Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

STRATÉGIE NATIONALE

POUR LA SÉCURITÉ DU NUMÉRIQUE

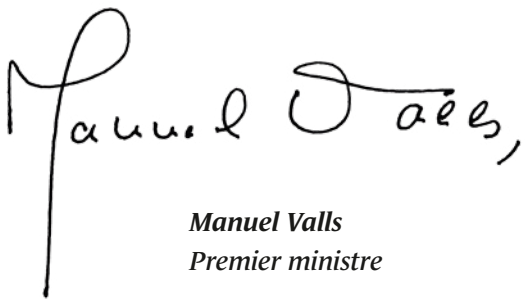
La France est pleinement engagée dans la transition numérique. Forte d'une population très largement connectée et portée par une économie numérique en croissance soutenue, la France dispose de talents et d'atouts à la pointe de l'innovation européenne et mondiale.

Le numérique est également un espace de compétition et de confrontation. Concurrence déloyale et espionnage, désinformation et propagande, terrorisme et criminalité trouvent dans le cyberespace un nouveau champ d'expression.

La « République numérique en actes », voulue par le gouvernement, doit promouvoir nos valeurs, notre économie et protéger les citoyens. Œuvrer pour la sécurité du numérique, c'est favoriser le développement d'un cyberespace gisement de croissance pérenne et lieu d'opportunités pour les entreprises françaises, c'est affirmer nos valeurs démocratiques, c'est enfin préserver la vie numérique et les données personnelles des Français.

Mon ambition dans le domaine est élevée. La stratégie nationale pour la sécurité du numérique doit s'appuyer en particulier sur la formation et sur la coopération internationale et doit être portée par l'ensemble de la communauté nationale : le gouvernement, les administrations, les collectivités territoriales, les entreprises et plus largement, tous nos compatriotes. Elle est l'affaire de tous.

Répondre aux enjeux de sécurité du monde numérique est un facteur clé de succès collectif. Je souhaite que cette stratégie nationale pour la sécurité du numérique enclenche une dynamique à la fois protectrice et libératrice d'énergies.



Manuel Valls
Premier ministre

STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE

La numérisation de la société française s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu national. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'État, les acteurs économiques et les citoyens. Cybercriminalité, espionnage, propagande, sabotage ou exploitation excessive de données personnelles menacent la confiance et la sécurité dans le numérique et appellent une réponse collective et coordonnée selon cinq objectifs stratégiques.

 # Intérêts fondamentaux, défense et sécurité des systèmes d'information de l'État et des infrastructures critiques, crise informatique majeure.

En développant une pensée stratégique autonome, soutenue par une expertise technique de premier plan, la France se donnera les moyens de défendre ses intérêts fondamentaux dans le cyberespace de demain. Parallèlement, elle continuera à renforcer la sécurité de ses réseaux critiques et sa résilience en cas d'attaque majeure en développant des coopérations tant à l'échelle nationale avec les acteurs privés qu'internationale.

 # Confiance numérique, vie privée, données personnelles, cybermalveillance.

Afin que le cyberespace reste un espace de confiance pour les entreprises de toutes tailles et les particuliers, des mesures de protection et de réaction seront adoptées. La protection passera par une vigilance accrue des pouvoirs publics sur l'utilisation des données personnelles et par le développement d'une offre de produits de sécurité numérique adaptée au grand public. La réaction s'articulera autour d'un dispositif d'assistance aux victimes de cybermalveillance qui apportera une réponse technique et judiciaire à de tels actes.

 # Sensibilisation, formations initiales, formations continues.

La prise de conscience individuelle des risques liés à la numérisation de la société reste insuffisante. Face à ce constat, la sensibilisation des écoliers et des étudiants sera renforcée. En outre, afin de répondre aux demandes croissantes des entreprises et des administrations en matière de cybersécurité, la formation d'experts dans ce domaine sera développée.

 # Environnement des entreprises du numérique, politique industrielle, export et internationalisation.

La croissance des marchés du numérique à l'échelle mondiale, et des exigences de sécurité qu'ils porteront constituent une opportunité de différenciation pour les produits et services français ayant un niveau de sécurité numérique adapté aux usages. Par le soutien à l'investissement, à l'innovation, et à l'export, par le biais de la commande publique, l'État développera un environnement favorable aux entreprises françaises du numérique proposant une offre de produits et de services sécurisés.

 # Europe, souveraineté numérique, stabilité du cyberespace.

La régulation des rapports dans le cyberespace est devenue un sujet majeur des relations internationales. La France promouvra, avec les États membres qui le souhaitent, une feuille de route pour l'autonomie stratégique numérique de l'Europe. Elle renforcera également son influence dans les instances internationales et soutiendra les pays volontaires les moins protégés dans la mise en place de capacités de cybersécurité afin de contribuer à la stabilité globale du cyberespace.

La sécurité du numérique conforte le projet de République numérique. L'État y joue un rôle majeur en élaborant cette stratégie et en lançant une dynamique dans laquelle les professionnels du numérique, les décideurs publics et privés et les citoyens sont invités à s'investir.

*La stratégie nationale pour la sécurité du numérique a été élaborée avec l'ensemble des ministères. Elle a été soumise par le secrétaire général de la défense et de la sécurité nationale à l'approbation du Premier ministre en application du 7° de l'article R*1132-3 du code de la défense.*

SOMMAIRE

INTRODUCTION

La France accomplit sa transition numérique. Les réseaux sont omniprésents dans le fonctionnement de l'État, dans l'activité économique et la vie quotidienne des citoyens.

Porteur de nouveaux usages, de nouveaux produits et de nouveaux services, le numérique est facteur d'innovation. Il engendre une mutation de la plupart des métiers. Il transforme des secteurs d'activités et des entreprises pour leur apporter plus de souplesse et de compétitivité. Enrichis par l'apport du numérique, ces secteurs sont simultanément plus exposés aux menaces issues du numérique.

Se priver du numérique ou ne pas pouvoir y accéder conduit à une forme d'exclusion économique et sociale. De même, un État qui ne disposerait pas de l'autonomie nécessaire dans le secteur du numérique verrait sa souveraineté menacée.

Pour que le numérique demeure un espace de liberté, d'échanges et de croissance, il est nécessaire que la confiance et la sécurité y soient établies et défendues. Seul un effort collectif et coordonné peut permettre d'atteindre cet objectif.

* *
*

Une première stratégie de cybersécurité de la France a été élaborée début 2010 et publiée début 2011, peu après la découverte d'une attaque informatique à des fins d'espionnage contre les ministères économiques et financiers. Présents depuis plusieurs mois, les attaquants avaient pris le contrôle du cœur d'un des réseaux des ministères et collectaient régulièrement des informations de nature politique, économique et financière.

Ce type d'attaque informatique vise de nombreuses entreprises françaises, de toutes tailles, dans tous les secteurs d'activité. Les entreprises sont également la cible d'escroqueries de toutes sortes comme, par exemple, l'infection par un logiciel malveillant qui rend les fichiers de l'entreprise inutilisables jusqu'au paiement d'une rançon effectuée par des moyens difficilement traçables.

Parallèlement, les intrusions informatiques destinées à dérober des informations personnelles (identité, données d'identification à des sites marchands, données bancaires) se multiplient. Il s'agit le plus souvent pour des criminels de commettre des délits identiques à ceux connus dans le monde matériel — vols, escroqueries, chantage —, mais de manière industrialisée, une part du risque d'être identifié et poursuivi en moins. Le crime organisé s'est saisi de l'avantage procuré par les réseaux de communications électroniques. Ses capacités techniques sont croissantes au point d'être désormais en mesure de pratiquer, pour lui-même ou en sous-traitance par hybridation, des actes de sabotage ou de prise en otage d'outils de production.

Des campagnes de harcèlement se développent sur les réseaux sociaux, comme des cas d'escroqueries aux sentiments destinés à amener les victimes crédules à transférer de l'argent vers l'étranger.

Les nombreuses défigurations de sites Internet, notamment ceux de collectivités territoriales, ayant suivi les attentats de janvier 2015 ou, quelques semaines plus tard, l'attaque informatique contre un média français

à vocation internationale, ont montré la volonté et la capacité de groupes organisés de rendre indisponibles des ressources informatiques qui soutiennent notre vie quotidienne.

Ce qu'il est convenu d'appeler « l'état de la menace » établi en 2010 s'est ainsi révélé juste. La menace est aujourd'hui accentuée par l'accroissement des capacités des attaquants, la prolifération des techniques d'attaques et le développement dans le cyberespace de la criminalité organisée.

Mais un défi d'une autre nature est apparu. Celui de la captation de richesses numériques par un oligopole d'entreprises utilisant leur position dominante pour gêner l'arrivée de nouveaux entrants et capter la valeur ajoutée de cette économie naissante qui exploitera les données pour inventer de nouveaux services, améliorer notre vie quotidienne ou rendre plus accessibles les services publics. Parmi ces données figurent au premier plan nos données personnelles, y compris celles relatives à notre vie privée. La maîtrise de ces masses de données ouvre la porte à la déstabilisation économique et à des formes sophistiquées de propagande ou d'orientation des convictions ou des habitudes. En ce sens, ce défi relève, par son ampleur nationale et ses enjeux stratégiques, de la défense et de la sécurité nationale.

