforcement de la résilience des réseaux, (ii) la lutte contre les circuits financiers illicites, (iii) les partenariats public-privé, (iv) la « disruption » des réseaux criminels, (v) l'action diplomatique, la coopération et l'assistance internationale. La France participe activement à cette initiative et à ses groupes de travail.

Lors du Sommet organisé à Washington en 2023, les Etats membres de la CRI se sont engagés à ne pas laisser leurs institutions gouvernementales payer des rançons demandées par les acteurs usant de rançongiciels.

La France contribue activement aux travaux de la CRI, auxquels plusieurs ministères prennent part. La France s'attache dans ce cadre à promouvoir l'approche, la stratégie et les modes d'action nationaux et européens en matière de lutte contre les rançongiciels.

‣ Soutenir et participer à l'approfondissement des échanges au sein de la Counter Ransomware Initiative.

Objectif stratégique 11. Agir en allié et partenaire fiable au sein d'une communauté d'intérêt cyber à l'international

La capacité d'action de la France et sa résilience dans le cyberespace se conçoit en premier lieu dans une logique partenariale.

La France est forte d'un modèle national singulier et robuste dans le domaine cyber, sur lequel elle entend s'appuyer pour agir comme un allié et partenaire fiable, à différents niveaux.

A l'échelon européen : la France recherche le renforcement de l'autonomie stratégique de l'Union européenne (UE) en matière de cybersécurité et de cyberdéfense. Elle considère l'UE comme une organisation politique incontournable et privilégiée pour préserver notre capacité collective d'initiative et d'action, en ce qu'elle permet d'appréhender l'ensemble des facettes du sujet cyber : cybersécurité du marché intérieur et marché européen de la cybersécurité, recherche, innovation et déploiement industriel, justice et affaires intérieures, diplomatie, défense, etc.

Au niveau de l'OTAN : la France promeut une intégration efficace de la cyberdéfense dans ses différents aspects : protection technique des réseaux de l'organisation et des Alliés, conduite des opérations, compréhension de la menace. La France y veille à la complémentarité avec l'UE et ses différents leviers d'action en matière de cybersécurité et de cyberdéfense.

Avec les partenaires formant une communauté d'intérêt : la France recherche le partage d'expertise, le renforcement mutuel des capacités et le développement de coopérations avec des partenaires partageant un niveau équivalent de maturité. Ces coopérations impliquent l'ensemble des ministères dans leurs domaines respectifs. Des dialogues interministériels sont également conduits avec les principaux partenaires.

Dans ces trois cercles d'action, la France cherchera à mobiliser des partenariats au service de différents champs d'action : connaissance de la menace, prévention, protection, réponse, conduite d'opérations militaires.

Face à la montée en puissance des cybermenaces, la France s'engage à mobiliser l'ensemble de ses acteurs et à déployer des moyens conséquents pour renforcer sa posture de cybersécurité. Aussi, la France valorisera l'action de l'Union européenne et de ses Etats membres et fera la promotion de l'acquis communautaire à l'échelle internationale.

Action structurante 40. Promouvoir l'émergence d'une capacité d'évaluation autonome au service des intérêts partagés des Européens

▸ Œuvrer à la convergence d'analyse de la menace cyber au niveau européen

Le renforcement de l'autonomie stratégique de l'Union européenne (UE) en matière de cybersécurité et de cyberdéfense requiert le développement de capacités européennes autonomes en matière d'évaluation de la menace afin que l'Union et ses Etats membres soient en mesure de défendre leurs intérêts de sécurité propres en se fondant sur une analyse de la menace cyber partagée et autonome vis-à-vis de l'analyse de partenaires tiers.

Dans un contexte de dégradation de notre environnement stratégique marqué par le retour de la guerre en Europe, les chefs d'Etat et de gouvernement des Etats membres de l'Union européenne ont endossé en mars 2022, dans un document intitulé Boussole stratégique, une analyse partagée des menaces et vulnérabilités auxquels les Européens sont confrontés. Cet exercice inédit dans l'histoire de l'UE illustre l'émergence d'une culture stratégique commune et au renforcement de la cohésion des Européens, dont la guerre en Ukraine souligne toute l'importance.

En capitalisant sur cette dynamique, la France opèrera un rapprochement avec ses partenaires de confiance au niveau européen afin de rechercher des convergences d'analyse dans ce domaine, préalable au renforcement de la cohérence dans la définition et la poursuite d'objectifs stratégiques communs. Elle contribuera dans le même temps de manière adéquate aux mécanismes d'échange de renseignement au niveau européen, et soutiendra le développement de la capacité unique d'analyse du renseignement de l'UE en tant que point d'entrée unique pour les contributions apportées par les États membres en matière de renseignement stratégique

▸ Se doter d'une capacité nationale et centralisée, adossée au C4, de diffusion de l'information sur la menace cyber vers nos partenaires européens et étrangers

Dans cette optique, la France renforcera son aptitude à partager des informations et des analyses en se dotant d'une capacité centralisée, adossée au C4, de diffusion de l'information sur la menace cyber vers nos partenaires européens et étrangers. Dans le respect des prérogatives des différentes entités étatiques, qui doivent garder à leur main les échanges avec leurs partenaires respectifs de leurs éléments, cette capacité centralisée permettra de faire peser la voix de la France et de nourrir les stratégies de réponse conjointe.

