RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

STRATÉGIE NATIONALE DE CYBERSÉCURITÉ 2026 — 2030

PRÉFACE

Il est des ruptures silencieuses qui bouleversent l'ordre du monde plus sûrement que les fracas de l'histoire. La révolution numérique est de celles-là.

À l'heure où nos vies, nos économies, nos démocraties se tissent à travers les réseaux et les algorithmes, où la frontière entre la souveraineté et la dépendance peut se jouer à une ligne de code, la cybersécurité est devenue une condition de la liberté. Une exigence vitale. Un impératif stratégique.

Car l'espace numérique est désormais un théâtre de puissance, reflet et relai des affrontements physiques. Un lieu où luttent les nations, les intérêts, les idéologies. Un champ d'opérations où se décident, souvent sans bruit, des batailles décisives pour l'indépendance de nos États, la sécurité de nos citoyens, et la solidité de nos institutions.

La France ne saurait y être spectatrice. Elle y sera, avec force, avec méthode, avec ambition, une puissance souveraine.

Cette stratégie nationale de cybersécurité 2026-2030 fixe notre cap. Elle prolonge et concrétise les orientations de la Revue nationale stratégique, pour faire de notre pays un pôle majeur de la cybersécurité mondiale.

Nous formerons des milliers de talents, car la guerre de demain se gagne dès aujourd'hui, sur les bancs de l'école, dans les laboratoires, dans les start-ups et les campus. Nous protégerons nos infrastructures, nos entreprises, nos collectivités, en conjuguant innovation et régulation, audace et vigilance.

Nous renforcerons notre capacité de résilience aux chocs d'un monde de plus en plus fragmenté, en préparant l'ensemble de la nation – acteurs publics comme privés – à affronter les crises, à en limiter l'impact, à en sortir plus forts.

Et nous découragerons les attaques, en affirmant une doctrine claire, crédible, respectueuse du droit international, mais apte à défendre nos intérêts avec fermeté et efficacité.

Nous ne le ferons pas seuls. Ce combat pour la souveraineté est celui de l'Union Européenne tout entière. Il appelle des coopérations accrues, une mutualisation des savoir-faire, un agenda industriel ambitieux. Ensemble, Européens, nous devons construire un cyberespace sûr, ouvert et démocratique, fidèle à nos valeurs.

C'est pourquoi je veux saluer ici l'engagement de toutes celles et ceux – agents publics, techniciens, ingénieurs, chercheurs, combattants numériques, entrepreneurs – qui font vivre au quotidien cette stratégie. Leur mission exigeante, souvent invisible, est essentielle à notre avenir.

Le XXI^{e} siècle est d'ores et déjà un siècle du numérique ; avec chacun d'entre vous, il nous revient d'en faire un siècle de confiance et de liberté.

Emmanuel Macron

SOMMAIRE

Une menace qui s'intensifie

La numérisation des usages est le vecteur de nombreux bénéfices pour les Français, tant dans leur vie professionnelle, personnelle que citoyenne, et pour les entreprises pour lesquelles elle représente un facteur d'innovation et de développement de nouvelles perspectives d'affaires. En tissant une toile complexe d'interconnexions et en générant une dépendance accrue à des infrastructures critiques, la numérisation a cependant profondément bouleversé les fondements de la société et expose des pans entiers de la vie quotidienne des citoyens et des organisations à des attaques informatiques d'une sophistication croissante.

Le cyberespace est devenu un espace de compétition, de contestation et parfois même d'affrontement désinhibé, en miroir des tensions géopolitiques et des rivalités internationales.

La France est confrontée, à l'instar de nombreux pays à travers le monde, à une cybermenace intense, étendue à tout le tissu économique et social – que celle-ci émane d'États, de cybercriminels ou d'activistes ou soit le fait d'une combinaison d'actions de ces différents acteurs.

Qu'elles soient motivées par des considérations économiques, politiques, militaires ou idéologiques, ces cyberattaques peuvent causer des dommages considérables, perturbant le fonctionnement de la société et menaçant la sécurité nationale. Elles peuvent également avoir des répercussions économiques importantes pour les victimes, entraînant des pertes financières considérables et perturbant les chaînes d'approvisionnement.

De l'espionnage au sabotage, en passant par l'extorsion et la subversion, cette pression permanente prend une multitude de formes. Elle se matérialise notamment par l'essor d'un marché de la cybercriminalité et la prolifération d'outils cyber-intrusifs.

Elle s'exerce sur l'ensemble des infrastructures numériques, jusqu'aux plus critiques, à l'instar des services de *cloud* hébergeant une part croissante des données sensibles et des applications critiques. L'essor des technologies de rupture telles les systèmes d'intelligence artificielle ou l'émergence potentielle d'un ordinateur quantique capable de mettre en défaut les mécanismes actuels de sécurité cryptographique, largement déployés pour sécuriser les infrastructures numériques, amplifie ces risques.

La vision stratégique de la France

Face aux défis majeurs que constitue cette menace, la France s'est résolument engagée depuis plus d'une décennie à renforcer sa cybersécurité. Ce domaine est une priorité nationale.