* *
*

Face à ces risques malheureusement avérés, beaucoup a déjà été accompli.

Comme l'annonçait le livre blanc sur la défense et la sécurité nationale de 2008, une agence nationale a été créée dès 2009 pour traiter les attaques informatiques et protéger les systèmes d'information de l'État et des infrastructures critiques.

Une politique industrielle en faveur de l'industrie nationale de cybersécurité est notamment portée par le programme des investissements d'avenir et dans le cadre du plan « Industrie du futur ».

Le Parlement a voté en 2013 les mesures proposées par le gouvernement qui visent à renforcer la sécurité informatique des opérateurs d'importance vitale et de ceux qui participent à leurs systèmes d'information les plus critiques.

Les positions de la France sont soutenues dans toutes les instances internationales, et notamment à l'Organisation des Nations Unies (ONU) qui a reconnu en 2013 l'application au cyberespace du droit international. Des relations bilatérales opérationnelles avec plusieurs pays ont par ailleurs été engagées par les services de l'État.

Les ministères ont pris conscience de l'impact politique et technique des technologies de l'information sur leurs missions et l'activité de leur administration et se dotent de coordonnateurs en charge des questions liées au numérique et à sa sécurité. Une politique de sécurité des systèmes d'information de l'État a été élaborée et est progressivement mise en œuvre.

Les années qui viennent doivent permettre de recueillir les bénéfices des actions engagées et d'élargir le périmètre de l'action publique et des acteurs impliqués. Le constat doit maintenant être établi et partagé que la défense et la sécurité du numérique relèvent de la communauté nationale et pas seulement de l'action de l'État.

* *
*

Jusqu'à ces dernières années, notre défense et notre sécurité nationale reposaient sur l'expertise, le comportement et les décisions des hommes et femmes ayant accès aux installations et équipements les plus sophistiqués, les plus protégés, les plus secrets. Alors qu'émerge une société massivement connectée, cette responsabilité est désormais en partie partagée par l'ensemble des Français. Un objet connecté ou un service insuffisamment sécurisé par ses développeurs, la négligence d'un décideur en matière de sécurité des systèmes d'information, le comportement dangereux d'un prestataire ou celui d'un salarié mélangeant sans précaution vie privée et vie professionnelle peuvent entraîner pertes de disponibilité, de confidentialité ou d'intégrité d'informations essentielles, ruptures d'activité et pertes écono-

miques, accidents industriels et pertes de vies humaines ou catastrophes écologiques et troubles à l'ordre public, susceptibles d'affecter la vie de la nation.

Jamais, en effet, la stabilité de notre avenir, porté par le numérique, n'a été aussi dépendante des responsabilités de chacun et de celles, collectives, de trois communautés d'acteurs.

Une première communauté a la responsabilité de proposer et de mettre en œuvre des technologies, des produits et des services dotés du niveau de sécurité adapté aux usages et capables de parer les risques identifiés. Les principaux acteurs de cette communauté sont les chercheurs, les inventeurs de produits et services et leurs intégrateurs, les entreprises du secteur de la cybersécurité, les opérateurs de réseaux de communications électroniques, les fournisseurs d'accès à Internet ou les fournisseurs de services informatiques distants.

La deuxième communauté a pour responsabilité de protéger la nation des prédateurs du numérique. Outre la mise en œuvre des politiques de cybersécurité, il s'agit notamment de conduire de façon volontariste une politique de développement des compétences techniques nécessaires et de mettre en place un écosystème de confiance qui accompagne la transformation numérique de la société, en défendant les citoyens, nos valeurs et nos intérêts dans le cyberespace. Cette responsabilité engage celui qui la porte à exprimer sa position en faveur de solutions de sécurité qualifiées et à promouvoir l'industrie nationale, y compris à l'export. Cette communauté est constituée des élus, du gouvernement, des administrations centrales et territoriales et des syndicats.

La troisième communauté a pour responsabilité d'utiliser de manière réfléchie les services et technologies disponibles, d'effectuer des choix raisonnés et d'éviter les comportements à risque dans les actes de la vie numérique. Cette communauté est constituée de tous les usagers, responsables d'entreprises, acteurs de la société civile et citoyens.

Ce sont ces engagements synallagmatiques pris par chacun des acteurs qui permettront à la France de bénéficier pleinement des apports du numérique, de transformer en avantage concurrentiel national les choix liés à la sécurité du numérique, souvent vécus aujourd'hui exclusivement comme une contrainte économique et comportementale, et de promouvoir nos valeurs, nos produits et nos services.

L'État a pour rôle dans le cyberespace de garantir la liberté d'expression et d'action de la France et d'assurer la sécurité de ses infrastructures critiques en cas d'attaque informatique majeure (objectif 1), de protéger la vie numérique des citoyens et des entreprises, de lutter contre la cybercriminalité (objectif 2), d'assurer la sensibilisation et la formation nécessaires à la sécurité du numérique (objectif 3), de favoriser le développement d'un écosystème favorable à la confiance dans le numérique (objectif 4) et de promouvoir la coopération entre États-membres de l'Union dans un sens favorable à l'émergence d'une autonomie stratégique numérique européenne, garante sur le long terme d'un cyberespace plus sûr et respectueux de nos valeurs (objectif 5).

CINQ
OBJECTIFS
STRATÉGIQUES

1

#INTÉRÊTS FONDAMENTAUX, DÉFENSE ET SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT ET DES INFRASTRUCTURES CRITIQUES, CRISE INFORMATIQUE MAJEURE

ENJEUX

La France est la cible d'attaques informatiques qui portent atteinte à ses intérêts fondamentaux.

Aujourd'hui, lorsqu'un attaquant cible l'État, les opérateurs d'importance vitale ou des entreprises stratégiques, il cherche à s'installer durablement dans le système d'information visé pour y voler des données confidentielles (politiques, diplomatiques, militaires, technologiques, économiques, financières ou commerciales). Demain, un attaquant pourrait prendre le contrôle d'objets connectés, interrompre à distance une activité industrielle ou détruire sa cible. Depuis 2011, une centaine d'attaques informatiques d'importance ont été traitées, le plus souvent en toute confidentialité, par les administrations et les prestataires de service compétents.

Parallèlement, des attaques informatiques destinées à frapper l'opinion publique accompagnent les prises de position de la France sur la scène internationale, ses opérations militaires ou certains débats publics. À titre d'exemple, les défigurations de sites Internet qui ont suivi les attentats ayant visé la France début 2015 ont eu un impact technique faible, mais une portée symbolique souhaitée par les attaquants. Dans le même ordre d'idée, l'attaque informatique ayant entraîné l'interruption de service d'un média français à vocation internationale visait également à frapper les esprits et favorise la radicalisation conduisant à des actes terroristes. Cette attaque a également montré la capacité d'attaquants déterminés à perturber le fonctionnement d'une infrastructure à forte valeur symbolique.

Depuis plusieurs années, plusieurs États ont mis en œuvre leur volonté politique et des moyens humains, techniques et financiers considérables afin de mener, à notre encontre, des opérations informatiques à grande échelle dans le cyberespace.

Qu'elles soient connues par des documents publiquement révélés ou mis en évidence lors du traitement d'attaques informatiques, les excès de telles pratiques entament la crédibilité de certains de ces États sur la scène internationale et ruinent la confiance qu'il serait naturel d'attribuer aux produits et services numériques de leurs entreprises.

« Les excès de telles pratiques entament la crédibilité de certains de ces États sur la scène internationale et ruinent la confiance qu'il serait naturel d'attribuer aux produits et services numériques de leurs entreprises. »

Ainsi, le risque cybernétique, placé en troisième position des menaces majeures pour la France par le Livre blanc sur la défense et la sécurité nationale de 2013, est aujourd'hui renforcé et constitue un défi majeur posé à la France.

OBJECTIF

La France se donnera les moyens de défendre ses intérêts fondamentaux dans le cyberespace. Elle consolidera la sécurité numérique de ses infrastructures critiques et œuvrera pour celle de ses opérateurs essentiels à l'économie.

ORIENTATIONS

> **Détenir les capacités scientifiques, techniques et industrielles nécessaires à la protection de l'information de souveraineté, à la cybersécurité et au développement d'une économie numérique de confiance.**

Un groupe d'experts pour la confiance numérique sera créé, sous l'égide du secrétariat d'État au numérique et de l'autorité nationale de sécurité des systèmes d'information.

Le groupe d'experts pour la confiance numérique réunira très régulièrement les administrations compétentes du premier ministre, des ministères de l'Éducation nationale, de l'Enseignement supérieur et de

la Recherche, de la Justice, de la Défense, des Affaires sociales, de la Santé et des droits des femmes, de l'Intérieur, de l'Économie, de l'Industrie et du numérique, le commissariat général à l'investissement, l'agence nationale de la recherche et les organismes de recherche concernés. Le groupe pourra associer à ses travaux des acteurs du secteur privé et des personnalités qualifiées.