Cette initiative s'intègrera dans une stratégie partenariale lisible, coordonnée et pragmatique. Au-delà de la centralisation du partage d'information vers nos partenaires, cette cellule centralisée permettra de faire émerger une capacité de productions stratégiques permettant d'opérationnaliser les stratégies de réponse conjointes avec nos partenaires étrangers, en priorité au sein de l'UE, telles que décidées dans le cadre du C4.

▸ Se doter d'une capacité nationale et centralisée, adossée au C4, de diffusion de l'information sur la menace cyber vers nos partenaires européens et étrangers

Action structurante 41. Se protéger : assurer un niveau adéquat et homogène de cybersécurité collective

Ces dernières années, la France a joué un rôle moteur dans l'élaboration par l'UE d'un cadre réglementaire innovant et ambitieux visant à assurer un haut niveau de cybersécurité dans l'Union.

Le cadre européen visant à relever le niveau de cybersécurité européen s'est vu renouvelé et renforcé grâce à l'adoption de la directive NIS2 et du règlement relatif au renforcement de la cybersécurité des institutions, agences, offices et organes européens (EUIBAs).

De plus, un premier schéma de certification de cybersécurité des produits a été adopté cinq ans après la formalisation du cadre européen de certification de sécurité (CSA), auquel viendra s'ajouter le Cyber Resilience Act (CRA), en vertu duquel les produits numériques placés sur le marché européen devront respecter un minimum d'exigences de cybersécurité.

Ce cadre est essentiel pour prévenir une fragmentation du niveau de résilience cyber entre les Etats membres et renforcer la coopération entre eux. La mise en œuvre de cette règlementation constitue une priorité pour la France, qui continuera à œuvrer prioritairement en faveur du renforcement de la cohérence et l'harmonisation des réglementations et exigences de cybersécurité au sein de l'Union.

La mise en œuvre harmonisée des principes et exigences de cybersécurité définis en commun doit d'une part concourir à relever le niveau de sécurité du tissu administratif, économique et social au sein de l'UE. Il s'agit d'autre part d'un impératif pour dynamiser, approfondir et continuer à renforcer la compétitivité du marché européen des produits et services de cybersécurité, auquel contribue le déploiement de la certification européenne de cybersécurité. Il s'agit enfin de promouvoir le modèle européen à l'échelle internationale.

Par ailleurs, la France a joué rôle moteur dans le renforcement de la coopération entre Etats membres en matière de lutte contre la cybercriminalité[16]. La France soutiendra dans le même temps le développement et la mise en application d'un cadre normatif européen au bénéfice d'une coopération internationale efficace dans la lutte contre la cybercriminalité (accès aux preuves numériques et facilitation des enquêtes, sans porter atteinte au chiffrement).

Pour sa part, l'OTAN dispose d'une politique de cyberdéfense commune depuis 2021, qui guide son action stratégique dans le domaine cyber au niveau politique (décision et communication), militaire (gestion de crise, opérations) et technique (résilience des infrastructures). A l'initiative de la France, les Alliés se sont par ailleurs dotés du *Cyber Defense Pledge*, qui vise à renforcer le niveau de résilience cyber de l'ensemble des Alliés en encourageant les efforts nationaux.

Pour prévenir toute duplication des efforts, une complémentarité UE-OTAN accrue, soutenable et durable doit être recherchée. La France promeut le développement des relations entre l'OTAN et l'UE dans le domaine cyber et veille à la bonne articulation des initiatives européennes avec les projets de l'Alliance. Elle a ainsi pour ambition de promouvoir le renforcement du pilier européen au sein de l'OTAN et d'assurer une cohérence globale du traitement des enjeux de cybersécurité et de cyberdéfense.

▸ Œuvrer en faveur du renforcement de la cohérence et l'harmonisation des réglementations et exigences de cybersécurité.

[16] dans le cadre de la plateforme européenne EMPACT (European Multidisciplinary Platform Against Criminal Threats) et auprès d'Europol et de ses services spécialisés, pilotage de plans d'actions opérationnels (OAP) sur la lutte contre les cyberattaques (CAIS) et la lutte contre les fraudes en ligne (OFS).

Action structurante 42. Se défendre collectivement et donner corps à la notion de solidarité européenne en cas de crise

Les Etats membres de l'Union européenne, comme les membres de l'Alliance Atlantique, œuvrent au développement d'un cadre de réponse commune à des attaques de grande ampleur qui toucheraient l'un ou simultanément plusieurs d'entre eux. La France continuera à œuvrer à la structuration et l'entrainement des mécanismes permettant (i) de mobiliser tous les échelons de coopération internationale, du niveau technique jusqu'au niveau politique et (ii) d'articuler ses stratégies de réponse au niveau national et son action au niveau européen/OTAN, afin d'en tirer le meilleur bénéfice.