Depuis 2008 et la publication du *Livre blanc sur la défense et la sécurité nationale*, la vision stratégique française de la cybersécurité s'est consolidée et a permis de doter la France d'une forte culture en ce domaine et d'élever progressivement son niveau de résilience cyber. Elle a posé les bases d'un modèle national, solide et reconnu internationalement, séparant les missions défensives et offensives de cyberdéfense.

Cet élan, matérialisé par la *Revue stratégique de cyberdéfense* de 2018 et soutenu par une forte dynamique d'investissements publics, permet à la France de disposer aujourd'hui d'une ressource humaine qualifiée, de capacités de recherche d'excellence, d'une filière économique de pointe, d'un écosystème étoffé d'acteurs publics et privés engagés dans la cybersécurité, et de capacités défensives et offensives lui permettant d'assurer la préservation de ses intérêts et sa place au niveau international.

Toutefois, les évolutions de la menace cyber rendent nécessaire l'élaboration d'une nouvelle stratégie nationale de cybersécurité pour adapter les capacités de la France à ce nouveau contexte. Le pays fait désormais face à un *continuum* d'agressions cyber plus fortement imbriquées, mêlant acteurs étatiques et cybercriminels dans un contexte géopolitique plus instable.

La stratégie nationale de cybersécurité s'inscrit en déclinaison de la *Revue nationale stratégique* qui fixe pour la France l'ambition d'une résilience cyber de premier rang. Elle développe une approche structurée autour de cinq piliers pour atteindre cette ambition d'ici 2030 :

PILIER 1 | FAIRE DE LA FRANCE LE PLUS GRAND VIVIER DE TALENTS CYBER D'EUROPE

PILIER 2 | RENFORCER LA RESILIENCE CYBER DE LA NATION

PILIER 3 | ENTRAVER L'EXPANSION DE LA CYBERMENACE

PILIER 4 | GARDER LA MAITRISE DE LA SECURITE DE NOS FONDEMENTS NUMERIQUES

PILIER 5 | SOUTENIR LA SECURITE ET LA STABILITE DU CYBERESPACE EN EUROPE ET A L'INTERNATIONAL

Les voies et moyens seront précisés et déclinés dans les feuilles de route que chacun des ministères et services concernés doivent consolider sous six mois. Leur mise en œuvre sera régulièrement suivie au niveau interministériel.

PILIER 01

FAIRE DE LA FRANCE LE PLUS GRAND VIVIER DE TALENTS CYBER D'EUROPE

La **capacité de la France à développer et attirer les talents dans les domaines de la cybersécurité** est la condition *sine qua non* pour atteindre une résilience cyber de premier rang. C'est pourquoi cette ambition constitue l'axe prioritaire au cœur de cette stratégie.

Le secteur du numérique en général, et celui de la cybersécurité en particulier, connaissent une pénurie de main-d'œuvre à l'échelle mondiale. Ce phénomène est aggravé par une insuffisante orientation professionnelle constatée des profils issus de milieux sociaux défavorisés, d'une part, et féminins, d'autre part, vers les domaines de l'informatique, pourtant en croissance rapide et continue depuis de nombreuses années.

Face à cette pénurie, ce pilier vise à investir massivement pour orienter vers ces métiers dès le plus jeune âge et soutenir les plans de formation et d'attractivité en ce domaine. En association étroite avec le secteur privé, la France mettra en œuvre une politique ambitieuse de ressources humaines qui visera à faire de la France un grand vivier de talents cyber.

OBJECTIF 1
Développer dès le plus jeune âge une culture inclusive de la cybersécurité

La jeunesse est l'avenir de la nation et donc le socle de la résilience collective du pays. Cet objectif répond à ce titre à un double enjeu : diffuser dès le plus jeune âge une culture de la cybersécurité et créer le vivier de talents de demain.

Des préjugés tenaces – « un métier masculin, solitaire, d'essence technique et exclusivement accessible à un haut niveau d'études » – freinent l'attractivité de ce domaine porteur. La France s'attachera ainsi à conduire des actions ambitieuses afin d'attirer vers les métiers de la cybersécurité des profils pour lesquels sont aujourd'hui constatés des freins dans cette orientation.

Ces efforts seront entrepris dans le champ éducatif et dans le champ culturel. Ils se matérialiseront notamment par des dispositifs ciblés de soutien pour les études et par un programme de mentorat spécifique pour les jeunes filles, en capitalisant sur le retour d'expérience des initiatives existantes. La France intégrera également la cybersécurité dans ses dispositifs d'engagement civique à destination de la jeunesse.

OBJECTIF 2
Investir dans tous les pans de la formation en cybersécurité

Pour valoriser les formations et les métiers de la cybersécurité, la France créera une plateforme nationale pour l'orientation vers ces métiers en faisant converger les efforts entrepris par les acteurs publics et privés du secteur.

Face à un domaine en constante évolution, la France soutiendra également le développement de la formation continue des professionnels de la cybersécurité et des programmes de reconversion vers les métiers de la cybersécurité. Dans cette perspective, la France encouragera les filières du numérique et de la cybersécurité françaises et européennes à développer leur offre de formation.

Par ailleurs, pour toucher l'ensemble du tissu social, le développement d'outils d'auto-formation (MOOC, etc.) aux enjeux de sécurité numérique sera favorisé.