La mission de ce groupe sera notamment d'identifier les technologies-clés dont la maîtrise est nécessaire pour les métiers de la cybersécurité et plus largement pour le développement d'un environnement numérique de confiance. Il évaluera les besoins en formations initiales et continues, suivra les travaux de recherche et en accompagnera la valorisation, participera à l'amélioration de l'accompagnement des jeunes docteurs. Il contribuera, dans le domaine des technologies numériques, à la définition des axes stratégiques des dispositifs de financement et d'accompagnement des travaux de recherche et de développement industriel. Ces travaux seront réalisés en cohérence avec ceux des structures déjà en place tel que le comité de filière des industries de sécurité (CoFIS).

Plus largement, les choix d'acteurs privés majeurs en matière de modèle économique, de technologie, parfois hors de tout cadre de normalisation, ou plus simplement certaines innovations dans les usages du numérique peuvent consolider la confiance ou susciter la défiance. Le groupe d'experts pour la confiance numérique organisera la veille technologique et économique permettant d'anticiper les évolutions des questions liées au numérique. Le cas échéant, des mesures adaptées seront proposées pour accompagner ou cadrer ces évolutions. Ces mesures pourront, par exemple, concerner la protection du potentiel scientifique et technique de la Nation ou le contrôle des investissements étrangers dans des entreprises nationales critiques.

Une commission du groupe d'experts réunira les coordinateurs ministériels des questions liées au cyberespace autour du secrétaire général de la défense et de la sécurité nationale pour les sujets relevant de sa compétence.

Ce groupe d'experts rendra compte annuellement de ses activités au Premier ministre.

> Assurer au profit de l'État, des entreprises et des citoyens une veille active en matière de sécurité des technologies et des usages.

Dans la perspective d'évolutions technologiques majeures, comme les télécommunications mobiles de 5e génération (5G) ou les « réseaux définis par le logiciel », la France restera vigilante sur la nature et les capacités des équipements matériels et logiciels installés au cœur de ses réseaux de communications électroniques, pour protéger le secret des correspondances, la vie privée de ses citoyens et la résilience de ces infrastructures, et poursuivra l'adaptation de son cadre réglementaire aux nouvelles technologies émergentes.

L'autorité nationale de sécurité des systèmes d'information informera régulièrement les ministères, les entreprises, les collectivités territoriales et les citoyens, par des moyens adaptés au public visé, des éléments susceptibles de présenter un danger dans leur utilisation du numérique. Le cas échéant, ces informations auront au préalable été consolidées avec les administrations compétentes.

> Accélérer le renforcement de la sécurité des systèmes d'information de l'État.

Depuis 2010, plusieurs actions destinées à élever le niveau de sécurité des systèmes d'information de l'État ont été conduites. Une politique de sécurité des systèmes d'information de l'État (PSSIE) a été élaborée, un réseau interministériel de communications électroniques est en essor, le déploiement de terminaux mobiles sécurisés a été initié. Ces actions, comme celles destinées à produire les équipements de sécurité destinés à protéger l'information de souveraineté, mobilisent des ressources humaines et budgétaires. Elles seront poursuivies afin d'offrir au gouvernement et à nos capacités militaires le niveau de sécurité adapté à une préservation à long terme de l'autonomie de décision et d'action de la France.

L'application de la politique de sécurité des systèmes d'information de l'État et l'efficacité des mesures adoptées seront évaluées annuellement. Un bilan annuel confidentiel sera transmis au Premier ministre et le Parlement sera informé au moyen d'indicateurs.

Dans le même objectif d'informer le Parlement, les projets de loi comporteront dans leur étude d'impact dès 2016 un volet consacré au numérique et, au sein de ce volet, à la cybersécurité, établi sous l'égide des hauts fonctionnaires chargés de la qualité de la réglementation. Plus largement, les hauts fonctionnaires chargés de la qualité de la réglementation veilleront à prendre en compte les questions liées au renforcement de la sécurité des systèmes d'information de l'État dans le cadre du pilotage de l'activité normative.

> Préparer la France et les organisations multilatérales dont elle est membre à faire face à une crise informatique majeure.

Annoncé par le Livre blanc sur la défense et la sécurité nationale de 2013, le renforcement de la sécurité des systèmes d'information les plus sensibles des opérateurs d'importance vitale a fait l'objet de mesures législatives (articles 21 et 22 de la loi n° 2013-1168 du 18 décembre 2013). Les travaux engagés avec ces opérateurs se poursuivront durablement, notamment par la mise à jour régulière des textes réglementaires. Ces travaux seront progressivement étendus, comme le précise la loi, aux opérateurs publics ou privés qui participent à ces systèmes d'information sensibles.

Ce choix fait par la France aura permis de participer activement à l'élaboration des orientations de la proposition de directive européenne concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union et d'anticiper sa transposition. Le moment venu, la France définira ses opérateurs essentiels à l'économie conformément aux orientations de la directive et participera aux initiatives européennes destinées à renforcer leur sécurité numérique.

Les exercices de gestion de crise cybernétique menés au niveau national concerneront progressivement l'ensemble du territoire et des secteurs d'activité d'importance vitale. Le ministère de la Défense, en lien avec l'autorité nationale de sécurité des systèmes d'information, poursuivra la mise en place d'une réserve de cyberdéfense à vocation opérationnelle destinée à faire face à une crise informatique majeure.

En parallèle, la France continuera de concourir à l'émergence d'un cadre de coopération volontaire de gestion de crises cybernétiques à l'échelle européenne, en soutenant en particulier les travaux de l'agence européenne ENISA.

Il appartient au CERT-EU (capacité de réponse aux incidents informatiques des institutions, entités et agences de l'Union européenne - UE) et au NCIRC (capacité de réponse aux incidents informatiques de l'Organisation du Traité de l'Atlantique-Nord - OTAN) d'assurer la cyberdéfense de leurs institutions respectives. Active lors des exercices de gestion de crises cybernétiques organisés par ces organisations et fortement représentée dans les instances qui orientent les choix de l'UE et de l'OTAN en matière de technologies numériques sécurisées, la France continuera à apporter son concours à ces institutions et à leurs membres dans le respect des compétences de chacun.

La France contribuera également à renforcer la cybersécurité d'autres organisations internationales dont elle est membre, au niveau politique et au niveau technique, notamment celles hébergées sur le territoire national qui bénéficient de l'écosystème technique national.

> Développer une pensée autonome et conforme à nos valeurs.

Les choix stratégiques effectués par la France au lendemain de la Deuxième Guerre mondiale ont entraîné l'émergence d'une pensée stratégique autonome et l'élaboration d'une doctrine qui a donné à la France une place singulière sur la scène internationale et irrigue aujourd'hui encore sa diplomatie et les concepts d'emploi de ses forces armées.

Si le numérique modifie en profondeur nos sociétés, il reste à mesurer son impact sur d'autres réalités comme celles de souveraineté, de territoire national, de monnaie ou d'intérêts fondamentaux de la Nation et à repenser l'organisation et les moyens de l'action publique pour y faire appliquer la loi ou pour assurer leur protection. Une réflexion sera conduite sous la coordination du secrétaire général de la défense et de la sécurité nationale, pour élaborer un corpus intellectuel relatif au cyberespace.

2

#CONFIANCE NUMÉRIQUE, VIE PRIVÉE, DONNÉES PERSONNELLES, CYBERMALVEILLANCE

ENJEUX

S'ils ont de manière générale confiance dans le numérique, les Français ont, en revanche, une certaine défiance quant à son impact sur leur vie quotidienne, notamment personnelle. Généralement soucieux de l'utilisation et de la conservation de leurs données personnelles, ils les confient toutefois à des plates-formes dont les conditions d'utilisation sont léonines au détriment des utilisateurs.

Le mode opératoire constaté lors de certaines attaques informatiques contre des entreprises ou des administrations montre également une réelle difficulté à dissocier vie privée et vie professionnelle dans l'utilisation des équipements comme des services.

Les attaques informatiques qui touchent les particuliers ont généralement pour objectif le gain financier. Par la prise de contrôle de l'équipement personnel utilisé — ordinateurs, tablette, ordiphone —, l'usurpation d'identité et le vol d'identifiants à des comptes bancaires ou à des sites commerciaux, par l'engagement d'une relation affective virtuelle débouchant sur une demande de transfert d'argent, par le chiffrement de données à l'insu de l'utilisateur conduisant au paiement d'une rançon, le racket est aujourd'hui pratiqué à grande échelle par une criminalité qui s'est organisée et a gagné en efficacité.

Bien qu'il ne fasse appel à aucune technique d'attaque particulière, le harcèlement, facilité et amplifié par les réseaux de communications électroniques est une agression informatique contre les personnes dont l'issue est parfois dramatique.