S'agissant des cyberattaques atteignant le seuil de l'agression armée, la France reconnait l'application des clauses d'assistance mutuelle de l'UE (42-7) et de l'OTAN (article 5). La solidarité ne saurait toutefois s'appuyer sur ces seules clauses. Compte tenu des interdépendances et des enjeux de sécurité partagés avec nos partenaires européens, l'Union européenne a depuis 2017 mis en place différents réseaux de coopération afin de faciliter le partage d'information, le développement d'un référentiel commun de gestion de crise, tout comme la mise en place de mécanismes de coopération et d'entraide.

La France est pleinement déterminée à continuer à s'investir dans les enceintes de coopération et mécanismes européens de gestion de crises ainsi construits ces dernières années. Elle encouragera le partage d'informations au sein des réseaux de coopération entérinés par la directive NIS2 (CSIRT network, CYCLONE) dans lesquels elle continuera à s'impliquer de manière proactive. Ce partage d'informations devra contribuer à nourrir la culture européenne de solidarité entre Etats membres.

▸ Le réseau CyCLONe (Cyber crisis liaison organisation network)

Créé à l'initiative de la France en 2020 et institutionnalisé par la directive NIS2, le réseau CyCLONe (Cyber crisis liaison organisation network) rassemble les agences en charge de la gestion de crise cyber des 27 Etats membres de l'UE. Son objectif est double : 1/ permettre le partage d'informations sur les stratégies nationales de réponse en cas de crise cyber et 2/ coordonner la construction d'une analyse consolidée de la crise, au profit des décideurs politiques, tant au niveau national qu'européen. Le secrétariat du réseau est assuré par l'ENISA. Son président est un représentant de l'Etat membre assurant la présidence du Conseil de l'UE.

Le réseau des CSIRTs (Computer security incident response teams network) a été établi en 2017 par la directive NIS. Il regroupe les équipes de réponse à incident de chaque Etat membre de l'UE et le service de cybersécurité pour les institutions, organes et organismes de l'Union (CERT-UE). L'objectif principal du réseau des CSIRTs est de favoriser les échanges d'informations entre ses membres pour améliorer le traitement des cyberattaques. Les membres du réseau des CSIRTs s'informent quotidiennement des incidents détectés et suivis sur le territoire européen. La Commission européenne participe en qualité d'observateur et l'ENISA assure le secrétariat du réseau. Comme pour le réseau CyCLONe, le président est un représentant du trio d'Etats membres assurant la présidence du Conseil de l'UE.

Au niveau militaire, la gestion de crise pourra être facilitée par une activation du réseau des cybercommandeurs européens (CYBERCO) (niveau stratégique) ou des MILCERT (MICNET).

▸ Le réseau MICNET (Military computer emergency response team operational network)

Le réseau MICNET est le pendant militaire du réseau des CSIRT européens. Il a été créé en novembre 2022 par 18 Etats membres de l'UE, dont la France. C'est une coopération militaire,

qui vise à répondre en urgence, au niveau des ministres de la défense, à des cyberattaques. La gestion du réseau MICNET est confiée à l'Agence européenne de défense. Le COMCYBER y représente la France.

La conférence des cyber commandeurs européens (le CYBERCO) a été créé en 2022 à l'initiative du COMCYBER. Il rassemble toutes les plus hautes autorités militaires de cyberdéfense des pays membres deux fois par an, sous l'animation du président du conseil de l'Union européenne. L'objectif du réseau est de créer des relations de confiance, échanger sur la menace cyber ainsi que sur des problématiques opérationnelles de cyberdéfense des nations.

Au niveau judiciaire, la France pourra formuler des stratégies de coopération pour favoriser la collecte de la preuve numérique et la judiciarisation des actions de cyber-guerre. Au niveau diplomatique, la France pourra s'appuyer sur la « boite à outils » cyber-diplomatique de l'UE.

La boîte à outils cyberdiplomatique de l'UE a été mise en place en juin 2017. Il s'agit d'un cadre, qui a pour objectif de développer une réponse diplomatique conjointe aux actes de cybermalveillance. Cette boîte à outils comporte cinq volets : des mesures préventives, par exemple des actions de renforcement capacitaire dans les Etats tiers ; des mesures coopératives, par exemple des dialogues politiques avec des Etats tiers ; des mesures de stabilité, par exemple des actions de sensibilisation dans les Etats tiers ; des mesures restrictives, avec un régime de sanctions cyber ; et des mesures de soutien à un Etat membre victime d'une cyberattaque.

Cette solidarité se verra renforcée par la mise en œuvre du prochain règlement européen sur la solidarité cyber, adopté en première lecture par le Parlement européen en avril 2024, qui prévoit en particulier la création d'une Réserve cyber européenne et la concrétisation d'un cadre européen de certification des prestations de services de cybersécurité, notamment en matière de réponse à incident.

