Défense et sécurité des systèmes d'information

Stratégie de la France

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence Nationale
de la Sécurité
des Systèmes
d'Information

Prologue

Sans doute n'en avons-nous pas encore pris collectivement la mesure : dans le *Livre blanc sur la défense et de la sécurité nationale* présenté par le Président de la République en juin 2008, la sécurité des systèmes d'information émergeait, avec la dissuasion, comme un domaine dans lequel la souveraineté de la France devrait s'exprimer pleinement.

Le cyberespace peut pourtant apparaitre bien éloigné du champ de la défense et de la sécurité nationale. En vingt ans, les technologies du numérique ont fusionné nos vies personnelles et professionnelles, porté la compétitivité des entreprises à un niveau inédit, rapproché les administrations des usagers et favorisé la transparence de la vie des institutions de notre pays.

Le cyberespace, nouvelle tour de Babel, est un lieu de partage des cultures du monde, de diffusion des idées et d'informations en temps réel, un lieu d'échanges entre personnes. L'exclusion du numérique condamne les individus à l'isolement, les entreprises à la décroissance et les nations à la dépendance.

Dans le monde matériel, les destructions causées par les guerres ou le terrorisme comme les exactions des criminels sont visibles et souvent médiatisées. Dans le cyberespace, monde immatériel, les conséquences des attaques informatiques contre les systèmes d'information des États, des entreprises ou contre les ordinateurs des citoyens ne sont le plus souvent visibles que des spécialistes et restent ignorées du grand public.

Le cyberespace, nouvelles Thermopyles, est devenu un lieu d'affrontement : appropriation de données personnelles, espionnage du patrimoine scientifique, économique et commercial d'entreprises victimes de leurs concurrents ou de puissances étrangères, arrêt de services nécessaires au bon fonctionnement de l'économie ou de la vie quotidienne, compromission d'informations de souveraineté et même, dans certaines circonstances, perte de vies humaines sont aujourd'hui les conséquences potentielles ou réelles de l'imbrication entre le numérique et l'activité humaine.

Devant l'irruption du cyberespace dans le champ de la sécurité nationale et à la mesure des enjeux, le Gouvernement a décidé de doter la France d'une capacité structurée de défense et de sécurité. Il a ainsi créé en 2009 l'Agence nationale de la sécurité des systèmes d'information (ANSSI), autorité au service des pouvoirs publics, des entreprises et des citoyens. Le Président de la République a décidé en juillet dernier de confier à l'Agence, en complément de sa mission de sécurité, une mission de défense des systèmes d'information.

L'objectif de ce document est de préciser les grandes lignes de la stratégie poursuivie par la France depuis la publication du *Livre blanc sur la défense et la sécurité nationale* afin de garantir, dans le cyberespace, la sécurité de nos compatriotes, de nos entreprises et de la Nation.

Francis DELON

Secrétaire général de la défense et de la sécurité nationale

Les mots suivis d'un astérisque sont définis dans le glossaire.

Crédits Photos :

couverture	Jean Mottershead (CC BY-NC-ND 2.0), ou libres de droits
page 11	Ruby MV (CC BY-NC-SA 2.0)
page 12	Simon BISSON (CC BY-NC-ND 2.0)
page 13	MrFenwick (CC BY-NC-ND 2.0)
page 14	Runran (CC BY-SA 2.0)

Sommaire

Synthèse

Parmi les menaces majeures auxquelles la France sera confrontée dans les quinze prochaines années, le *Livre blanc sur la défense et la sécurité nationale* de 2008 a retenu l'attaque informatique de grande envergure contre les infrastructures nationales. Ce constat a conduit le Gouvernement à décider de renforcer significativement les capacités nationales en matière de cyberdéfense. La création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en 2009, a été la première étape de cet engagement.

Exposée dans le présent document, la stratégie nationale en matière de défense et de sécurité des systèmes d'information incarne l'ambition affichée par le *Livre blanc*.

Elle repose sur quatre objectifs.

1. Être une puissance mondiale de cyberdéfense

Tout en conservant son autonomie stratégique, la France doit effectuer l'effort nécessaire pour appartenir au premier cercle très restreint des nations majeures dans le domaine de la cyberdéfense. Nous bénéficierons ainsi de l'effet démultiplicateur des coopérations tant au plan opérationnel que pour la mise en place d'une stratégie unifiée face à des menaces communes.