Si l'agence nationale de la sécurité des systèmes d'information (ANSSI) est l'interlocuteur étatique identifié en cas d'incident informatique grave affectant les administrations et les opérateurs d'importance vitale, la lisibilité de l'offre publique est nettement moindre en matière d'assistance aux victimes d'actes de cybermalveillance pour les autres acteurs, qu'il s'agisse d'entreprises de taille intermédiaire, de petites et moyennes entreprises, de professions libérales, de collectivités territoriales ou de particuliers.

Les victimes d'actes de cybermalveillance sont encouragées à déposer une plainte, auprès des services de police et de gendarmerie qui se sont adaptés au traitement de tels contentieux. Toutefois, la réponse qui leur est apportée dans ce cadre est centrée sur l'identification des auteurs présumés de la cybermalveillance et sur l'engagement éventuel de poursuites contre ces auteurs. Les victimes doivent pouvoir être orientées vers un service d'assistance au traitement de l'incident informatique à l'origine de l'acte de cybermalveillance.

Plus insidieusement, les plates-formes numériques et notamment les réseaux sociaux peuvent façonner l'opinion et parfois être vecteurs de valeurs qui ne sont pas celles de la République. Dans certains cas, ils peuvent être instrumentalisés à des fins de désinformation et de propagande envers les citoyens français, notamment les plus jeunes. Les opinions diffusées vont alors à l'encontre des intérêts fondamentaux de la France et relèvent d'une atteinte à la défense ou à la sécurité nationale sanctionnée par la loi.

Dans un registre différent, les développements récents et simultanés de nouveaux usages et de nouvelles techniques de stockage et de traitement des données favorisent l'émergence de risques de déséquilibre économique et d'atteinte à la sécurité individuelle des personnes ainsi qu'à celle des nations. Le souhait de voir instaurer, par exemple au travers de traités commerciaux, la libre circulation des données, dont les données personnelles collectées par

« Les plates-formes numériques et notamment les réseaux sociaux peuvent façonner l'opinion et parfois être vecteurs de valeurs qui ne sont pas celles de la République »

« Le développement numérique ne peut être durable dans un cyberespace où les États ne respectent pas les bonnes pratiques nécessaires à une transition numérique équilibrée et profitable à toutes les nations »

des objets connectés, masque difficilement la volonté de captation de ces données par des oligopoles dont les valeurs et les pratiques ne correspondent ni à la conception de la vie privée française ou européenne ni à son encadrement juridique. La captation massive et illicite de certains types de données personnelles, comme par exemple les données de santé, peut en effet entraîner des atteintes à la sécurité individuelle et collective, ou plus simplement une exploitation commerciale abusive (revente à des compagnies d'assurance, par exemple).

Le développement numérique ne peut être durable dans un cyberespace où les États ne respectent pas les bonnes pratiques nécessaires à une transition numérique équilibrée et profitable à toutes les nations et où quelques acteurs économiques s'accaparent la richesse que constituent les données numériques, notamment les données personnelles, véritables ressources des générations futures.

OBJECTIF

La France développera un usage du cyberespace conforme à ses valeurs et y protègera la vie numérique de ses citoyens. Elle accroîtra sa lutte contre la cybercriminalité et l'assistance aux victimes d'actes de cybermalveillance.

ORIENTATIONS

> Promouvoir et défendre nos valeurs sur les réseaux de communications électroniques et dans les instances internationales.

Les droits des personnes s'appliquent de la même manière « en ligne » et « hors ligne ». Le cyberespace doit ainsi rester un lieu de libre expression pour tous les citoyens, où les abus ne peuvent être prévenus que dans la mesure des limites fixées par la loi et en conformité avec nos engagements internationaux. La France promeut cette approche destinée à préserver un cyberespace libre et ouvert dans les instances internationales.

Il appartient à l'État d'informer les citoyens sur les risques de manipulation et les techniques de propagande utilisées par des acteurs malveillants sur Internet. Après les attentats perpétrés contre la France en janvier 2015, le gouvernement a mis en place une plateforme d'information sur les risques liés à la radicalisation islamiste via les réseaux de communications électroniques. « Stop-djihadisme.gouv.fr ». Cette approche pourrait être étendue pour répondre à d'autres phénomènes de propagande ou de déstabilisation. Il appartient aux services compétents en matière de défense et de sécurité de détecter ces phénomènes et de proposer au gouvernement la mise en œuvre de ces moyens.

> Apporter une assistance de proximité aux victimes d'actes de cybermalveillance.

Copiloté par le ministère de l'Intérieur et l'agence nationale de sécurité des systèmes d'information, avec l'appui des ministères de la Justice, des Finances et des comptes publics, de la Défense, de l'Économie, de l'Industrie et du numérique, un dispositif national sera mis en place dès 2016 destinés à porter assistance aux victimes d'acte de cybermalveillance.

Ce dispositif aura également une mission de sensibilisation aux enjeux de protection de la vie privée numérique et de prévention qui s'appuiera localement sur l'action des préfets et des services de l'État. Le réseau territorial de l'ANSSI, les délégués régionaux à l'intelligence économique et les services du ministère de l'Intérieur compétents en matière de sécurité économique, le réseau « transition numérique », celui de la Banque de France — qui pourrait à terme intégrer dans sa cotation des entreprises un critère lié à la prise en compte du risque cybernétique —, participeront à cette

mission. Les chambres de commerce et d'industrie, les chambres des métiers et plus largement tous les réseaux professionnels seront également sollicités.

Le dispositif adoptera une forme juridique et une organisation lui permettant de bénéficier de l'apport des acteurs économiques du secteur de la cybersécurité — éditeurs de logiciels, plates-formes numériques, fournisseurs de solutions. Grâce aux technologies mises en œuvre, le dispositif devra proposer aux victimes des solutions techniques s'appuyant sur des acteurs de proximité et faciliter les démarches administratives, notamment afin de favoriser le dépôt de plainte.

> Mesurer la cybercriminalité.

Les travaux interministériels menés à l'initiative du ministère de l'Intérieur depuis 2013 ont conduit au constat qu'il n'existe pas aujourd'hui de statistiques fiables relatives spécifiquement à la délinquance ou à la criminalité informatique, la plupart des infractions concernées étant enregistrées sous une appellation qui ne rend pas compte de cette dimension, aujourd'hui absente des référentiels utilisés.

L'absence de telles statistiques est préjudiciable à la conception par les pouvoirs publics de politiques constamment réévaluées et à la mise en place des moyens adaptés. C'est pourquoi le ministère de l'Intérieur mettra en œuvre de nouveaux instruments de suivi de l'évolution de la cybercriminalité afin d'éclairer l'action publique. L'Observatoire national de la délinquance et des réponses pénales y contribuera également en consacrant un volet de ses travaux à l'examen statistique de la cybercriminalité. Ce volet intégrera les données transmises par l'autorité nationale de sécurité des systèmes d'information et le dispositif d'assistance aux victimes d'actes de cybermalveillance, qui auront participé à son élaboration.

> Protéger la vie numérique, la vie privée et les données personnelles des Français.

À la faveur du règlement européen en matière d'identité électronique (eIDAS), la France se dotera d'une feuille de route claire en matière d'identité numérique délivrée par l'État. Cette feuille de route sera élaborée avant la fin de l'année 2015 sous l'égide du mi-

nistère de l'intérieur et des secrétariats d'État chargés du numérique et de la réforme de l'État, appuyés par les services du Premier ministre, et devra comprendre un volet qui définira un cadre de référence pour l'utilisation au profit des collectivités territoriales de l'identité numérique délivrée par l'État.

Cette feuille de route prendra en compte la stratégie numérique du Gouvernement qui prévoit le déploiement de dispositifs de fédération d'identité permettant d'utiliser une même identité numérique pour s'authentifier sur différents services. Grâce à ces dispositifs, les identités numériques peuvent avoir été fournies par des entités différentes tant que le tiers chargé de la gestion de la fédération d'identité est capable de déterminer le niveau de confiance associé à l'identité.

Sous réserve de respecter des exigences de sécurité adaptées aux usages et aux menaces, ces dispositifs sont de nature à renforcer la confiance des utilisateurs dans leur vie numérique, à en favoriser la fluidité tout en limitant le risque d'une exploitation non désirée de leurs données personnelles. Pour les usages les plus sensibles, tels que ceux concernant la vie démocratique ou les échanges internationaux relatifs à la justice, des niveaux de confiance élevés dans les dispositifs et services seront systématiquement employés. Ces niveaux élevés de confiance s'appuieront sur le tissu industriel national et le schéma de certification de sécurité en place.

La France protègera la vie privée et les données personnelles de ses ressortissants. Les droits à la vie privée et à la maîtrise individuelle et collective des données personnelles seront réaffirmés chaque fois que nécessaire et notamment à l'occasion des négociations commerciales entre États, qu'elles soient bilatérales ou multilatérales.

Pour informer les Français sur l'utilisation faite des données confiées aux services numériques, une signalétique adaptée et partagée avec les États volontaires et en cohérence avec les travaux européens effectués dans le cadre du règlement européen relatif à la protection des données à caractère personnel sera mise en place courant 2016. Cette signalétique permettra de visualiser les caractéristiques essentielles des conditions d'utilisation des plates-formes et services numériques ou des moyens de paiement utilisés.