Enfin, pour pérenniser la place centrale de la cybersécurité dans le paysage scientifique et technologique français et européen, la France mettra en œuvre des "stratégies passerelles" entre différentes disciplines scientifiques et technologiques cyber et non cyber. Ces passerelles permettront de favoriser la fertilisation croisée des expertises, renforçant ainsi la position de la France et de l'Union européenne (UE) dans ce domaine stratégique. Les parcours au sein du secteur public et entre le secteur public et le secteur privé seront également encouragés.

OBJECTIF 3
Soutenir la dynamique des ressources humaines cyber au niveau européen

La France accompagnera l'émergence d'un socle commun de compétences de cybersécurité au niveau européen pour soutenir les capacités européennes de cybersécurité et favoriser la collaboration entre les Etats membres.

Dans cette perspective, elle encouragera la création de cursus de formation harmonisés et reconnus dans tous les pays de l'UE, ainsi que la mobilité de professionnels au sein des institutions européennes et entre les Etats membres.

PILIER 02

RENFORCER LA RESILIENCE CYBER DE LA NATION

Depuis le *Livre blanc sur la défense et la sécurité nationale*, la résilience est définie 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 majeure, puis à rétablir rapidement leur capacité de fonctionner normalement, ou à tout le moins dans un mode socialement acceptable. La guerre d'agression de la Russie en Ukraine témoigne de ce besoin vital pour un pays d'une préparation collective face à des attaques d'ampleur, y compris dans le champ de la cybersécurité. La nature des cyberattaques susceptibles d'affecter la France dans les prochaines années appelle au renforcement de la résilience cyber de la nation.

Face à une menace qui touche désormais tous les pans de l'économie et de la société, la France déploiera un plan ambitieux pour élever le niveau général de cybersécurité de l'ensemble du tissu économique et social, dont le socle informatique de l'Etat, et entrainer la nation à réagir aux crises créées par des cyberattaques. Ce plan reposera sur une synergie renforcée entre l'Etat, les collectivités territoriales, les entreprises, les acteurs de la recherche et de la société civile.

OBJECTIF 4
Préparer la Nation aux crises dues aux cyberattaques

Pour atteindre une résilience collective, il faut que la conscience des menaces et des risques induits soit partagée et entretenue dans la durée. Pour ce faire, la France amplifiera sa politique de prévention et de sensibilisation aux risques de cybersécurité. Cette politique reposera notamment sur une marque nationale de prévention du risque numérique pour porter des campagnes de sensibilisation, sur le modèle des campagnes de la prévention routière.

La France renforcera également sa préparation et sa capacité de réaction face à des cyberattaques multiples et à la crise systémique qui en résulterait. Elle diffusera notamment à l'ensemble du tissu économique et social une culture de la gestion de crise cyber accessible à tous. Un programme d'exercices de crise sera développé afin d'éprouver l'articulation et l'efficience de l'ensemble des capacités de réponse de la France. Cette démarche se déclinera au niveau territorial, sectoriel, national, européen et international. La France intégrera au cœur de sa planification et de ses investissements l'enjeu capacitaire, avec la possibilité de recours à de nouvelles capacités de réponse publiques et privées.

OBJECTIF 5
Rehausser le niveau global de cyber-protection de la Nation

Le rehaussement du niveau de cyber-protection reposera sur une approche proportionnée. Les services et infrastructures les plus vitaux de la nation, à commencer par ceux de l'État et de ses opérateurs critiques, continueront d'être portés à un niveau de sécurité très élevé, apte à résister aux menaces les plus sophistiquées. Il s'agira notamment de consolider le socle numérique mutualisé de l'Etat et d'y concentrer d'importants efforts de cybersécurité.

La France déploiera par ailleurs des obligations proportionnées de cybersécurité auprès d'un périmètre étendu d'entités, en cohérence avec les exigences prévues par la directive européenne NIS2[1]. Dans cette perspective, la France mobilisera de manière accrue les représentants publics et privés des secteurs réglementés en tant que relais de ce changement d'échelle pour accompagner les entités soumises à cette réglementation. Elle soutiendra aussi des programmes d'accompagnement à la cybersécurité pour les entités les moins matures en termes de cybersécurité.

Cette approche sera enfin complétée par des démarches d'incitation à l'attention de l'ensemble des autres entreprises, collectivités et associations, qui seront encouragées à élever leur niveau de sécurité à un niveau suffisant pour résister à des attaques de moindre sophistication. Un label de confiance sera mis en œuvre pour permettre à ces acteurs de valoriser leurs efforts de sécurisation auprès de leurs partenaires, clients, investisseurs.

OBJECTIF 6
Faciliter les parcours vers une meilleure cybersécurité

Pour rendre la cybersécurité plus accessible, la France mettra en œuvre une démarche de simplification du cadre normatif et soutiendra son harmonisation au niveau européen et international.

Afin d'accompagner un large public, un portail national de la cybersécurité du quotidien sera créé pour offrir aux différents publics, en particulier les citoyens, une information claire, les aiguiller vers les dispositifs à leur disposition et les guider dans leurs démarches relatives à la cybersécurité. La France soutiendra également le développement d'une offre de services et de produits de cybersécurité accessible et adaptée aux différents acteurs. Elle valorisera cette offre à travers les nombreux relais sectoriels et territoriaux de la cybersécurité.