2. Garantir la liberté de décision de la France par la protection de l'information de souveraineté

Les autorités gouvernementales comme les acteurs de la gestion des crises doivent disposer des moyens de communiquer en toute situation et en toute confidentialité. Les réseaux qui répondent à ce besoin doivent être étendus, notamment à l'échelon territorial.

La confidentialité de l'information qui transite par ces réseaux nécessite la réalisation de produits de sécurité maîtrisés. Nous devons conserver les compétences nécessaires à leur conception et optimiser leurs modes de développement et de production.

3. Renforcer la cybersécurité des infrastructures vitales nationales

Le fonctionnement de notre société dépend de manière croissante des systèmes d'information et des réseaux, notamment d'Internet. Une attaque réussie contre un système d'information critique ou contre l'Internet français peut entraîner des conséquences humaines ou économiques graves. Il importe que l'État, en liaison étroite avec les équipementiers et les opérateurs concernés, travaille à garantir et à améliorer la sécurité de ces systèmes critiques.

4. Assurer la sécurité dans le cyberespace

Les menaces qui pèsent sur les systèmes d'information touchent tout à la fois les administrations, les entreprises et les citoyens.

L'administration doit être exemplaire et améliorer la protection de ses systèmes d'information et des données qui lui sont confiées.

S'agissant des entreprises et des particuliers, un travail d'information et de sensibilisation doit être engagé.

En matière de lutte contre la cybercriminalité, la France encouragera le renforcement du droit et l'entraide judiciaire internationale.

Pour atteindre ces objectifs, sept axes d'effort sont retenus :

1. Mieux anticiper et analyser l'environnement afin de prendre les décisions adaptées.
2. Détecter les attaques et les contrer, alerter les victimes potentielles et les accompagner.
3. Accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines dans l'objectif de conserver l'autonomie nécessaire.
4. Protéger les systèmes d'information de l'État et des opérateurs d'infrastructures vitales pour une meilleure résilience nationale.
5. Adapter notre droit afin de prendre en compte les évolutions technologiques et les nouveaux usages.
6. Développer nos collaborations internationales en matière de sécurité des systèmes d'information, de lutte contre la cybercriminalité et de cyberdéfense pour mieux protéger les systèmes d'information nationaux.
7. Communiquer, informer et convaincre afin de permettre aux Français de prendre la mesure des enjeux liés à la sécurité des systèmes d'information.

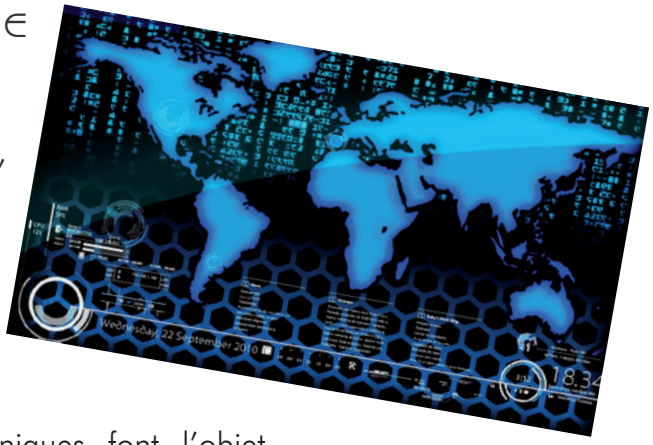
Ce document résume la partie publique des orientations et actions approuvées par le comité stratégique de la sécurité des systèmes d'information institué par le décret n° 2009-834 du 7 juillet 2009 portant création de l'agence nationale de la sécurité des systèmes d'information* (ANSSI).

« La France doit garder un domaine de souveraineté, concentré sur les capacités nécessaires au maintien de l'autonomie stratégique et politique de la nation : la dissuasion nucléaire, le secteur des missiles balistiques, les sous-marins nucléaires d'attaque, la sécurité des systèmes d'information font partie de ce premier cercle. »

« Défense et sécurité nationale, le livre blanc », p.318

Quatre objectifs stratégiques

I. Être une puissance mondiale de cyberdéfense



Le développement de la société de l'information, porté par les réseaux de communications électroniques, parce qu'il crée de la valeur et de nombreux emplois, est un formidable moteur de notre croissance. Il contribue fortement à la compétitivité du tissu économique national et donc au rang de la France dans le monde.

Or, les réseaux de communications électroniques font l'objet d'activités illicites menées directement ou indirectement par des États. Certains se livrent à des opérations massives d'espionnage via ces réseaux et cherchent à obtenir des informations de souveraineté, comme celles relevant du secret de la défense nationale ou encore du patrimoine scientifique, technologique, commercial ou financier des entreprises de nos secteurs stratégiques.