▸ La Réserve cyber européenne

Composée d'entreprises privées dont les services feront l'objet d'une certification, la Réserve cyber européenne pourra être activée rapidement en cas de cyberattaque d'ampleur et de dépassement capacitaire d'un Etat membre ou d'une institution de l'Union européenne. La France, qui a activement soutenu la création de cette réserve et plaidé en faveur de son déploiement au bénéfice des Etats de la Communauté politique européenne (CPE), participera de manière volontariste à sa mise en place. Elle veillera à ce que le budget alloué à la Réserve soit à la hauteur de l'enjeu et veillera à la bonne articulation entre la réserve cyber et le mécanisme d'assistance mutuelle otanien VCISC (Virtual Cyber Incident Support Capability). Le VCISC peut être activé à la demande d'un Allié de l'OTAN victime d'une cyberattaque. Le cas échéant, le secrétariat du VCISC, confié au Secrétariat international de l'OTAN, transmet la demande aux autres membres de l'Alliance (ANSSI, COMCYBER et MEAE pour la France) et met en relation le demandeur et les Alliés disposant de ressources pour y répondre.

La France s'attachera à mobiliser ses entreprises et encouragera ses partenaires européens à faire de même, pour que ces instruments contribuent au développement d'une capacité industrielle cyber européenne.

Enfin, la France soutiendra une approche ambitieuse en matière de préparation à la gestion de crises, en soutenant la réédition d'exercices du même type que l'exercice EU-CyCLEs organisé sous présidence française du Conseil de l'Union européenne, dont l'objet portait sur la bonne

articulation entre les communautés techniques, opérationnelles, stratégiques et politiques en cas de crise.

- Développer les capacités européennes de solidarité, de gestion de criseet de partage au sein des réseaux de coopération UE.

Action structurante 43. Conduire en coalition des opérations militaires dans le cyberespace

Les opérations dans le cyberespace représentent le versant numérique des opérations militaires, auxquelles elles sont pleinement intégrées. La France, comme pour toutes ses opérations militaires, place son action dans le cyberespace dans le cadre du droit national et international.

Si la conduite des opérations militaires dans le cyberespace relève d'une action souveraine, ces opérations participent à la solidarité stratégique et sont susceptibles de s'inscrire dans une logique de coalition.

La France veillera à soutenir l'intégration de la cyberdéfense dans les opérations et missions de l'UE et de l'OTAN. Elle veillera ainsi à renforcer la coordination et l'interopérabilité des forces via une coordination accrue (ex : réseau Cyberco ou MICNET) et des exercices conjoints (ex : Cyber Coalation de l'OTAN - Cydef-X).

Enfin, elle cherchera également à développer des modes d'actions conjoints et des opérations conjointes avec des partenaires sélectionnés dans l'ensemble des domaines de lutte informatique. La politique partenariale du COMCYBER est ainsi conduite par la recherche de synergies ou de complémentarité dans les capacités ou la connaissance de l'adversaire.

Objectif stratégique 12. Améliorer le niveau de cybersécurité à l'échelle internationale : organiser l'assistance structurelle et opérationnelle vis-à-vis de nos partenaires

Dans un espace de conflictualité en partie immatériel où les attaquants se jouent des frontières, le renforcement de notre résilience nationale requiert un effort de renforcement global des capacités de cyberrésilience collective, en cohérence avec le positionnement de la France comme puissance responsable et solidaire. Deux domaines d'actions sont envisagés en matière d'assistance internationale.

Des actions en matière de coopération structurelle (ou « capacity building » selon la terminologie internationale), dont le but est d'agir dans une vision de long terme sur les structures du partenaire, en favorisant sa montée en puissance par le biais notamment de la formation, du conseil (structures, organisations, formations) et de l'aide logistique.

Des actions en matière de coopération opérationnelle, dont la vocation est d'appuyer un partenaire par des opérations ponctuelles, soit sur un plan préventif (ex : audit des systèmes d'information), soit sur un plan réactif (ex : réponse à incident). Sur le plan militaire, le COMCYBER continuera de développer des partenariats de long terme, dits « Partenariat Cyber Agiles » (ou *Tailor Cyber Partnership - TCP*), qui permettent d'appuyer les forces armées de pays partenaires dans le développement de leur capacité cyber et dans les phases de réponse à incident.

Ces actions seront proposées à nos partenaires sans que la France ne se substitue aux prérogatives et aux responsabilités des États ou organisations partenaires. Le développement d'une telle offre ne saurait remettre en cause ni la souveraineté des Etats partenaires, ni leur responsabilité dans la sécurisation et la protection de leurs réseaux numériques.