La France instaurera enfin un parcours d'accompagnement fluide et adapté au statut ou à la nature de chaque victime, en y associant les acteurs de l'accompagnement aux victimes au niveau national et dans les territoires, et en particulier les centres de réponse à incident sectoriels et territoriaux. Dans cette perspective, la plateforme 17Cyber constituera le guichet grand public des individus et entités victimes de cybermalveillance, au-delà des entités soumises à une réglementation cyber particulière, et sera directement intégrée au portail national.

[1] Directive européenne sur la sécurité des réseaux et des systèmes d'information.

PILIER 03

ENTRAVER L'EXPANSION DE LA CYBERMENACE

La France est confrontée à une menace d'attaques informatiques croissante 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 grandissante 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 la pression et du niveau de sophistication d'opérations d'espionnage, de déstabilisation et de sabotage visant des intérêts fondamentaux de la Nation.

La France est déterminée à entraver l'expansion de cette cybermenace. Elle mobilisera l'ensemble des leviers d'action à sa disposition pour augmenter significativement le coût financier, humain et réputationnel pour ses adversaires potentiels qui pourraient nuire à son économie, à la stabilité de sa démocratie, ou à la sécurité des biens et des personnes sur son territoire, et pour les décourager de s'en prendre à la France et à ses partenaires.

OBJECTIF 7
Activer l'ensemble des leviers pour décourager les agressions cyber

La France est déterminée à enrayer la dynamique de développement de la cybermenace. Elle mobilisera de manière coordonnée l'ensemble des leviers à sa disposition – judiciaires, techniques, diplomatiques, militaires, économiques – pour accroître les coûts et les risques pour ceux qui portent atteinte à son économie, à ses institutions démocratiques ou à la sécurité de ses citoyens.

Cette orientation inclut une meilleure mobilisation du levier des sanctions, de la capacité d'entrave offerte par les capacités nationales cyberoffensives dans le strict respect du droit international, des capacités de recueil de renseignement (y compris financier) ainsi qu'un renforcement de la réponse judiciaire.

Sous l'égide du Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), le Centre de coordination des crises cyber (C4), composé de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), du Commandement de la cyberdéfense (COMCYBER), de la Direction générale de l'Armement (DGA), de la Direction générale de la Sécurité extérieure (DGSE), de la Direction générale de la Sécurité intérieure (DGSI) et du Ministère de l'Europe et des Affaires étrangères, joue actuellement un rôle central dans la réponse à une cyberattaque. En rassemblant désormais, au-delà de ce seul cercle, l'ensemble des acteurs de l'Etat capables de mobiliser un levier de réponse à une cyberattaque, il assurera une activation plus large des moyens de réponse les plus pertinents et proposera des options à l'autorité politique – l'attribution publique en fera partie.

Enfin, la France renforcera la coordination avec ses partenaires européens et soutiendra pleinement la mise en œuvre de la boîte à outils cyber-diplomatique de l'Union européenne, notamment son régime de sanctions.

OBJECTIF 8
Mobiliser les acteurs privés dans la cyberdéfense de la Nation

Internet repose sur des opérateurs privés qui, par leur position, jouent un rôle structurant dans la cybersécurité globale. En partenariat avec ces acteurs, la France mettra en place un ensemble de mesures de protection pour détecter et caractériser au plus tôt les attaques, et éventuellement les bloquer.

La France déploiera également un filtre de cybersécurité à destination du grand public, visant à prévenir l'accès aux sites web malveillants.

La France renforcera en outre le partage d'informations techniques sur les menaces entre les services de l'Etat et les acteurs privés. Cette mise en réseau reposera en particulier sur le développement de l'InterCERT France, première communauté de centres de réponse à incident en France, dans son rôle fédérateur. La France agira également pour renforcer ce partage aux niveaux européen et international pour amplifier son effet.

PILIER 04

GARDER LA MAITRÎSE DE LA SÉCURITÉ DE NOS FONDEMENTS NUMÉRIQUES

Le fonctionnement de l'économie et de la société repose sur un ensemble de technologies numériques essentielles, telles que les réseaux de communication, les systèmes d'exploitation, le *cloud* et les applications logicielles. Ces technologies sont la cible de cyberattaques et leur vulnérabilité peut avoir des conséquences graves et durables dans les infrastructures numériques de la Nation.

La France se fixe une ambition claire de maitriser ses dépendances technologiques et de conserver son autonomie d'appréciation et sa liberté d'action dans le cyberespace. Pour cela, elle pérennisera et développera sa maîtrise de technologies critiques de cybersécurité et de capacités autonomes d'évaluation, et soutiendra la consolidation d'acteurs industriels cyber de premier rang mondial au niveau européen.

Cet effort reposera sur la poursuite des investissements de l'Etat en matière d'innovation dans le cadre du plan France 2030, et sur un dialogue renforcé entre les parties prenantes – acteurs de la recherche et de l'innovation, filières économiques, acteurs du financement et pilotes de la politique publique industrielle – afin de mobiliser l'ensemble des leviers de politique industrielle et d'orienter au mieux les investissements financiers.