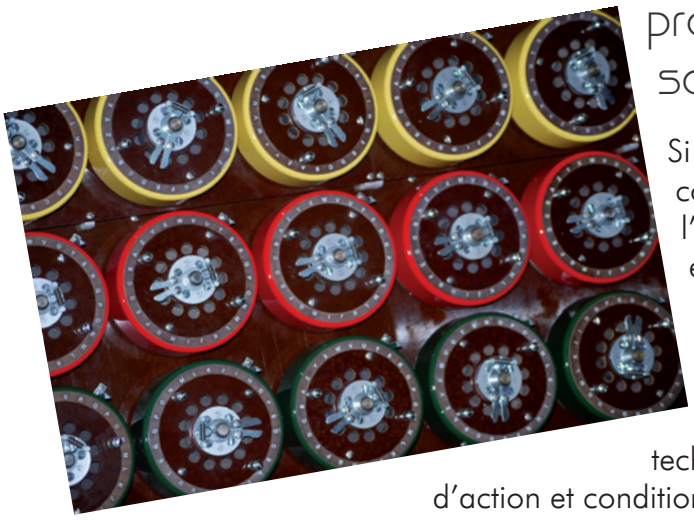
De leur côté, des groupes terroristes utilisent ces mêmes réseaux de communications électroniques pour propager leurs idées, diffuser de l'information opérationnelle à leur organisation et se livrer à des activités de propagande.

Dans un avenir proche, États ou groupes terroristes pourraient attaquer les infrastructures vitales d'États considérés comme idéologiquement hostiles.

Il est donc indispensable que la France se dote d'une capacité de cyberdéfense.

Or, contrairement à ceux du monde matériel, les affrontements dans le cyberespace ne connaissent pas les frontières. Ainsi, une cyberdéfense crédible ne peut être uniquement nationale et doit s'appuyer sur un réseau d'alliés avec lesquels il est possible d'échanger, en temps réel, des informations sur les vulnérabilités, les dispositifs de protection, les attaques et les parades à mettre en œuvre face aux agressions menées dans le cyberespace directement ou indirectement par des États ou des groupes terroristes. La France renforcera ses partenariats opérationnels avec ses alliés les plus proches et mettra à profit son expertise pour contribuer activement à la formulation des politiques de cyberdéfense au sein des organisations internationales, et notamment au sein de l'Union européenne.

2. Garantir la liberté de décision de la France par la protection de l'information de souveraineté



Si l'évolution de la société tend à imposer comme règle l'existence et le partage de l'information et son accès, à la fois instantané et sous de multiples formes, une part de l'équilibre du monde réside toujours dans la capacité à maintenir secrète « l'information de souveraineté », fraction de l'information diplomatique, militaire, scientifique, technique et économique qui permet la liberté d'action et conditionne la prospérité des nations.

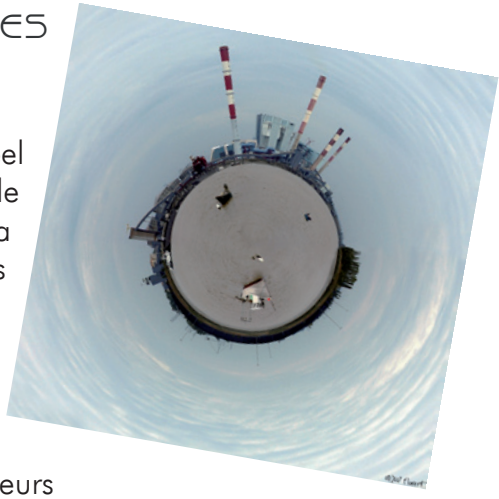
Comme par le passé, les services de renseignement du monde entier, parmi d'autres acteurs, tentent d'obtenir l'information de souveraineté. Les réseaux de télécommunications, notamment Internet, les informations qui y circulent, celles disponibles sur les réseaux ou les terminaux qui s'y connectent, sont devenus à la fois sources d'information et vecteurs de collecte.

Le moyen le plus efficace pour protéger l'information de souveraineté est d'utiliser des techniques de cryptographie* qui rendent impossible, ou du moins retardent, sa compréhension si cette information venait à être altérée, divulguée ou interceptée. Les progrès de la cryptanalyse*, qui suivent notamment ceux de la puissance de calcul des ordinateurs, obligent à concevoir et utiliser des méthodes et techniques plus difficiles à analyser et renouvelées régulièrement.