Deux options de rédaction ici :

Version courte :

[La France développera une stratégie partenariale lisible, coordonnée et pragmatique, visant l'augmentation du niveau de sécurité globale et donc de la résilience de ses partenaires. Elle concentrera son action en priorité sur l'Union européenne, ainsi que sur :

- les Etats partenaires proches, et les Etats qui font face à une menace qui s'est encore récemment matérialisée par des attaques d'ampleurs, dont les répercussion pourraient être importantes sur les réseaux de l'UE et de l'OTAN et/ou sur notre sécurité nationale ;
- les Etat dans lesquels la grande disparité des capacités numérique et la croissance rapide des besoins en infrastructures numériques a contribué à l'augmentation rapide de la cybercriminalité et des menaces cyber.]

Version longue :

[La France développera une stratégie partenariale lisible, coordonnée et pragmatique, visant l'augmentation du niveau de sécurité globale et donc de la résilience de ses partenaires. Elle concentrera son action en priorité sur :

- le voisinage oriental de l'Union européenne, à savoir les Etats du partenariat oriental et les Balkans occidentaux. Les Etats de cette région font face à une menace qui s'est encore récemment matérialisée par des attaques d'ampleur, dont les répercussions pourraient être

importantes sur les réseaux de l'UE et de l'OTAN et/ou sur notre sécurité nationale. Le soutien de l'Ukraine en matière de cybersécurité et de cyberdéfense, et plus généralement celui des Etats les plus vulnérables au sein de la Communauté politique européenne, relève de cette priorité géographique.

- le continent africain dans son ensemble, notamment dans le cadre du suivi des engagements formulés lors du sommet UE-UA des 17/18 février 2022 et du dialogue cyber UE-UA qui en a découlé, en raison de nos intérêts stratégiques, de la présence forte de la Chine et de la perméabilité du continent à la cybercriminalité.
- l'espace Indopacifique, zone dans laquelle la grande disparité des capacités numériques et la croissance rapide des besoins en infrastructures numériques a contribué à l'augmentation rapide de la cybercriminalité et des menaces cyber. La France s'appuiera dans la région sur ses partenaires privilégiés, au premier rang desquels le Japon et l'Inde, avec lesquels elle mène des dialogues cyber réguliers, afin de déployer des actions conjointes de renforcement capacitaire.]

Action structurante 44. Renforcer l'action de la France en matière de coopération structurelle à l'international (« capacity building »)

La France est régulièrement sollicitée par des partenaires étrangers (Etats et organisations internationales) pour renforcer leurs capacités en matière de cybersécurité et de cyberdéfense. Ces sollicitations peuvent concerner une expertise technique, des demandes d'outils ou de formation.

Répondre à ces besoins requiert de la part de l'Etat qu'il s'organise parfaitement pour développer une vision d'ensemble des actions conduites par une grande diversité d'acteurs (administrations publiques, opérateurs[17], organisations internationales, etc.), et bâtir sur le fondement de celle-ci une approche transverse, au croisement de logiques sécuritaire, d'influence et de développement, conformément aux orientations de l'Appel d'Accra.

▸ L'Appel d'Accra

Pour une aide au développement cyber-résiliente, il s'inspire du format de l'Appel de Paris, rassemble des Etats, des organisations internationales, des entreprises et des organisations de la société civile autour de quatre objectifs fondateurs du renforcement capacitaire cyber à l'international :

(i) renforcer le rôle de la résilience cyber comme un facilitateur au service du développement durable ;
(ii) faire progresser un renforcement capacitaire (capacity building) porté par la demande, efficace et durable ;
(iii) encourager des partenariats plus forts et une meilleure coordination ;
(iv) débloquer les ressources financières et les modalités de mises en œuvre.

La France a contribué à la négociation de l'Appel d'Accra et y a apporté son soutien dès son adoption à l'occasion de la conférence mondiale sur le renforcement capacitaire cyber des 29 et 30 novembre 2023.

Une organisation spécifique sera mise en place pour améliorer la coordination au sein de l'Etat et avec nos partenaires internationaux. A cet égard, la France renforcera sa participation aux mécanismes de coordination internationale dans ce domaine, de manière à mettre en cohérence son action et à développer les synergies avec les projets portés par l'UE, notamment dans le cadre de « Global Gateway », par le Conseil de l'Europe, par l'OTAN et au sein d'autres fora internationaux.

La France investira dans EUCyberNet, réseau lancé en 2019 visant à construire un réseau d'experts cyber afin de proposer des formations dans le cadre des engagements cyber de l'UE vers des partenaires extérieurs, et veillera à la bonne articulation entre les projets de l'*EU external cyber capacity building agenda* et nos propres actions de coopération.

La France travaillera avec les services de la Commission européenne et du SEAE, avec le Conseil de l'Europe et avec la Banque mondiale pour que les fonds pilotés par ces acteurs (NDICI, Banque européenne d'investissement, Mécanisme pour l'Interconnexion en Europe, …) soient mobilisés sur des projets compatibles avec nos priorités de renforcement capacitaire.