> Proposer des solutions techniques destinées à sécuriser la vie numérique, accessibles à toutes les entreprises et au grand public.

Les services de l'État labelliseront des solutions de sécurisation des terminaux personnels. Une signalétique cohérente avec celle proposée ci-dessus permettra aux utilisateurs d'être informés d'éventuelles transmissions d'informations à un tiers dans le cadre de cette protection. Une fois créé, le dispositif d'assistance aux victimes d'actes de cybermalveillance évoqué ci-dessus fera, au titre de sa mission de prévention, la promotion de ces dispositifs auprès des publics concernés.

Par ailleurs, et comme cela a pu être engagé par le programme des investissements d'avenir, l'offre de solutions accessibles et adaptées destinées à sécuriser la vie numérique des petites et moyennes entreprises sera soutenue.

Un soutien au développement de solutions françaises sera apporté ainsi qu'aux communautés du logiciel libre développant des solutions de sécurité.

> Renforcer les mécanismes opérationnels d'entraide judiciaire internationale et universaliser les principes de la Convention de Budapest sur la lutte contre la cybercriminalité.

Adoptée en 2001 dans le cadre du Conseil de l'Europe, la Convention de Budapest est devenue un instrument de référence qui permet la coopération dans la lutte contre la cybercriminalité entre États des cinq continents. Ratifié par 46 États, dont 7 non membres du Conseil de l'Europe, cet instrument rassemble d'ores et déjà 125 États à un titre ou à un autre (signataires, États invités à adhérer, États recevant de l'assistance technique en vue d'une future adhésion, États ayant adopté leur loi interne sur le modèle de la Convention).

Il est aujourd'hui essentiel d'universaliser et de consolider aussi bien le socle de normes que l'outil de coopération que constitue ce texte.

Par ailleurs, la France fera la promotion au sein de l'Union européenne de la définition d'un dispositif de coopération judiciaire simplifiée entre États membres afin d'accélérer la transmission des données et de mettre un terme aux activités illégales.

3

#SENSIBILISATION, FORMATIONS INITIALES, FORMATIONS CONTINUES

ENJEUX

La France est en retard par rapport à ses partenaires en matière de sensibilisation de sa population aux risques associés aux usages du numérique et de formation à la cybersécurité.

Les Français négligent en général les bonnes pratiques lors de l'utilisation des réseaux de communications électroniques.

Dans l'usage privé des réseaux de communications électroniques, les enfants et adolescents, confrontés à des contenus inadaptés, exposés au harcèlement ou à la prédation, sont les premières victimes. Afin de rompre le silence et de permettre les poursuites, les plus jeunes devraient être initiés à la conduite à tenir lorsqu'ils sont victimes de malveillance numérique.

La sensibilisation de tous est un préalable nécessaire pour que les élus, les dirigeants d'administrations ou d'entreprises puissent prendre en compte le « risque cyber » à son juste niveau et décider des mesures susceptibles de protéger les citoyens qu'ils représentent ou les organismes qu'ils dirigent, face à des menaces de vol d'informations ou de propriété intellectuelle, d'atteinte aux données personnelles, voire l'exposition à des ruptures d'activité, d'accidents de production, avec des impacts technologiques ou environnementaux auxquels ils sont potentiellement exposés.

Outre la sensibilisation des plus jeunes, la formation aux métiers du numérique doit permettre aux futurs professionnels du domaine de bénéficier d'un enseignement poussé en sécurité des systèmes d'information, aujourd'hui encore absent de nombreuses formations supérieures.

Par ailleurs, le contenu et le nombre de formations initiales et supérieures aux métiers de la cybersécurité ne permettent pas de satisfaire la demande des entreprises et des administrations.

OBJECTIF

La France sensibilisera dès l'école à la sécurité du numérique et aux comportements responsables dans le cyberespace. Les formations initiales supérieures et continues intégreront un volet consacré à la sécurité du numérique adapté à la filière considérée.

ORIENTATIONS

> Sensibiliser l'ensemble des Français.

Un programme ambitieux de sensibilisation de l'ensemble des Français doit être engagé.

Sous la conduite du ministère de l'Éducation nationale, de l'enseignement supérieur et de la recherche et du secrétariat d'État au numérique, avec l'appui du service d'information du Gouvernement et de l'agence nationale de la sécurité des systèmes d'information, un appel à manifestation d'intérêt pour la réalisation de contenus de sensibilisation à destination du grand public sera lancé.

Le ministère de l'Intérieur poursuivra l'opération « Permis Internet » initiée en 2014 par la gendarmerie nationale en partenariat avec une fondation privée, et relayée depuis le début de l'année 2015 par la Police nationale. Cette opération permet de sensibiliser aux risques et de conseiller plus de 300 000 élèves de CM2 chaque année pour les protéger dans leur navigation sur Internet.

La visibilité du portail « une éducation numérique

pour tous » de la Commission nationale informatiques et libertés (CNIL) sera renforcée.

Les associations seront invitées à élaborer des projets de campagnes de communication visant à renforcer la confiance dans le numérique susceptibles de rentrer dans le cadre d'une « grande cause nationale ».

> Intégrer la sensibilisation à la cybersécurité dans toute formation supérieure et dans les formations continues.

Le ministère de l'Éducation nationale, de l'enseignement supérieur et de la recherche, avec l'aide de la Conférence des présidents d'université, de la conférence des grandes écoles et des administrations compétentes, incitera à ce que, dès la rentrée 2016, des sensibilisations à la cybersécurité correspondant à la filière de formation soient mises en place dans toute formation initiale supérieure.

Le ministère du travail, de l'emploi, de la formation professionnelle et du dialogue social, appuyé par les administrations de l'État compétentes en matière de cybersécurité, engagera les consultations nécessaires afin que, dès 2016, les organismes dispensateurs de formations continues intègrent dans les différents cursus une sensibilisation aux questions de cybersécurité adaptée à la formation.

Enfin, sous la coordination du secrétariat d'État chargé du numérique, avec les ministères concernés et l'appui de l'ANSSI, la sensibilisation de catégories professionnelles pour lesquelles une imprégnation des questions de cybersécurité est particulièrement nécessaire au regard de leurs responsabilités sociétales sera engagée. Ces catégories seront précisées par le comité stratégique pour la confiance numérique.

> Intégrer la formation à la cybersécurité dans toute formation supérieure intégrant une part d'informatique.

L'initiative « CyberÉdu » lancée en 2013 a permis de confirmer l'intérêt des enseignants intervenants dans les cursus de formations supérieures aux métiers de l'informatique pour les sujets de sécurité des systèmes d'information. Cette initiative doit être confortée.

Le ministère de l'Éducation nationale, de l'enseignement supérieur et de la recherche, avec l'aide de la conférence des présidents d'universités, la conférence des grandes écoles, les administrations et les organisations professionnelles compétentes, veillera à ce que dès la rentrée 2016, une formation à la sécurité des systèmes d'information adaptée à la filière soit dispensée dans toute formation initiale supérieure comprenant des questions liées au numérique. Une intégration de ces éléments de sécurité dans les cours existants devra être recherchée en priorité et s'inscrire de manière pertinente dans le contexte plus large de chaque spécialité enseignée. Ces démarches pourront utilement s'appuyer sur les contenus pédagogiques en cours d'élaboration, en lien étroit avec la communauté enseignante, dans le cadre du projet CyberÉdu.

Le ministère de la Décentralisation et de la Fonction publique s'attachera à ce que les formations aux postes de responsabilités de la fonction publique comportent des éléments de sensibilisation à la cybersécurité. En lien avec le ministère de l'Intérieur, il veillera à ce que le concours de recrutement dans le corps des ingénieurs des systèmes d'information et de communication prévu par le décret n°2015-576 du 27 mai 2015 ainsi que les formations qui seront dispensées à ses membres comportent un volet cybersécurité.

Face à une demande croissante de nos partenaires, il conviendra, dans la mesure du possible, d'adapter une partie de l'offre de formation et de sensibilisation à un public international, en proposant notamment des programmes en langue anglaise.

> Recenser et anticiper les besoins en formations initiales et continues.

Sous l'égide du groupe d'experts pour la confiance numérique, les besoins en formations initiales à court, moyen et long terme seront établis, en lien avec l'ensemble des acteurs concernés de l'administration et du secteur privé.

Les syndicats professionnels seront sollicités pour l'élaboration et la mise en place de formations continues adaptées aux besoins des salariés et des entreprises.

4

#ENVIRONNEMENT DES ENTREPRISES DU NUMÉRIQUE, POLITIQUE INDUSTRIELLE, EXPORT ET INTERNATIONALISATION

ENJEUX

« Le développement, par les entreprises nationales du secteur numérique, d'une offre de produits et de services sécurisés doit également être vu comme un facteur essentiel de compétitivité pour ces entreprises. »

Le cyberespace est en construction rapide. 100 000 objets nouveaux se connectent chaque heure à Internet. La présence de nombreuses entreprises françaises sur les salons internationaux comme le succès de l'initiative « French Tech » montre un réel dynamisme de l'innovation française en matière de produits et services numériques. Cette réalité ne doit cependant pas masquer une certaine perte de maîtrise et une réelle dépendance technologiques.