Le maintien de notre autonomie stratégique repose sur notre capacité à maîtriser les techniques cryptographiques et les technologies clés nécessaires à la conception de produits de sécurité* qui les utilisent, ce qui implique de veiller à ce que le domaine de la sécurité des systèmes d'information reste attractif pour les jeunes diplômés afin d'éviter le tarissement progressif des compétences.

Parallèlement à la nécessité de pouvoir communiquer de manière sûre et confidentielle, les décideurs comme les organismes associés à la gestion des situations de crise doivent avoir à leur disposition des moyens de communication disponibles en toutes circonstances. Ces moyens d'échanges électroniques, de téléphonie et de visioconférence sécurisés ont été conçus et développés. Leur déploiement va se poursuivre dans les années qui viennent, notamment au profit des opérateurs d'importance vitale*.

3. Renforcer la cybersécurité des infrastructures vitales nationales



Par la convergence de multiples technologies, le monde réel et les réseaux s'interpénètrent. De nombreux objets du monde réel — de l'étiquette de supermarché à la raffinerie, de la photocopieuse au drone de combat — embarquent des systèmes d'information et s'y intègrent. À distance, via les réseaux, il est possible de collecter les informations transmises par ces objets, de les maintenir en fonction et de les piloter.

La France a défini dans son code de la défense des secteurs d'activités d'importance vitale dans lesquels agissent des opérateurs qui concourent à la satisfaction des besoins indispensables à la vie des populations, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la Nation, dès lors que ces activités sont difficilement substituables ou remplaçables.

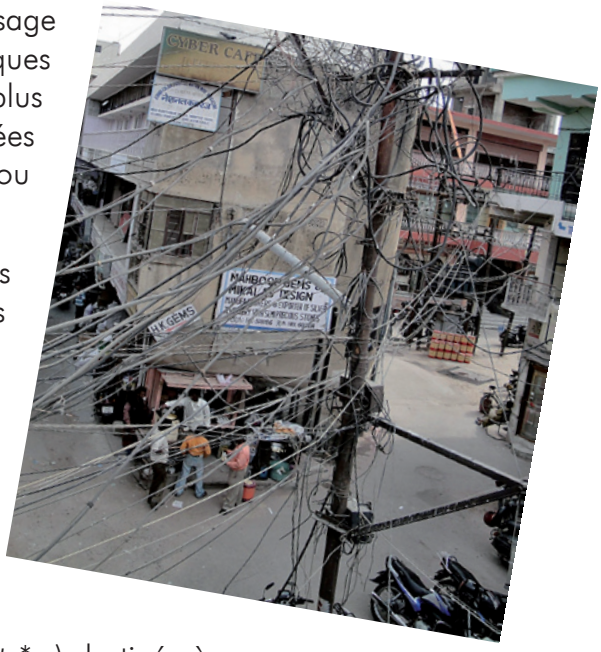
La plupart des opérateurs d'importance vitale utilisent largement les réseaux de télécommunications, et singulièrement Internet, tant pour leur gestion que pour l'exercice de leur métier. Pourtant, dans la rencontre, ancienne et pourtant inédite parce que bousculée par l'interconnexion des systèmes, entre le monde industriel et le monde de l'informatique, le premier manque de formation et de sensibilisation à la sécurité des systèmes d'information, tandis que le second méconnaît souvent les contraintes et le fonctionnement des systèmes industriels.

La dépendance de chacun des acteurs vis-à-vis d'Internet est accrue par des tendances lourdes de notre organisation économique et sociale : l'externalisation et l'informatique en nuage, la mutualisation des services supports, la gestion en temps réel et en flux tendus, le nomadisme, le transfert de tâches vers les clients ou les administrés, la création ou la réingénierie de nombreux processus.

En cas d'interruption du fonctionnement des réseaux de télécommunications ou d'Internet, les moyens de substitution peuvent s'avérer très insuffisants, notamment par manque de personnels qualifiés susceptibles de remettre en fonction les processus antérieurs à l'avènement de l'ère numérique. Dans le cas de processus directement issus de nouveaux usages liés aux technologies de l'information, les moyens de substitution n'existent pas.

Comme le démontre régulièrement l'actualité mondiale, les conséquences possibles d'actes de malveillance contre les systèmes automatisés de contrôle des processus industriels déployés par les opérateurs d'importance vitale sont aujourd'hui insuffisamment mesurées. Ainsi, la protection des réseaux de communications électroniques — et notamment d'Internet — comme la sécurisation des systèmes critiques des opérateurs d'importance vitale constituent des priorités nationales.