[17] Expertise France, agence interministérielle de coopération technique internationale rattachée à l'Agence française de développement ; CIVIPOL, opérateur de coopération du ministère de l'intérieur ; groupe DCI opérateur ministère des armées pour le transfert du savoir-faire des forces françaises à l'international,…

Le centre régional de développement des capacités en cybersécurité dans les Balkans occidentaux (C3BO)

Le Centre de développement de capacités cyber (C3BO) est une initiative franco-slovène, en partenariat avec le Monténégro, portée par le MEAE (Direction de la coopération de sécurité et de défense), visant à établir un centre de formation régional à Podgorica. Le Centre vise à former les administrations compétentes des six pays des Balkans occidentaux à la cybersécurité, la lutte contre la cybercriminalité et les normes internationales, tout en favorisant le dialogue régional sur ces sujets.

En activité depuis mai 2023, le Centre a vocation à devenir une organisation internationale à partir de 2025, de façon à agréger les partenariats européens et internationaux autour d'une gouvernance et d'un programme d'activités communes.

L'Etat renforcera enfin les synergies avec le secteur privé, en structurant un dialogue avec les représentants des entreprises afin de nourrir leur compréhension des enjeux et objectifs internationaux du renforcement capacitaire. Il soutiendra l'offre française en matière de cybersécurité auprès de nos partenaires via les prêts du Trésor et d'éventuels autres instruments (soutien par Business France, garanties publiques à l'export via BpiFrance par exemple), dans la limite des obligations qui s'imposent à la France quant à l'aide au développement, et en communiquant sur ces outils auprès des entreprises de cette filière.

A l'appui de cette approche, la France renforcera le détachement d'experts (Experts techniques internationaux - ETI) pour accompagner les Etats partenaires dans la durée, notamment dans les pays où l'organisation en matière de cybersécurité est embryonnaire.

Développer un plan de financement des services de renforcement capacitaire cyber mis en œuvre par l'Etat et le secteur privé et consacrer une enveloppe budgétaire ambitieuse en conséquence.

Action structurante 45. Inscrire dans des partenariats militaires de long terme une offre de services en matière d'assistance opérationnelle

L'augmentation des menaces et la sophistication croissante des cyberattaques se traduisent aujourd'hui dans le domaine cyber par une augmentation des demandes d'assistance opérationnelle émises par des pays ou organisations tiers.

La France développera ses capacités d'assistance sur mesure et en réponse à la demande explicite d'un Etat, de l'UE[18] ou de l'OTAN[19], qui souhaiterait obtenir une aide de sa part, soit en cas de crise, soit en anticipation de celle-ci.

Le COMCYBER développera notamment une capacité d'appui technique pour anticiper et réagir en cas d'incident cyber sur les réseaux militaires de l'UE et de l'OTAN.

L'efficacité de ces mécanismes d'assistance repose sur la confiance entre les pays partenaires. Il est donc nécessaire de développer des capacités d'accompagnement sur le long terme, capacités qui se doivent de rester agile afin de s'adapter aux besoins et contraintes de nos partenaire.

Ces opérations d'assistance pourront recouvrir plusieurs types d'activités opérationnelles, allant de l'anticipation et l'observation jusqu'à la collecte et l'analyse d'éléments techniques sur la menace. Elles viseront à aider nos partenaires à améliorer la défense de leurs réseaux (audits techniques, mission commune de recherche de la menace, appui à la résolution d'incident, …)

La France mettra en place un mécanisme national permettant de prioriser les réponses aux partenaires et mobiliser au mieux les différents leviers existants.

- Développer une capacité de « Partenariat Cyber Agile » (Tailored Cyber Partnership) »

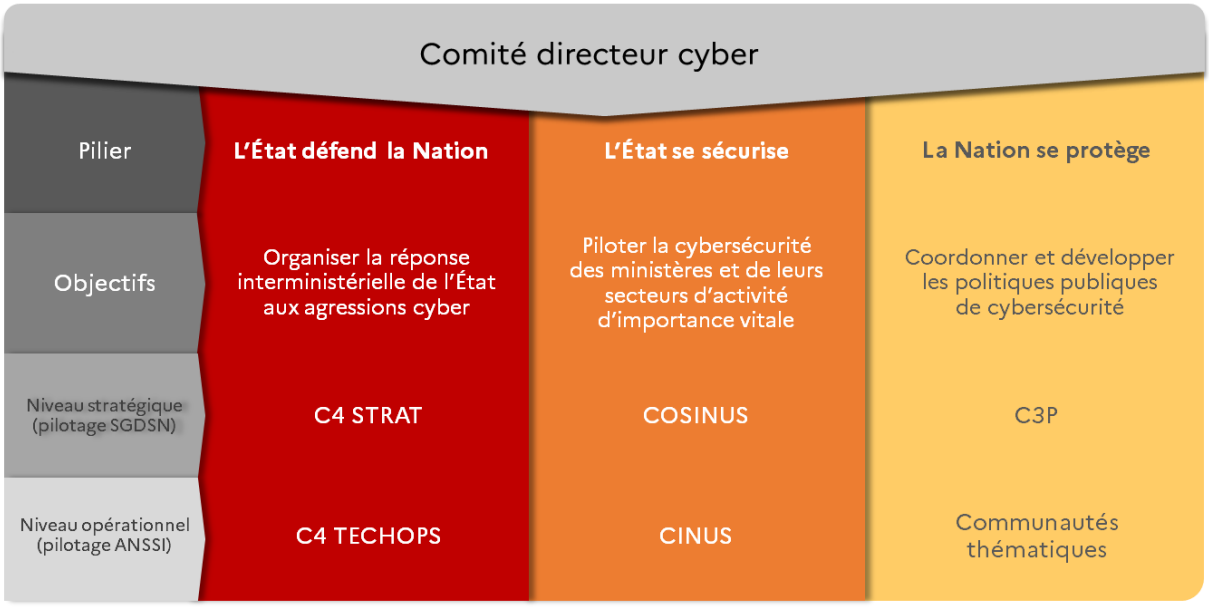
[18] dans le cadre du projet CRRT, qui vise à la création d'équipes de réponse à incident cyber pouvant porter assistance aux Etats membres, institutions européennes et missions et opérations de l'UE. La France est observatrice de ce projet.
[19] dans le cadre du Virtual Cyber Incident Support Capability (VCISC), qui consiste à réunir les nations membres volontaires au sein d'une communauté d'assistance mutuelle. Il est doté d'un secrétariat, armé par le Comité de Cyberdéfense, chargé de prendre en compte les demandes d'assistance des membres, les diffuser vers les autres membres, regrouper les offres de services et mettre en relation le demandeur et le volontaire.