OBJECTIF 9
Investir dans la sécurité des technologies numériques

La France accompagnera les fournisseurs dans la mise en œuvre du règlement européen sur la résilience cyber (*Cyber Resilience Act* – CRA), qui étend les exigences essentielles de cybersécurité à l'ensemble des produits numériques. Elle renforcera à cette fin sa politique nationale de gestion coordonnée des vulnérabilités, en concertation avec les acteurs concernés, et soutiendra de meilleures pratiques de développement logiciel ainsi que la recherche sur la sécurité des produits *open source*.

Elle investira également dans la recherche sur les risques et opportunités liés aux technologies de rupture. Pour l'intelligence artificielle, cette action s'appuiera notamment sur l'Institut national de l'évaluation et de la sécurité de l'intelligence artificielle (INESIA). La France soutiendra en parallèle un plan de transition vers la cryptographie post-quantique aux niveaux national et européen.

Dans le domaine du *cloud*, elle accompagnera les secteurs public et privé dans leur migration, en adoptant une approche proportionnée à la sensibilité des données et des systèmes d'information concernés. Elle poursuivra son soutien à l'émergence d'une offre de cloud de confiance et promouvra cette approche proportionnée au niveau européen.

L'identité numérique, levier majeur contre la cybercriminalité de masse, fera l'objet d'une attention particulière. La France encouragera la mise à disposition de moyens d'identification de confiance pour les particuliers et les organisations, et leur usage généralisé. Elle soutiendra

également l'harmonisation des exigences de sécurité dans le cadre du portefeuille européen d'identités numériques.

Enfin, elle établira les conditions favorables à un renforcement de la prise en compte de la cybersécurité dans l'ensemble des filières industrielles. Cela passera notamment par l'intégration de critères de cybersécurité dans les dispositifs d'aides de l'État, à l'instar de France 2030 ou encore un dialogue renforcé avec le Conseil national de l'Industrie sur l'intégration dans les contrats de filière d'une prise en compte de la cybersécurité au juste niveau.

OBJECTIF 10
Soutenir la structuration d'un marché européen des produits et services de cybersécurité

L'Union européenne s'est dotée d'une stratégie ambitieuse pour renforcer ses capacités en cybersécurité, en harmonisant les standards et en favorisant la coopération entre les États membres.

Dans le contexte favorable d'une dynamique forte de croissance du marché intérieur européen des produits et services de sécurité, la France mobilisera l'ensemble des instruments de politique industrielle pour susciter et accompagner une consolidation du secteur, contribuant de manière proactive à **l'autonomie stratégique européenne dans ce domaine.**

La France soutiendra ainsi l'émergence de capacités industrielles européennes de cybersécurité de premier plan, en recherchant notamment des synergies entre les domaines civil et militaire. Avec l'appui des fonds européens et en partenariat avec le secteur privé, elle poursuivra ses investissements dans le secteur et accompagnera l'essor d'entreprises de référence à l'échelle mondiale. Elle encouragera en particulier le développement de fonds d'investissement porteurs de stratégies adaptées et soutiendra la filière dans son internationalisation.

Cette dynamique sera appuyée par le déploiement du cadre européen de certification des produits et services de cybersécurité, auquel la France contribuera activement.

OBJECTIF 11

Maitriser les dépendances technologiques dans le champ de la sécurité numérique

Le chiffrement est un composant essentiel du socle de sécurité permettant d'assurer la confidentialité et l'intégrité des communications ou du stockage des données. La France investira massivement pour conserver la maitrise des technologies critiques dans le domaine de la cryptographie. Elle soutiendra également les travaux relatifs aux technologies de protection des données, sur l'ensemble de leur cycle de vie.

Par ailleurs, la France poursuivra ses investissements afin de se doter d'une gamme élargie de produits aptes à contrer les menaces les plus avancées, notamment pour les usages régaliens. Il s'agira aussi pour la France d'offrir des solutions de sécurité au meilleur niveau à ses partenaires européens et ses alliés.

Enfin, la France soutiendra le développement de sa filière d'évaluation de sécurité, reconnue au niveau international pour son excellence. Elle promouvra également l'émergence d'une capacité d'évaluation de sécurité autonome au sein de l'Union européenne.

PILIER 05

SOUTENIR LA SÉCURITÉ ET LA STABILITÉ DU CYBERESPACE EN EUROPE ET À L'INTERNATIONAL

Facteur clé de la résilience des Nations et de la stabilité du cyberespace, la coopération internationale fait aujourd'hui face à de nombreux défis : conflictualité croissante, y compris dans le cadre de stratégies hybrides[2], remise en cause du multilatéralisme et des mécanismes onusiens, promotion d'une vision autoritaire du numérique, prolifération d'outils cyber-intrusifs, ruptures technologiques facilitant l'accès aux capacités offensives, rôle accru des acteurs non étatiques. Dans ce contexte, la France cherchera à maximiser l'impact de son action internationale en s'appuyant sur plusieurs principes fondamentaux :

Le respect des valeurs démocratiques, la promotion de l'État de droit et l'application du droit international dans le cyberespace. Par ces principes, elle défend un cyberespace libre, ouvert, sûr et non fragmenté. Elle contribue pleinement à la construction d'une autonomie stratégique européenne fondée sur une résilience cyber multisectorielle (règlementaire, industrielle, judiciaire, diplomatique, militaire), au service de la sécurité euro-atlantique et du pilier européen de l'OTAN.