1. Assurer la sécurité dans le cyberespace



Pour une part croissante de nos concitoyens, l'usage des réseaux de communications électroniques comme Internet imprègne les fonctions les plus courantes de la vie quotidienne comme celles liées au commerce, aux démarches administratives ou aux échanges interpersonnels.

Parallèlement, les techniques utilisées dans le cyberespace par des individus ou groupes d'individus malveillants sont de plus en plus performantes et visent à usurper des identités, à se procurer les informations nécessaires à l'accès à des comptes bancaires ou à collecter et revendre des données personnelles. On observe également une multiplication des cas de prises de contrôle malveillantes à distance d'ordinateurs visant à les intégrer dans des réseaux de machines compromises (« *botnets** ») destinés à accomplir des actes illicites tels que des attaques informatiques ou des envois de courriels malveillants.

Dans ce contexte, les administrations doivent montrer l'exemple en protégeant le cyberespace public. Les usagers doivent utiliser en confiance les services électroniques proposés par les autorités publiques, notamment au regard de la protection de leurs données personnelles. Le référentiel général de sécurité* (RGS) publié début 2010 offre un cadre réglementaire susceptible de renforcer cette sécurité. Son respect et sa mise en œuvre par les autorités publiques sont prioritaires.

La sécurisation du cyberespace passe par une démarche systématique d'information des entreprises et des citoyens sur les risques encourus et les moyens de s'en protéger. L'objectif est qu'à terme, chaque citoyen puisse être sensibilisé aux questions de cybersécurité au cours de son éducation. Cette démarche appelle la mise en place d'une politique de communication gouvernementale active.

Enfin, Internet est un espace de droit. La France doit encourager le renforcement ou l'édiction de règles juridiques dans le cyberespace lorsque le droit existant est insuffisant et amplifier l'entraide judiciaire internationale en matière de répression des infractions commises sur ou à travers les réseaux de communications électroniques.

Afin de remplir les quatre objectifs stratégiques,
7 axes d'effort ont été retenus.

Sept axes d'effort

1. Anticiper, analyser

Risques et menaces évoluent rapidement dans le cyberespace. La parution d'un nouveau produit ou d'une nouvelle version d'un logiciel, la publication d'une faille* non corrigée d'un logiciel largement utilisé, l'apparition d'une nouvelle technologie ou d'un nouvel usage, une déclaration politique, peuvent entraîner, dans des délais très courts, une mise en danger de la sécurité des systèmes d'information.

- Dans ce contexte, la défense et la sécurité de nos systèmes d'information passe en premier lieu par un suivi de l'actualité des technologies et par une analyse, une bonne compréhension voire une anticipation du jeu des acteurs publics ou privés.

2. Détecter, alerter, réagir

Compte-tenu de la dépendance croissante à Internet des entreprises, des infrastructures et des services, et en raison des risques systémiques portés par certaines faiblesses, il est nécessaire d'être en mesure de détecter au plus tôt failles et attaques, d'alerter les victimes potentielles ou avérées et de leur proposer dans un délai bref une aide à l'analyse et à l'élaboration de parades.

- Comme l'a prévu le *Livre blanc sur la défense et la sécurité nationale*, la France développe une capacité de détection des attaques sur les systèmes d'information. Notamment déployés dans les réseaux des ministères, des dispositifs permettent d'alerter leurs responsables, d'aider à élucider la nature des attaques et d'élaborer des parades adaptées.
- Pour gérer l'ensemble des informations recueillies par les outils de détection, par les dispositifs de veille ou transmises par nos partenaires, afin de présenter une image en temps réel de la situation des réseaux nationaux et pour être capable de gérer une situation de crise, l'ANSSI se dote d'une « salle d'opération » à la hauteur des enjeux.
- Pour répondre aux crises majeures affectant ou menaçant la sécurité des systèmes d'information des autorités administratives ou des opérateurs d'importance vitale, l'État doit être en mesure de prendre rapidement les mesures nécessaires. Dans cette optique, l'ANSSI assure la fonction d'autorité nationale de défense des systèmes d'information.

3. Accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines

La sécurité des systèmes d'information repose sur une maîtrise de technologies et de savoir-faire, également accessibles aux organisations et individus qui veulent y porter atteinte. Si les acteurs étatiques de la sécurité des systèmes d'information doivent connaître « l'état de l'art », ils doivent également être en mesure d'anticiper voire de créer les évolutions technologiques en maintenant leurs capacités de recherche, seules capables de permettre de limiter l'avantage tactique de l'attaquant sur le défenseur.