METTRE EN ŒUVRE COLLECTIVEMENT CETTE STRATEGIE NATIONALE

La cybersécurité portée dans toutes les dimensions de la Nation

Le modèle d'organisation adopté par la France, garant du respect des libertés individuelles, sépare les missions et capacités défensives des missions et capacités offensives. La gouvernance mise en place permet toutefois de garantir une très forte coordination entre les pôles défensif et offensif, gage de l'efficacité de notre cyberdéfense.

La gouvernance du volet défensif, objet de la présente stratégie, s'organise ainsi autour de trois missions essentielles et s'appuie sur des instances dont le périmètre, le mode d'intervention et les participants évoluent pour demeurer en adéquation avec les nombreux enjeux de sécurité de la Nation.



Le secrétariat du CODIR et celui des trois chaînes de gouvernance sera assurée au sein du SGDSN par une équipe dédiée permanente, qui mobilisera les compétences idoines au sein de l'ANSSI.

Le Comité directeur définit les grandes orientations de l'État en matière de cybersécurité

Au niveau politique, **la stratégie nationale de cybersécurité** est décidée par le président de la République en conseil de défense et de sécurité nationale. Le **suivi de sa mise en œuvre** est assuré par le **Comité directeur cyber**.

Présidé par le Premier ministre ou son représentant, le comité directeur cyber réunit *a minima* une fois par an les cabinets ministériels concernés afin de définir les grandes orientations de l'État en matière de cybersécurité. Il alimente le Conseil de défense et de sécurité nationale (CDSN), dont il décline les instructions.

Le comité directeur cyber couvre l'ensemble des trois missions décrites ci-dessous. Il veille en particulier au déploiement de la stratégie de cybersécurité et en suit dans la durée les différents axes, qu'il actualise au besoin.

Mission « L'État défend la Nation »

Cette mission a pour objectifs la connaissance de la menace et l'élaboration de la réponse de la France aux cyberattaques.

Elle repose sur un dialogue et un partage d'informations entre services de l'État qui s'incarne dans le Centre de coordination des crises cyber (C4). Cette organe réunit les administrations concernées en charge de l'action opérationnelle permettant de détecter, caractériser, imputer les atteintes aux intérêts fondamentaux de la Nation et y répondre.

Mission « L'État se sécurise »

Cette mission consiste à assurer le pilotage du renforcement de la cybersécurité des systèmes d'information (SI) les plus essentiels à la vie de la Nation.

Il s'agit des SI de l'État et de ses établissements publics[20], ainsi que celle des SI support des activités d'importance vitale pour l'État, que ceux-ci relèvent d'opérateurs publics ou privés.

Elle veille à disposer des moyens permettant de mesurer le niveau de cybersécurité de l'ensemble des acteurs concernés et la performance des actions conduites. Elle donne à l'ANSSI les moyens d'accompagner les ministères les moins matures dans la mise en œuvre de leurs responsabilités sectorielles – en particulier vis-à-vis des opérateurs d'importance vitale (OIV).

Mission « La Nation se renforce »

Cette mission a pour objectif la coordination des politiques publiques concourant à renforcer la cybersécurité des citoyens, des entreprises, des associations et des collectivités territoriales.

L'action publique dans le champ cyber est caractérisé par une forte transversalité et requiert un pilotage interministériel renforcé, qui sera exercé par le SGDSN au travers du **Comité de pilotage des politiques publiques cyber (C3PC).**

Le SGDSN sera notamment responsable de la synthèse des investissements financiers et humains de l'Etat dans le domaine cyber, afin d'établir une planification interministérielle pluriannuelle des ressources de l'état, déclinée dans les exercices budgétaires annuels des différents ministères. Sans préjudice des responsabilités des ministères et administrations, un tel mécanisme de planification et de synthèse s'impose afin de donner au plus haut de niveau de l'Etat une visibilité sur les actions majeures portées par chaque ministère et les moyens de s'assurer de la parfaite complémentarité entre celles-ci.