Une gouvernance internationale adaptative, combinant gouvernance multilatérale (organisations internationales et États membres) et gouvernance multi-acteurs (États, secteur privé, recherche, société civile), où les droits et responsabilités de chacun sont clairement définis. La France reste particulièrement attachée au caractère multi-acteurs de la gouvernance de l'Internet.

La recherche du consensus. Dotée d'une diplomatie proactive et inclusive (Appel de Paris, Processus de Pall Mall, réforme de l'ONU), la France rejette les logiques de blocs géopolitiques, sources d'instabilité et de fragmentation. Elle défend sa liberté d'action dans le cyberespace, reposant sur des capacités de lutte informatique défensive et offensive, mises en œuvre seules ou avec ses partenaires, dans le respect du droit international.

Forte du respect de ces principes, la France œuvrera en tant que puissance responsable, coopérative et solidaire à la sécurité et la stabilité du cyberespace.

OBJECTIF 12

Promouvoir un cadre et une gouvernance internationale garantissant la sécurité et la stabilité du cyberespace

La France inscrira le plus largement possible son action dans un cadre multilatéral afin de promouvoir et de soutenir la mise en œuvre d'un cadre normatif à même de garantir la sécurité et la stabilité du cyberespace. Elle poursuivra notamment sa contribution à la réforme de la gouvernance de l'Organisation des Nations unies (ONU) via l'établissement d'un Mécanisme

[2] Les stratégies hybrides se caractérisent notamment par la conjonction de cyberattaques, de manipulations de l'information, de l'instrumentalisation du droit (ou *lawfare*) et de l'économie, et le recours à des opérations militaires. Une stratégie hybride désigne pour la France le recours par un acteur étranger à une combinaison intégrée et volontairement ambiguë de modes d'actions militaires et non militaires, directs et indirects, légaux ou illégaux, difficilement attribuables. Jouant avec les seuils estimés de riposte et de conflit armé, cette combinaison est conçue pour contraindre et affaiblir la France et ses partenaires.

global sur la cybersécurité à l'horizon 2026, dans le but notamment d'opérationnaliser les engagements pris au titre des normes de comportement responsable agréées à l'ONU en 2015. Elle continuera également de s'engager dans la mise en œuvre de mesures de confiance appliquées à la conduite des États dans le cyberespace, dans un cadre bilatéral comme multilatéral, notamment à l'Organisation pour la sécurité et la coopération en Europe (OSCE).

La France s'engagera par ailleurs à associer à cette ambition les différentes parties prenantes. Dans cette perspective, elle poursuivra l'animation de la communauté issue de l'Appel de Paris[3] et soutiendra les initiatives internationales connexes visant à mettre en œuvre les principes de cette initiative. A ce titre, la France poursuivra son implication active dans le Processus de Pall Mall[4] qui vise à lutter contre la prolifération et l'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché.

Enfin, la France continuera de défendre un régime efficace de coopération judiciaire en matière pénale pour lutter contre la cybercriminalité dans le respect d'une part des droits de l'Homme et de la souveraineté des États. Elle veillera à ce titre à préserver les fondamentaux portés par la Convention de Budapest du Conseil de l'Europe, notamment dans le cadre de la mise en œuvre de la nouvelle Convention des Nations unies contre la cybercriminalité.

OBJECTIF 13
Agir en allié et partenaire coopératif et fiable au sein d'une communauté d'intérêt cyber internationale

La capacité d'action de la France et sa résilience dans le cyberespace se conçoivent en premier lieu dans une logique partenariale. Forte d'un modèle national robuste et singulier, elle entend agir comme un partenaire fiable à plusieurs niveaux.

A l'échelle européenne, la France considère l'UE comme une organisation politique incontournable et privilégiée pour préserver sa capacité d'initiative et d'action dans le cyberespace. La France recherchera le renforcement de l'autonomie stratégique de l'Union européenne en matière de cybersécurité et de cyberdéfense. Elle s'engagera pleinement dans les enceintes de coopération et mécanismes européens de gestion de crise (CSIRT Network[5],

[3] Lancé le 12 novembre 2018 par le Président de la République française, l'Appel de Paris fédère plus de 1 200 acteurs autour de neuf principes fondateurs pour promouvoir un cyberespace ouvert, sûr, stable, accessible et pacifique. En particulier, l'Appel de Paris a joué un rôle pionnier dans l'élaboration d'une régulation autour de la sécurité des produits numériques ou encore du phénomène de « cyber-mercenariat ».

[4] Fruit d'une initiative franco-britannique lors du sommet bilatéral du 10 mars 2023, le processus de Pall Mall a été officiellement lancé lors d'une conférence co-organisée par la France et le Royaume-Uni à Lancaster House à Londres, les 6 et 7 février 2024. Il a vocation à déboucher sur des recommandations concrètes à destination des États et de l'industrie. En avril 2025, un code de bonnes pratiques à destination des Etats visant à lutter contre la prolifération et l'usage irresponsable de capacités commerciales de cyber-intrusion a été adopté à Paris. En août 2025, il est soutenu par 27 Etats.

[5] Etabli en 2017 par la directive NIS, le réseau des CSIRT (*CSIRT Network*) regroupe les équipes de réponse à incident de chaque État membre de l'UE et le service de cybersécurité pour les institutions, organes et organismes de l'Union (CERT-UE). L'objectif du réseau est de favoriser les échanges d'informations entre ses membres pour améliorer le traitement des cyberattaques.