Les grands équipements qui assurent le fonctionnement des réseaux de communications électroniques dont les infrastructures sont situées en France sont souvent conçus, développés et administrés depuis des centres situés hors de l'Europe. Il en est de même pour l'essentiel des équipements de communications et de sécurité informatique de nos opérateurs d'importance vitale. Le fonctionnement d'un nombre croissant d'entreprises repose sur l'utilisation d'applications et le traitement de données hébergés dans des espaces immatériels non maîtrisés, portés par des infrastructures physiques situées hors du territoire national et non soumises au droit européen.

Les évolutions en cours tant au niveau des technologies que dans les modèles économiques, avec par exemple la multiplication des objets connectés ou la concentration des plates-formes de service en ligne entre les mains de quelques acteurs seulement, sont de nature à amplifier cette perte de maîtrise du cyberespace national. En cas de crise internationale, l'accès à des pans entiers du cyberespace pourrait nous être contesté.

La réponse à cet enjeu de souveraineté nécessite en premier lieu le maintien d'une industrie nationale et européenne forte et compétitive dans le domaine spécialisé des produits et services de cybersécurité. Plus généralement, elle passe par le développement, en France et en Europe, d'une offre d'équipements et de services numériques qui apportent à leurs clients les garanties de sécurité et de confiance adaptées aux enjeux et aux usages.

Les utilisateurs n'ont pas le moyen de s'assurer eux-mêmes du niveau de sécurité des objets et services numériques. La promotion de la sécurité dans le discours commercial des fournisseurs se généralise sans toutefois permettre une évaluation objective du niveau de sécurité réellement atteint. Le développement d'une plus grande lisibilité sur le plan de la sécurité de l'offre numérique, fondée sur des éléments objectifs et vérifiables par un tiers, constitue un défi majeur pour assurer la confiance dans l'économie numérique.

Le développement, par les entreprises nationales du secteur numérique, d'une offre de produits et de services sécurisés doit également être vu comme un facteur essentiel de compétitivité pour ces entreprises. Le domaine des moyens de paiements (cartes à puce, terminaux de paiement, etc.) est l'archétype d'un secteur économique dans lequel un niveau de sécurité adapté à la menace et vérifiable par un tiers constitue un argument commercial de premier plan. Plusieurs entreprises nationales disposent dans ce secteur d'une position concurrentielle au niveau mondial qui doit beaucoup à l'excellence qu'elles ont su développer et démontrer en matière de sécurité.

La multiplication des menaces cybernétiques et la prise de conscience de plus en plus large de la réalité de ces menaces conduiront dans quelques années à faire de la sécurité un critère d'achat essentiel dans de nombreux autres secteurs. Agir dès à présent pour améliorer la sécurité et la transparence de l'offre nationale de solutions numériques, c'est aussi préparer leur compétitivité à venir.

En 2015, la part des entreprises françaises et singulièrement des PME-PMI utilisant largement

le numérique n'est que dans la moyenne des pays européens. Le rattrapage de ce retard doit s'accompagner d'une meilleure sécurisation de la vie numérique des entreprises et en premier lieu d'une meilleure sécurité de leurs systèmes d'information. Il en va de notre compétitivité et donc de nos emplois.

Le défi posé aux entreprises françaises est de concilier recherche de productivité, d'économies, de rentabilité et utilisation ou développement de produits et services numériques ne mettant pas en danger leur compétitivité ou leur sécurité, celles de leurs partenaires ou celles de leurs clients.

La plupart des équipements, objets et services numériques disponibles aujourd'hui sur le marché n'ont pas le niveau de sécurité informatique leur permettant d'éviter un incident — fuite de données, dysfonctionnement ou rupture de service. Pour les entreprises françaises l'ergonomie, la protection des données personnelles, le niveau de sécurité des produits et services numériques qu'elles développent et produisent, doivent devenir à court terme un différenciateur, un avantage concurrentiel pour ces entreprises et en retour pour la nation.

Par ailleurs, si la contrefaçon ne relève pas directement de la sécurité des systèmes d'information, des produits de sécurité informatique contrefaits peuvent mettre en danger l'activité des organisations qui les acquièrent.

« Pour les entreprises françaises l'ergonomie, la protection des données personnelles, le niveau de sécurité des produits et services numériques qu'elles développent et produisent, doivent devenir à court terme un différenciateur, un avantage concurrentiel pour ces entreprises et en retour pour la nation. »

En matière d'internationalisation des entreprises et d'export, face à une concurrence internationale exacerbée où nos partenaires accordent un soutien appuyé et structuré à leur industrie, les services de l'État doivent s'organiser de manière pérenne pour soutenir les entreprises françaises de la cybersécurité.

La mobilisation et la coordination de toutes les ressources publiques et privées disponibles sont essentielles pour accroître la visibilité et la compétitivité de l'offre française à l'international, mutualiser les connaissances, les retours d'expérience et ainsi favoriser le partage d'informations entre les différents acteurs de la filière.

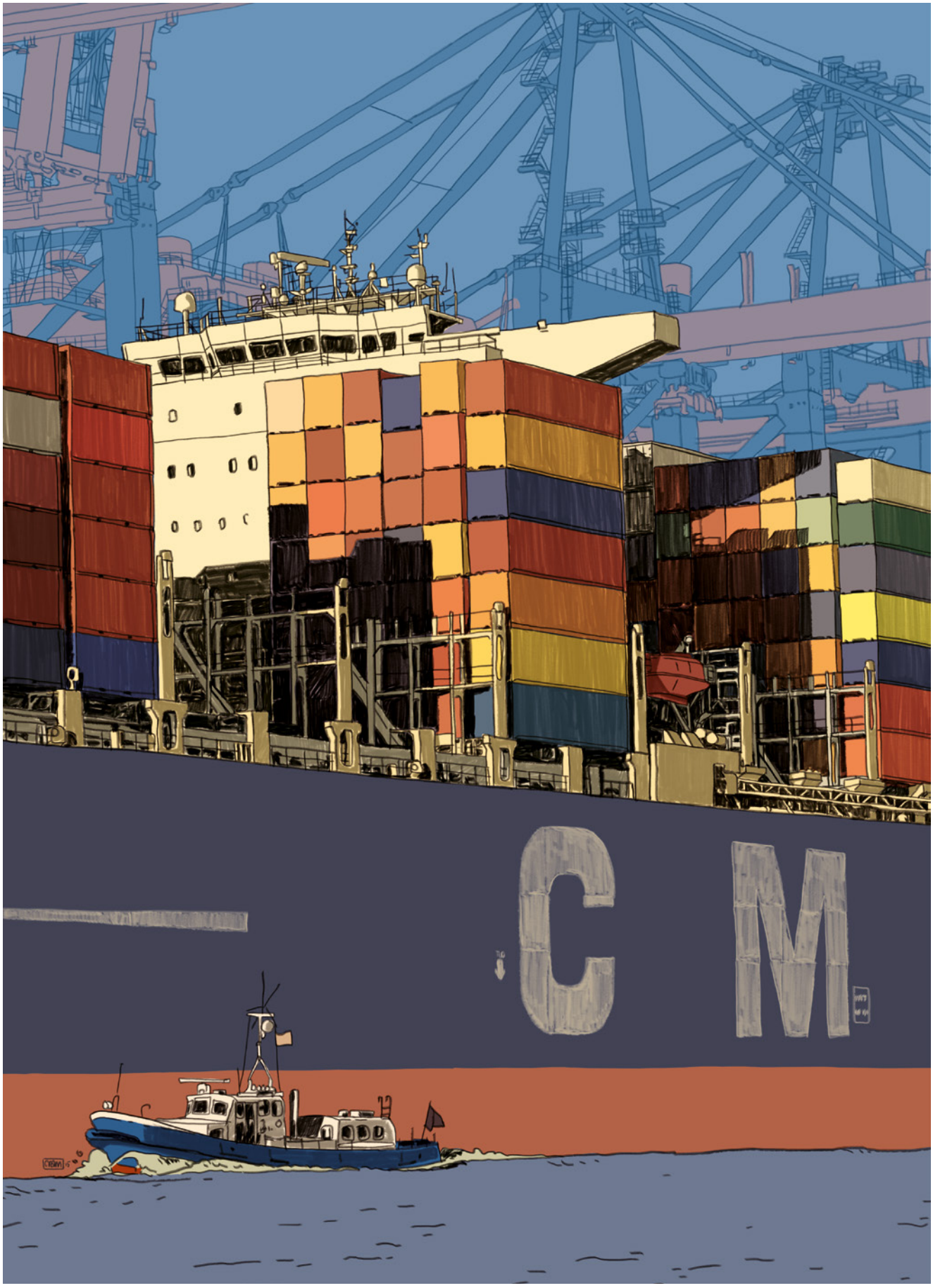
OBJECTIF

La France développera un écosystème favorable à la recherche et à l'innovation et fera de la sécurité du numérique un facteur de compétitivité. Elle accompagnera le développement de l'économie et la promotion internationale de ses produits et services numériques. Elle s'assurera de la disponibilité pour ses citoyens, ses entreprises et ses administrations, de produits et services numériques présentant des niveaux d'ergonomie, de confiance et de sécurité adaptés aux usages et aux cybermenaces.