Une gouvernance cyber multipartite au service d'une résilience nationale

La menace cyber concerne aujourd'hui tous les pans de notre société, de notre économie et de notre territoire. **Les secteurs professionnels, les représentants des territoires, le monde académique, la société civile sont désormais tout à la fois des victimes de la menace cyber et des partenaires incontournables dans la construction et la mise en œuvre de notre réponse à cette menace**. C'est pourquoi ces acteurs seront intégrés dans la gouvernance cyber nationale, tant à l'échelon national qu'à l'échelon territorial.

[20] tel que décrit dans l'Instruction générale interministérielle (IGI) 1337

Installer un comité stratégique externe auprès du SGDSN

Dans le cadre de son ouverture vers l'extérieur, l'État crée un comité stratégique externe pour conseiller le SGDSN dans l'exécution de la stratégie nationale de cybersécurité.

Ce comité, composé d'experts issus de divers horizons (acteurs de l'innovation, du monde de la recherche, de la société civile, etc.), apportera une expertise précieuse et un regard extérieur pour enrichir la réflexion stratégique et identifier des risques et opportunités méconnus.

Il permettra également de renforcer la légitimité de la stratégie en impliquant des acteurs indépendants et impartiaux, de faciliter la collaboration entre les secteurs public et privé, et d'assurer une continuité stratégique sur le long terme.

Ouvrir la gouvernance aux différentes aux parties prenantes

La troisième mission de la gouvernance cyber de la France vise à organiser la cyberprotection de la nation, ce que l'Etat ne peut faire seul.

Il s'agit de co-construire et de coordonner les politiques publiques concourant à renforcer la cybersécurité de la Nation, en mobilisant pleinement les acteurs concernés. Cela passe par le renforcement de la coordination interministérielle et l'association à des instances de dialogue des autres parties prenantes.

Au sein de l'Etat, cette gouvernance se matérialisera au travers d'un Comité de pilotage des politiques publiques (C3P). Sous la tutelle du SGDSN et réunissant les ministères, il assurera le suivi des priorités définies par la stratégie. Il sera décliné en comités spécialisés dédiés à ces priorités. Des instances de dialogue avec le secteur privé, le monde académique et la société civile seront institués à ces différents niveaux.

Faire des territoires un maillon fort de cette gouvernance

A l'instar du réseau des CSIRT régionaux qui s'est constitué ces dernières années, les acteurs territoriaux jouent un rôle essentiel dans la construction d'une résilience cyber de la Nation. Or, ils sont encore insuffisamment entendus dans la gouvernance cyber du pays.

La refonte de cette gouvernance passera ainsi par l'institutionnalisation de ce dialogue et le pilotage territorial au travers d'un comité, sous l'égide du C3P, qui réunira acteurs des territoires, autorité nationale et ministères concernés.

Cette gouvernance se déclinera également au niveau territorial sous l'impulsion des représentants de l'État.

Optimiser le pilotage des politiques publiques de cybersécurité

Sans connaissance fine des composantes de notre résilience cyber et de leur évolution, l'impact des actions portées dans cette stratégie sera difficilement mesurable. Aussi, il est nécessaire de consolider notre connaissance du niveau de résilience cyber de la nation. Il est aussi nécessaire que cette connaissance ne soit pas retenue par l'Etat mais infuse largement notre tissu économique et notre société, afin qu'elle puisse être pleinement exploitée au bénéfice de notre résilience générale.

Créer un observatoire national afin de suivre dans le temps le niveau de résilience de la nation

Il existe aujourd'hui une multitude de « données cyber », dispersées au sein de l'écosystème national (Etat, collectivités, société civile, acteurs économiques privés, etc.). L'incidentologie en est un exemple marquant avec la multiplication de rapports dédiés non agrégés.

Certaines données n'existent également pas aujourd'hui et sont à construire. Ce rôle de conception et d'agrégation de données sera confié à un observatoire de la cybersécurité, qui dans sa gouvernance réunira les acteurs producteurs et utilisateurs des données.

Au regard de son positionnement transversal, et en tant que première source de cette connaissance, l'ANSSI sera chargée de mettre en place cet observatoire, en coordination avec les ministères et dans une logique partenariale public-privé.

Rendre accessible cette connaissance cyber au plus grand nombre

Au-delà de l'intérêt pour le pilotage des politiques publiques, cette base de connaissance doit être mise à la disposition du plus grand nombre (acteurs du marché cyber, chercheurs…), dans une logique d'open data.

Cela passera par une double approche : l'accès à des données « brut », en format API, et l'accès à des données consolidées au travers d'indicateurs et d'études construits par l'observatoire.