CyCLONe[6], CYBERCO[7], MICNET[8]). Elle y encouragera notamment le partage d'informations sur la menace, dans le but de parvenir à une autonomie croissante des Européens en la matière.

Au sein de l'OTAN, la France continuera de promouvoir l'intégration de la cyberdéfense dans les missions et opérations de l'Alliance, ainsi que le renforcement de la cybersécurité de l'organisation, tout en veillant à la complémentarité avec les actions de l'UE.

Au-delà de ces cadres, la France développera des coopérations avec des partenaires partageant des intérêts communs et un niveau équivalent de maturité en cyberdéfense, en misant sur le partage d'expertise et le renforcement mutuel des capacités.

Dans ces trois cercles d'action, la France mobilisera ses partenariats pour améliorer la connaissance de la menace, la prévention, la protection, la réponse aux attaques et la conduite d'opérations militaires. Elle renforcera également sa capacité à porter des stratégies de réponse aux agressions cyber conjointes aux niveaux européen et international.

OBJECTIF 14
Développer une capacité de cyber-solidarité

Le renforcement de notre résilience nationale requiert un effort de renforcement des capacités de résilience à l'échelle globale.

En coordination avec ses partenaires et alliés, la France contribuera à relever le niveau de cybersécurité à l'échelle internationale en développant des capacités d'assistance ciblées vis-à-vis de ses partenaires les plus vulnérables, conformément aux orientations de l'Appel d'Accra[9].

Dans cette perspective, la France interviendra dans deux domaines d'action :

- **Elle conduira des actions en matière de coopération structurelle** (*capacity building*), dont le but sera d'agir dans le long terme sur les capacités de cybersécurité du

[6] 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 de cybersécurité des 27 États membres de l'UE. Son objectif est double : permettre le partage d'informations sur les stratégies nationales de réponse en cas de crise cyber et coordonner la construction d'une analyse consolidée de la crise, au profit des décideurs politiques, tant au niveau national qu'européen.

[7] La Conférence des cybercommandeurs européens (CYBERCO) a été créée en 2022 à l'initiative de la France. Elle rassemble l'ensemble des plus hautes autorités militaires de cyberdéfense des Etats membres de l'UE 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 cybermenace ainsi que sur des problématiques opérationnelles de cyberdéfense des Nations.

[8] Le réseau MICNET (*Military computer emergency response team operational network*) est le pendant militaire du réseau des CSIRT européens. Il a été créé en novembre 2022 par 18 États 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.

[9] Cet Appel s'inspire du format de l'Appel de Paris et rassemble des États, des organisations internationales, des entreprises et des organisations de la société civile au profit du renforcement capacitaire cyber à l'international. La France 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.

partenaire, en favorisant sa montée en puissance par le biais notamment du conseil, de la formation et de l'aide logistique. Dans cette perspective, la France poursuivra notamment son action en faveur du développement des centres régionaux de renforcement capacitaire, ainsi que son implication dans les projets européens. Le soutien en cybersécurité à l'Ukraine sera poursuivi dans le cadre du Mécanisme de Tallinn. La coordination et la synergie avec l'action des opérateurs de l'Etat en matière de coopération technique internationale (Expertise France, Civipol) seront recherchées.

- **Elle conduira également des actions en matière de coopération opérationnelle**, dont la vocation sera d'appuyer un partenaire par des opérations ponctuelles, soit sur un plan préventif (audit des systèmes d'information), soit sur un plan réactif (réponse à incident). Le recours au secteur privé en matière d'assistance sera également encouragé. La France soutiendra ainsi l'opérationnalisation de la Réserve cyber de l'UE[10] et son extension au bénéfice des Etats de la Communauté politique européenne. Sur le plan militaire, la France développera des partenariats de long terme, dits « partenariats cyber agiles » (ou en anglais *Tailored Cyber Partnership* - TCP), qui permettent d'appuyer les forces armées de pays partenaires dans le développement de leur capacité de cyberdéfense et dans les phases de réponse à incident.

[10] Opérationnelle à l'horizon 2026, la Réserve de cybersécurité de l'UE sera composée de services de réaction aux incidents fournis par des prestataires privés de confiance, qui pourront être déployés pour aider à faire face à ces incidents de cybersécurité auxquels sont confrontés les États membres de l'UE, les institutions, organes et agences de l'UE et, le cas échéant, les pays tiers associés au programme pour une Europe numérique.

