Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

SGDSN

DOSSIER DE PRESSE

STRATÉGIE NATIONALE

POUR LA SÉCURITÉ DU NUMÉRIQUE

#StratSecNum

16 OCTOBRE 2015

SOMMAIRE

Communiqué de presse
Paris, le 16 octobre 2015

LA FRANCE SE DOTE D'UNE STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE

Le 16 octobre 2015, Monsieur Manuel Valls, Premier ministre, rend publique la Stratégie nationale pour la sécurité du numérique, destinée à accompagner la transition numérique de la société française en présence de Madame Axelle Lemaire, Secrétaire d'État chargée du numérique, de Monsieur Louis Gautier, Secrétaire général de la défense et de la sécurité nationale, et de Monsieur Guillaume Poupard, Directeur général de l'Agence nationale de la sécurité des systèmes d'information.

Cette stratégie nationale pour la sécurité du numérique a fait l'objet de travaux interministériels coordonnés par l'ANSSI ; ses objectifs ont été consolidés par la Secrétaire d'État chargée du numérique et le Secrétaire général de la défense et de la sécurité nationale.

Cette nouvelle stratégie, qui a pour ambition de répondre aux nouveaux enjeux nés des évolutions des usages numériques et des menaces qui y sont liées, compte cinq objectifs : garantir la souveraineté nationale par des mesures propres à renforcer la sécurité des infrastructures critiques ; apporter une réponse forte contre les actes de cybermalveillance affectant les systèmes d'information de l'État, des entreprises et des particuliers ; sensibiliser et former à la cybersécurité ; faire de la sécurité numérique un vecteur de compétitivité et renforcer la voix de la France à l'international par le soutien à une autonomie stratégique européenne cyber et l'appui aux pays émergents désireux de contribuer à la stabilité du cyberespace.

Elle sera progressivement mise en œuvre dans les mois à venir par l'ensemble des acteurs concernés. Cette Stratégie est un engagement de l'État au bénéfice de la sécurité des systèmes d'information pour aller ensemble, par une réponse collective et coordonnée vers la confiance numérique propice à la stabilité de l'État, au développement économique et à la protection des citoyens.

À propos du SGDSN

Service du Premier ministre travaillant en liaison étroite avec le président de la République, le secrétariat général de la défense et de la sécurité nationale (SGDSN) assiste le chef du gouvernement dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

Contact : *armelle.ceglec@sgdsn.gouv.fr*

À propos de l'ANSSI

En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'ANSSI assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

Contact : *communication@ssi.gouv.fr – 01.71.75.84.04*

POURQUOI UNE STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE ?

La numérisation de la société française s'accélère : la part du numérique dans les services, les objets, et les métiers ne cesse de croître. Enjeu national, cette transition numérique est porteuse d'innovation et de croissance, mais aussi de risques pour l'État, les acteurs économiques et les citoyens. La confiance et la sécurité dans le numérique appellent une réponse collective et coordonnée pour faire face à des pratiques criminelles, délictuelles ou déloyales — cybercriminalité, espionnage, propagande, sabotage ou exploitation excessive de données personnelles.

Annoncée par la stratégie numérique du Gouvernement, la « République numérique en actes » présentée le 18 juin 2015 et avant le prochain débat au Parlement sur le projet de loi numérique porté par le secrétariat d'État chargé du numérique, le Premier ministre a validé une stratégie, élaborée avec l'ensemble des ministères, destinée à accompagner la transition numérique de la société française, à accompagner les entreprises du numérique et à défendre nos intérêts fondamentaux.

Cette Stratégie nationale pour la sécurité du numérique succède à la stratégie de défense et de sécurité des systèmes d'information adoptée en 2010. Elle vient rappeler que la sécurité de l'écosystème numérique est une responsabilité partagée : responsabilité de l'État dans la protection des citoyens et des infrastructures critiques, dans l'organisation de la défense et de la sécurité des systèmes d'information ; responsabilité des acteurs économiques dans la sécurité des produits et services qu'ils proposent ; responsabilité des citoyens dans l'exercice de leur vie numérique.

QUELS OBJECTIFS À LA STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE ?

1

« 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. »

Garantir la souveraineté et assurer la sécurité des infrastructures critiques en cas d'attaque informatique majeure : des capacités d'anticipation et une réglementation renforcées.

En construisant une pensée stratégique autonome soutenue par une expertise technique de premier plan, la France se donne les moyens de défendre ses intérêts fondamentaux :

> par le développement des capacités scientifiques, techniques et industrielles nécessaires
La France dispose de capacités techniques de premier plan. Pour les conserver et anticiper les besoins à venir, un groupe d'experts pour la confiance numérique interviendra dans l'identification de nouvelles technologies de sécurité et dans la définition d'offres de formation supérieure *ad hoc* en matière de cybersécurité.

> par le renforcement de la sécurité des infrastructures vitales
Les travaux engagés dans le cadre de la mise en œuvre des dispositions visant à renforcer la sécurité des systèmes d'information des opérateurs d'importance vitale prévues dans la loi n° 2013-1168 du 18 décembre 2013 seront complétés par les possibilités portées par le projet de directive européenne « *Network Information Security* » *(NIS)*, en phase finale de négociation.

2

« 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. »

Protéger tous les citoyens et lutter contre la cybercriminalité : de nouveaux dispositifs en faveur de la protection des données personnelles.