ORIENTATIONS

> Développer et valoriser l'offre nationale et européenne de produits et services de sécurité.

En lien avec les administrations compétentes du ministère de l'Économie, de l'Industrie et du numérique et du ministère de la Défense, l'agence nationale de la sécurité des systèmes d'information a engagé en 2012 une politique industrielle afin de développer le tissu national des entreprises développant des produits et services de sécurité informatique.


C
M

Le lancement en 2013 du plan « cybersécurité » de la Nouvelle France industrielle, désormais englobé dans la solution « Confiance numérique » accompagné de l'appui du commissariat général à l'investissement et de BpiFrance ont permis d'organiser la filière et de lancer des appels à projets visant à créer une offre d'équipements de confiance pour la détection d'attaques informatiques, essentiellement destinés aux opérateurs d'importance vitale, et de produits de mobilité sécurisée à l'intention de toutes les entreprises.

Les services de l'État vont accentuer leur effort en matière de qualification et de suivi de produits et de services de sécurité informatique, ainsi que de soutien au développement de nouveaux produits de sécurité répondant à l'évolution des usages. Ils soutiendront également la valorisation et la pérennisation de ces offres par le biais d'une commande publique privilégiant les produits et services de sécurité qualifiés au bon niveau, ainsi que par des actions de communication et de sensibilisation à destination du secteur privé.

Par ailleurs, les services de l'État chercheront à diffuser les résultats des travaux de recherche et développement qu'ils financent pour des équipements de haut niveau de sécurité afin d'élever celle des produits destinés aux entreprises et au grand public.

Enfin, la France s'attachera à tirer pleinement parti des leviers offerts par l'Union européenne afin de soutenir, promouvoir et défendre les compétences scientifiques, technologiques et industrielles françaises dans les domaines de la cybersécurité. Elle encouragera par ailleurs l'UE à ne pas se limiter à un rôle de consommateur, mais à s'imposer comme un acteur global incontournable de l'offre dans ce secteur.

> Transférer les savoir-faire acquis vers le secteur privé pour favoriser la prise en charge de sa sécurité informatique.

La France s'est dotée depuis cinq ans d'une capacité de détection et de traitement des attaques informatiques, comme l'annonçait le Livre blanc sur la défense et la sécurité nationale de 2008. Si cet effort doit être poursuivi, notamment par l'ANSSI, il appartient au secteur privé d'assurer sa propre sécurité dans le domaine informatique comme dans d'autres domaines, les services de l'État ne devant intervenir qu'en cas de crise grave.

Appuyée par le transfert de savoir-faire acquis par les administrations vers le secteur privé, la labellisation de prestataires compétents et de confiance devrait permettre de détecter et de traiter l'inévitable croissance du nombre d'attaques informatiques subies par les entreprises.

> Préparer un monde numérique plus sûr par une meilleure anticipation des usages, un accompagnement adapté et une information des acteurs.

Pour les cinq ans à venir, la priorité des administrations compétentes en matière de sécurité des systèmes d'information doit être l'anticipation et la prévention.

Il s'agira d'obtenir que les produits et services numériques ou intégrant du numérique, conçus, développés et produits en France, soient parmi les plus sûrs au monde. Pour atteindre cet objectif, les administrations compétentes devront orienter leurs efforts de communication vers la communauté scientifique, publique et privée, et les lieux d'innovation — pôles de compétitivité, instituts de recherche technologiques, incubateurs, « fab labs », en y consacrant au besoin des moyens spécifiques, comme c'est le cas au ministère de la Défense, et, plus récemment, au ministère de l'Intérieur.

Lorsque les produits et services numériques hébergeront des données personnelles ou seront destinés aux secteurs d'activité d'importance vitale, les services de l'État apporteront les éléments utiles à l'analyse des risques ou les conseils nécessaires à l'obtention du niveau de sécurité correspondant à l'usage du produit ou du service en cours de conception ou de développement. Ils contribueront également, pour les usages qui le justifient, à mettre en place des dispositifs permettant d'évaluer de manière indépendante le niveau de sécurité et de confiance de ces produits et services, et d'offrir à leurs utilisateurs potentiels des garanties adaptées par le biais d'une labellisation.

Parallèlement, l'environnement juridique d'accueil des nouveaux produits et services devra être anticipé. À titre d'exemple, la prochaine arrivée de véhicules autonomes doit inciter le régulateur à préparer les conditions assurant la sécurité de leur circulation. La cybersécurité doit être prise en compte dans les groupes de travail internationaux définissant le référentiel et les procédures techniques de contrôle.

Pour d'autres types de produits ou services, une signalétique adaptée devra informer le consommateur de leurs caractéristiques numériques essentielles et notamment du traitement qui est réalisé des données collectées. Pour certains secteurs, comme celui de la santé, une labellisation systématique des produits et services numériques sera étudiée.

La France cherchera à associer d'autres États membres de l'Union européenne à la mise en œuvre de ces pratiques afin de créer une zone de confiance et de sécurité numériques. Les travaux engagés avec l'Allemagne en matière d'informatique en nuage ou de messageries sécurisés vont en ce sens.

> Intégrer l'exigence de cybersécurité dans la commande et le soutien publics.

Pour la protection de sa souveraineté et notamment la protection de ses informations relevant du secret de la défense nationale, la France conservera sa capacité financière et industrielle à développer des solutions atteignant les plus hauts niveaux de sécurité.

Plus généralement, l'ensemble de l'administration devra démontrer son exemplarité dans le cadre de la commande publique, en intégrant des critères de sécurité au juste niveau dans ses choix des produits et services numériques.

Enfin, dès 2016, tout produit ou service embarquant ou s'appuyant sur un système d'information et souhaitant répondre à un appel d'offres, à un appel à projets publics, ou accéder à des fonds publics bénéficiera d'un facteur de bonification s'il est accompagné d'une analyse de risque en matière de cybersécurité correspondant à l'usage prévu du produit ou service et de la réponse technique apportée.

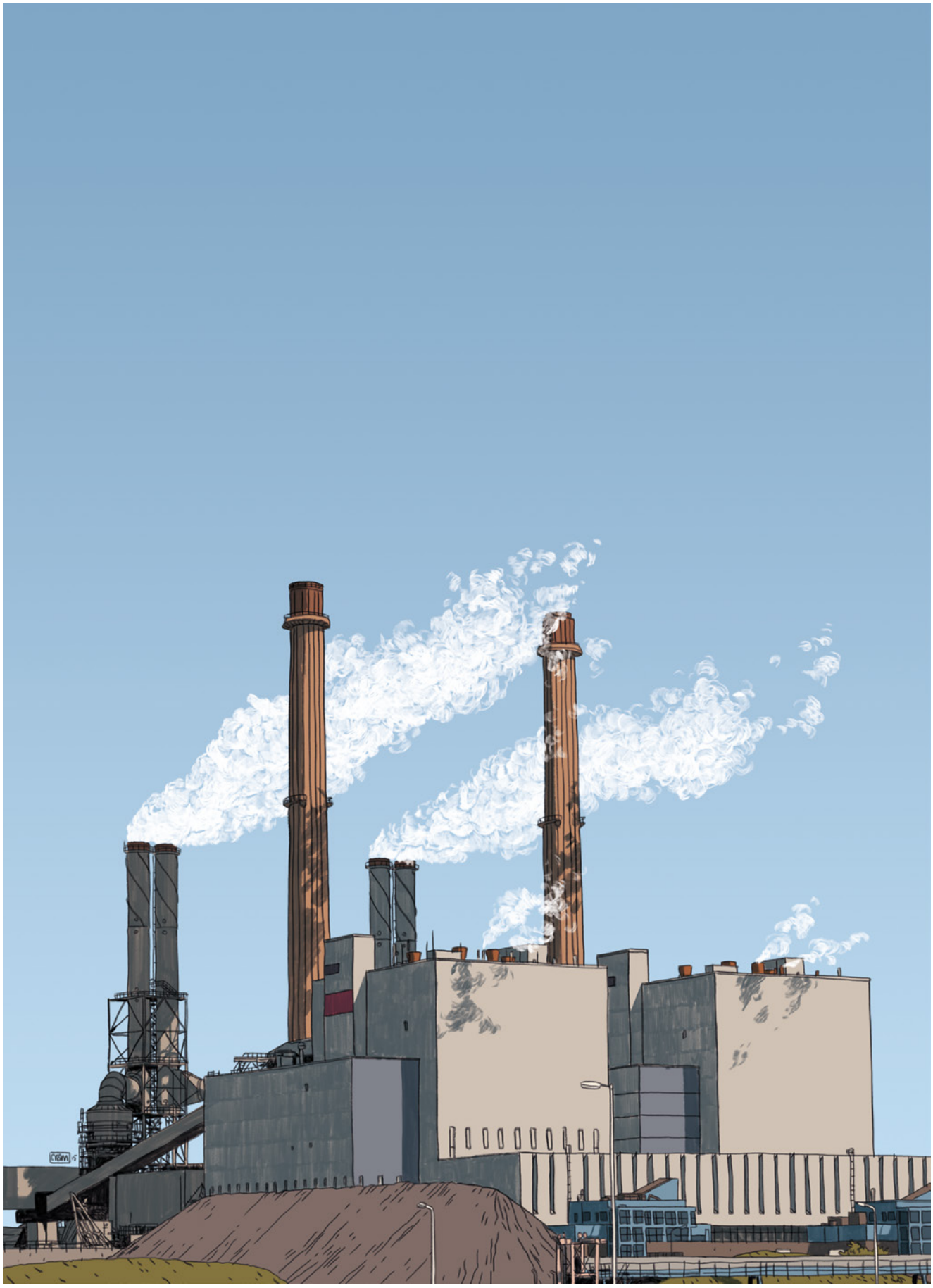
> Soutenir l'export et l'internationalisation des entreprises du secteur.