UNE GOUVERNANCE MULTI PARTIES PRENANTES AU SERVICE D'UNE RÉSILIENCE NATIONALE

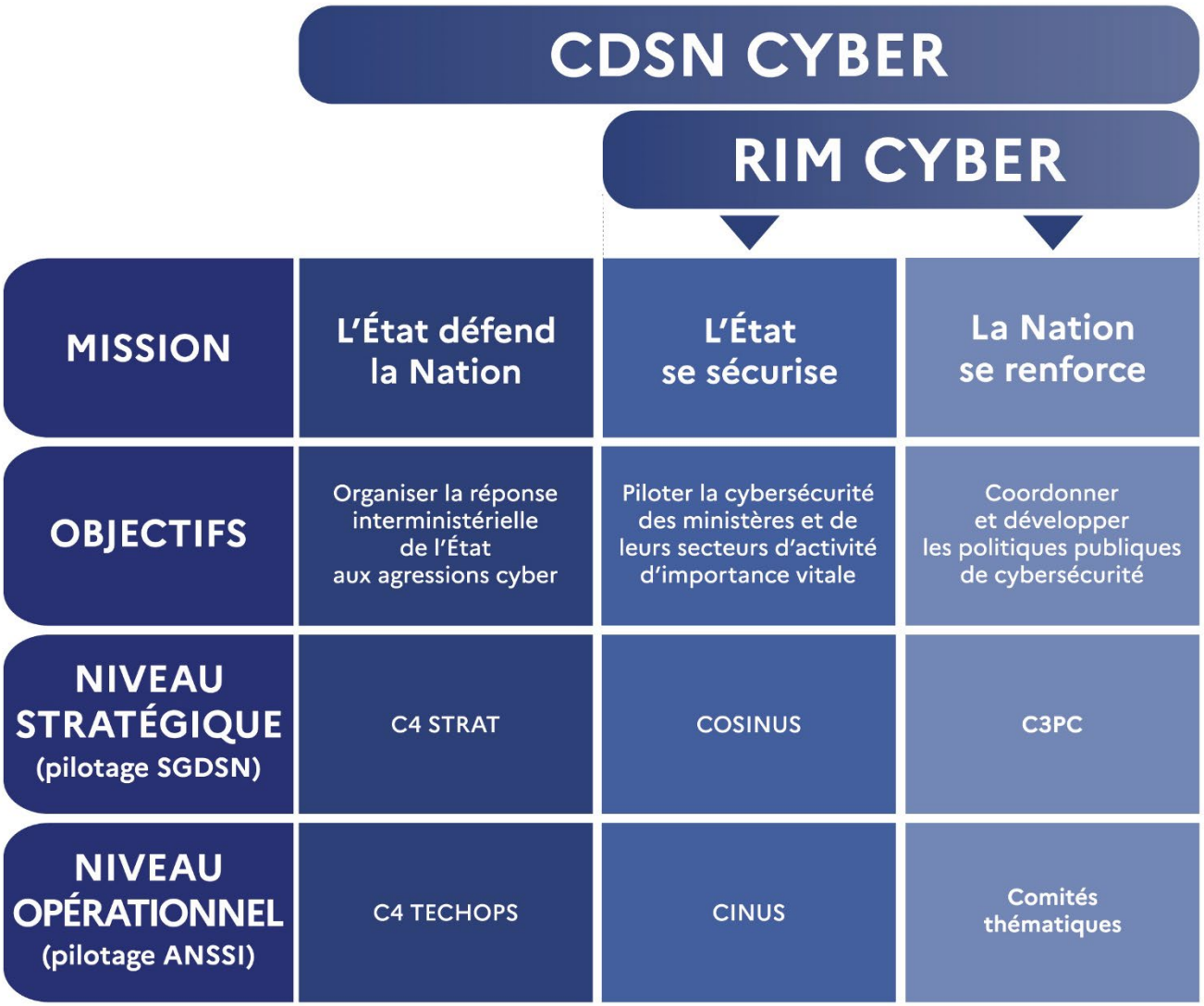
Le modèle d'organisation de la cybersécurité adopté par la France est garant du respect des libertés publiques et sépare les missions et capacités défensives et offensives. La gouvernance mise en place permet toutefois de garantir une coordination efficace entre ces pôles, gage de l'efficacité de la cyberdéfense de la France.

S'agissant du volet défensif, cette gouvernance repose sur trois missions qui associe chacune des parties prenantes différentes :

- « L'Etat défend la Nation » : cette mission a pour objectifs la connaissance de la menace et l'élaboration de la réponse de la France aux cyberattaques ;
- « L'Etat se sécurise » : cette mission assure le pilotage de la sécurité des systèmes d'information de l'État et de ses opérateurs les plus critiques ;
- « La Nation se renforce » : cette mission coordonne l'action publique et les efforts privés concourant à renforcer la cybersécurité des particuliers, des entreprises, des associations et des collectivités territoriales.

La cybermenace concerne aujourd'hui tous les pans de la société, de l'économie et du territoire national. Les secteurs professionnels, l'administration dans les territoires (collectivités territoriales, services déconcentrés de l'État, etc.), le monde académique, la société civile sont désormais tout à la fois des victimes de cyberattaques et des partenaires incontournables dans la construction et la mise en œuvre de la réponse à cette menace. C'est pourquoi la France renforcera l'intégration de toutes ces parties prenantes dans la gouvernance nationale de la cybersécurité, tant à l'échelon national que dans sa déclinaison territoriale.

Schéma de la gouvernance cyber de la France[11]



[11] *CDSN : Conseil de défense et de sécurité nationale*
RIM : réunion interministérielle
C4 STRAT : Centre de coordination des crises cyber de niveau stratégique
C4 TECHOPS : Centre de coordination des crises cyber de niveau technico-opérationnel
COSINUS : Comité stratégique interministériel de la sécurité numérique
CINUS : Comité interministériel de suivi de la sécurité numérique
C3PC : Comité de pilotage des politiques publiques cyber