Le cyberespace doit être un espace de confiance. Des mesures de protection et de réaction seront adoptées pour protéger la vie numérique des Français :

> Lancement d'une feuille de route « identité numérique »
Cette feuille de route a pour objectif de renforcer la confiance des utilisateurs dans leur vie numérique tout en limitant le risque d'une exploitation non désirée de leurs données. Elle sera élaborée avant la fin de l'année 2015 sous l'égide du ministère 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.

> Création du Dispositif national d'assistance aux victimes d'actes de de cybermalveillance
Ce dispositif national mis en place dès 2016 fournira une assistance aux victimes d'acte de cybermalveillance. Les travaux préliminaires ont été menés par le ministère de l'Intérieur et l'Agence nationale de la sécurité des systèmes d'information, avec l'appui des ministères de la Justice, de l'Économie, de l'Industrie et du numérique, des Finances et des comptes publics, du secrétariat d'État chargé du Numérique

3

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

Sensibiliser, former, informer.

La prise de conscience individuelle et collective des risques liés à la numérisation de la société reste insuffisante. Plusieurs initiatives seront lancées pour encourager l'application des bonnes pratiques informatiques dont :

> Appel à la réalisation de contenus de sensibilisation à destination des écoles et du grand public
Cet appel sera mené 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.

4

« La France développera un écosystème favorable à la recherche et à l'innovation et fera de la sécurité 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 de confiance et de sécurité adaptés aux usages et aux cybermenaces. »

Faire de la sécurité numérique un facteur de compétitivité : soutien à l'innovation et labellisation.

L'enjeu est d'aider les entreprises françaises à fournir des produits et services numériques parmi les mieux sécurisés au monde afin de leur donner un avantage concurrentiel. Par le soutien à l'investissement, à l'innovation, à l'export et par le biais de la commande publique, l'État concourt à créer un environnement favorable aux entreprises françaises qui proposent une offre de produits et de services sécurisés. Parmi les mesures engagées :

> Développement d'une offre nationale et européenne
La démarche initiée par le Plan « Cybersécurité » de la Nouvelle France industrielle devenu la solution « Confiance numérique » sera accentuée.

> Renforcement capacitaire du secteur privé dans le traitement des incidents informatiques.
La labellisation de prestataires compétents et de confiance devrait permettre de répondre à la croissance des attaques informatiques subies par les entreprises.

5

« 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. »

Contribuer à l'avènement d'une Autonomie stratégique numérique européenne et au renforcement des capacités de pays alliés : la France au premier rang de l'espace cyber.

La régulation des rapports entre États dans le cyberespace est devenue un sujet majeur du droit international où la France agit en force de proposition.

> Autonomie stratégique numérique européenne
La France promouvra une feuille de route pour l'autonomie stratégique numérique avec les États membres de l'Union volontaires.

> Soutien aux pays désireux de contribuer à la stabilité du cyberespace.
La France soutiendra, à leur demande, la mise en place de capacités de cybersécurité dans les pays volontaires.

LA STRATÉGIE EN TROIS IDÉES FORTES

#1 — LA SÉCURITÉ NUMÉRIQUE, UNE RESPONSABILITÉ PARTAGÉE.

Porteur de nouveaux usages, de nouveaux produits et de nouveaux services, le numérique est facteur d'innovation et engendre de nombreuses mutations, qu'elles soient sociales (métiers, usages), économiques ou politiques (nouveaux enjeux internationaux du cyberespace).

Se priver du numérique ou ne pas pouvoir y accéder peut aujourd'hui mener 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 de la part de l'État, des administrations, des entreprises et des citoyens peut permettre d'atteindre cet objectif. La défense et la sécurité du numérique relèvent de la communauté nationale et pas seulement de l'action de l'État.

En lançant cette stratégie nationale pour la sécurité du numérique, l'État s'engage sur des actions concrètes à même d'élargir le périmètre de l'action publique et des acteurs impliqués.

#2 — UNE ATTEINTE SIGNIFICATIVE AUX DONNÉES PERSONNELLES DES FRANÇAIS PEUT DEVENIR UN ENJEU DE SÉCURITÉ NATIONALE.

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.

La captation massive et illicite de certains types de données personnelles et leur traitement peut en effet entraîner des atteintes à la vie privée, voire à la sécurité individuelle ou collective, ou une exploitation commerciale abusive.

Il y a, d'une part, le risque que les données soient exploitées par des oligopoles non soumis à un régime juridique suffisamment protecteur de la vie privée et traitées comme de simples marchandises, éventuellement revendues à des tiers. Il y a, d'autre part, le risque que ces données tombent aux mains de groupes cybercriminels, liés ou non à des États, qui les utilisent pour des actions d'espionnage, de propagande et de déstabilisation.

#3 — LA SÉCURITÉ NUMÉRIQUE DES PRODUITS ET SERVICES DES ENTREPRISES FRANÇAISES DOIT DEVENIR UN AVANTAGE CONCURRENTIEL

Agir dès à présent pour améliorer la sécurité et la confiance de l'offre nationale de solutions numériques, c'est renforcer leur compétitivité. La valeur de cette démarche est confirmée dans le domaine des moyens de paiement, où plusieurs entreprises nationales disposent d'une position concurrentielle au niveau mondial qui doit beaucoup à l'excellence qu'elles ont su développer et démontrer en matière de sécurité.

Les produits et services numériques ou intégrant du numérique, conçus, développés et produits en France, doivent être 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* ».

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.

Contact presse

SGDSN
armelle.ceglec@sgdsn.gouv.fr

ANSSI
+33 (0)1 71 75 84 04
communication@ssi.gouv.fr