Afin de soutenir le développement économique de la filière industrielle de cybersécurité, la France s'attachera donc à renforcer la visibilité et la compétitivité de l'offre française à l'international et à faciliter l'accès des PME et des start-ups notamment aux marchés internationaux.

La coordination interministérielle sera structurée et renforcée. Une organisation adaptée en soutien des entreprises françaises sera mise en œuvre au-delà des actions ponctuelles et souvent isolées actuellement menées par les différents ministères et entités étatiques.

En sus de la création possible de dispositifs de soutien spécifiques aux acteurs de la filière cybersécurité, les conditions d'accès aux dispositifs de soutien existants, ainsi que leurs modalités de mise en œuvre seront clarifiées et optimisées. Les procédures de contrôle des exportations de solutions de cybersécurité seront clarifiées et optimisées.

Par ailleurs, à l'image des réalisations de « French Tech », les initiatives collaboratives issues du secteur privé et destinées à favoriser l'accompagnement des PME et des start-ups à l'international seront soutenues.



5

#EUROPE, SOUVERAINETÉ NUMÉRIQUE, STABILITÉ DU CYBERESPACE

ENJEUX

Le cyberespace est devenu un sujet majeur de négociation au sein des organisations internationales dont les travaux portent désormais sur l'ensemble du champ du numérique.

En 2013, les États ont reconnu que loin d'être d'un espace sans règle, le cyberespace était régi par le droit international existant. Pour autant, le cadre normatif international est encore en débat, ce qui, en l'absence d'avancée des négociations, pourrait nuire à la préservation d'un cyberespace stable et sûr, respectueux des droits fondamentaux et propice au développement d'une économie prospère et de confiance à l'ère numérique.

Tandis qu'un nombre croissant de pays déclarent se doter de capacités offensives, la conflictualité entre États trouve à s'exprimer de manière croissante dans le cyberespace. Par ailleurs, les révélations de pratiques massives et de techniques d'espionnage menées par de grands États ou des alliances d'États contre d'autres — parfois alliés —, des personnes et des entreprises, ont accru la défiance politique contre les pays à l'origine de ces pratiques et la méfiance technique vis-à-vis de leurs produits et services. Ces révélations favorisent aussi la prolifération de moyens techniques similaires.

Parallèlement, des groupes d'individus aux motivations et soutiens divers, mercenaires recrutés mondialement et associés au gré des circonstances, recourent régulièrement à des attaques informatiques dans le cyberespace pour tenter de déstabiliser les autorités gouvernementales de nombreux pays ou des entreprises qui les incarnent symboliquement. Des organisations terroristes profitent par ailleurs de l'audience portée par les réseaux sociaux pour diffuser une propagande destinée à attirer des volontaires et terroriser des populations. Ces différents groupes bénéficient d'un impact médiatique constant.

Sur le plan économique, la tendance du début de la décennie se confirme. Un petit nombre d'entreprises, portées par les États qui ont permis leur développement, utilisent leur avance technologique, leur domination sur le marché et leurs capacités financières pour préempter l'innovation numérique. Cette privatisation du cyberespace au profit de quelques monopoles condamne les autres acteurs du numérique à la dépendance et capte une part trop importante de la valeur ajoutée du numérique pour que cette situation soit supportable par les économies des autres pays.

« S'il porte la croissance du monde, le cyberespace est devenu un lieu de compétition souvent déloyale et de conflits »

S'il porte la croissance du monde, le cyberespace est devenu un lieu de compétition souvent déloyale et de conflits, jusqu'à présent de basse intensité informatique, de déstabilisation politique et d'hégémonie économique.

L'Europe a su identifier ces enjeux et tente d'apporter par le discours et la réglementation des idées et des solutions plus respectueuses d'un développement numérique durable, tant en matière de gouvernance d'Internet que de protection des données personnelles ou de sécurité informatique des opérateurs essentiels à l'économie. L'Europe, qui a adopté en 2013 une stratégie de cybersécurité, peine toutefois à oser une autonomie stratégique numérique et à se doter des outils nécessaires à un rééquilibrage du cyberespace en sa faveur, bien que ce sujet soit désormais inscrit à l'ordre du jour de nombreuses enceintes de discussions et négociations européennes.

Parce qu'elle partage des valeurs communes avec d'autres États membres de l'Union européenne, la France doit y avoir avec eux un rôle moteur en matière de numérique.

La France veut participer à la transformation numérique de l'Europe par des alliances. L'Europe s'est construite hier par une alliance autour de matières premières. L'Europe numérique se construira sur des alliances, de la confiance et la maîtrise des données, matières premières des prochaines décennies.

OBJECTIF

La France sera, avec les États membres volontaires, le moteur d'une autonomie stratégique numérique européenne. Elle jouera un rôle actif dans la promotion d'un cyberespace sûr, stable et ouvert.

ORIENTATIONS

> **Établir avec les États-membres volontaires une feuille de route pour l'autonomie stratégique numérique de l'Europe.**

Ouverte aux États membres de l'Union européenne, cette feuille de route déterminera les facteurs-clés de succès de la mise en place à court terme des politiques propices à l'émergence d'une autonomie stratégique numérique européenne, notamment en matière de réglementation, de normalisation et de certification, de recherche et développement, de confiance dans le numérique, — en veillant au respect de la souveraineté des États membres, de protection de la vie privée et des données personnelles conçues comme un bien d'intérêt public.

De la même manière, la France veillera à ce que les traités internationaux négociés au nom de l'Europe ne conduisent pas à la dépendance technologique ou économique des acteurs européens et à l'aliénation des données personnelles de ses citoyens ou des données sensibles de ses administrations, sources de déstabilisation du cyberespace.

Il s'agira de faire de l'Europe le territoire numérique le plus respectueux des droits fondamentaux et individuels et de mettre en place, dans le sens des travaux précurseurs entre la France et l'Allemagne relativement à l'informatique en nuage ou à l'échange chiffré de courriels entre les deux pays, une zone de confiance et de prospérité économique.

> **Renforcer la présence et l'influence française dans les discussions internationales sur la cybersécurité.**

Afin de renforcer la confiance à l'échelle internationale et d'explorer de nouveaux mécanismes de régulation visant à prévenir les conflits dans le cyberespace, la France renforcera ses contacts avec toutes les parties prenantes disposées à engager le dialogue sur les enjeux de cybersécurité.

La participation aux négociations multilatérales sur la cybersécurité (ONU, OSCE) sera accentuée afin de consolider un socle global d'engagements de bonne conduite pour les États dans le cyberespace, dans le respect du droit international.

Les contacts bilatéraux seront renforcés, dans le cadre notamment des dialogues diplomatiques à vocation interministérielle sur les enjeux relatifs au cyberespace, pilotés par le ministère des Affaires étrangères et du Développement international.

Enfin, dans une logique d'influence, la France investira davantage les forums internationaux plus informels dans lesquels les communautés techniques et académiques et les décideurs politiques pensent ensemble les équilibres à venir.

> Contribuer à la stabilité globale du cyberespace en soutenant les pays volontaires dans la mise en place de capacités de cybersécurité .

La transition numérique, porteuse d'opportunités politiques, sociales et économiques, est loin d'être maîtrisée de manière homogène dans tous les pays. Cela porte préjudice à la sécurité et au développement des États les moins protégés, et fragilise à l'échelle internationale, l'ensemble de l'écosystème numérique.

Afin de contribuer à un déploiement fiable et soutenable des technologies numériques dans l'ensemble des pays, et en particulier les pays en voie de développement, la France se doit de contribuer au renforcement capacitaire des pays souhaitant accroître la résilience et la sécurité de leurs systèmes d'information, notamment en matière de protection des infrastructures critiques et de lutte contre la cybercriminalité.

Afin d'assurer la durabilité et la soutenabilité des projets de renforcement des capacités, la France inscrira de préférence son action dans des partenariats de confiance à long terme. Cette action devra également permettre à la France de renforcer sa propre cybersécurité.