La France dispose d'équipes de recherche de niveau mondial dans les domaines de la cryptologie et des méthodes formelles. Dans d'autres domaines, comme celui des architectures de sécurité des systèmes d'information, elle rattrape le niveau des nations les plus avancées.

- Pour catalyser ces travaux, la création, avec des partenaires industriels, d'un centre de recherche consacré à la cyberdéfense est à l'étude. Ce centre mènera des activités de recherche scientifique (recherche en cryptologie, étude des groupes d'attaquants et de leurs méthodes, expertise sur les logiciels malveillants et les failles informatiques, développement de logiciels libres sécurisés, élaboration de concepts de défense informatique, etc.), et des actions d'expertise et de formation.

Le développement de la société de l'information crée pour les entreprises un marché d'emblée mondial, aujourd'hui préempté par des acteurs situés hors d'Europe. S'agissant de la sécurité des systèmes d'information, cette situation n'est ni souhaitable ni tenable. La France dispose pourtant d'un tissu industriel de pointe unique en Europe, qui lui permet potentiellement de maîtriser une grande partie des technologies nécessaires à la conception de produits de sécurité, y compris en matière de composants. De nombreuses PME innovantes composent ce tissu. Elles n'ont cependant pas aujourd'hui la taille critique nécessaire et ne sont pas portées par une demande suffisante.

- Les consolidations industrielles seront favorisées par les différents moyens de l'État, notamment par les fonds d'investissement stratégique.

Pour une meilleure efficacité, les concepteurs de produits informatiques et de systèmes d'information doivent prendre en compte les questions de sécurité dès l'origine de leurs développements. L'imprégnation du tissu industriel par des experts en sécurité des systèmes d'information doit donc être renforcée. L'orientation de jeunes vers ces métiers sera encouragée afin d'accroître le vivier national de compétences.

De manière générale, les formations scientifiques et techniques dans les domaines des technologies de l'information devront intégrer un volet relatif à la sécurité des systèmes d'information.

4. Protéger les systèmes d'information de l'État et des opérateurs d'infrastructures vitales

Comme le souligne le *Livre blanc sur la défense et la sécurité nationale*, nous devons disposer « d'une offre de produits de très haute sécurité totalement maîtrisés, pour la protection des secrets de l'État, ainsi que d'une offre de produits et de services de confiance labellisés, à laquelle recourront les administrations et qui seront largement accessibles au secteur économique ». Des réseaux sécurisés résilients* pour « l'ensemble de la chaîne de décision et de commandement sur le territoire métropolitain » doivent être utilisés.

- Relevant de l'information classifiée*, la stratégie française en matière de produits de sécurité et de composants a été redéfinie. Elle prend notamment pleinement en compte le retour de la France dans le commandement intégré de l'OTAN.
- Dans les réseaux ministériels, la mise en place de systèmes d'authentification forte reposant, par exemple, sur l'utilisation de cartes à puce, domaine d'excellence française, va permettre d'en améliorer très significativement la sécurité.
- Les autorités gouvernementales disposent aujourd'hui d'un intranet sécurisé interministériel, d'un réseau de téléphonie à forte disponibilité qui sera totalement équipé de nouveaux terminaux chiffrants d'ici 2012, et d'une solution de visio-conférence protégée, en particulier destinée à équiper les centres de décision ministériels. Le déploiement de ces différents réseaux se poursuivra, notamment dans les administrations territoriales.
- Dans le domaine de la sécurité des systèmes d'information des opérateurs d'importance vitale, un partenariat public-privé sera mis en place afin, d'une part, de faire profiter les opérateurs de l'information dont dispose l'État en matière d'analyse des menaces, et d'autre part, de permettre à l'État de s'assurer que les infrastructures essentielles au bon fonctionnement de la Nation disposent d'un niveau de protection adéquat. Un travail sera également engagé avec les équipementiers.

5. Adapter notre droit

Les nouveaux usages portés par le développement du cyberespace peuvent, si l'on n'est suffisamment vigilant, présenter des dangers pour nos libertés individuelles, le fonctionnement des infrastructures vitales ou l'équilibre de nos entreprises.

Notre cadre législatif et réglementaire doit suivre l'évolution des techniques. Les textes seront adaptés en fonction de l'apparition de nouvelles technologies ou de nouveaux usages, afin de renforcer la sécurité des particuliers et avec le souci du

respect de l'équilibre entre la volonté de peser le moins possible sur la compétitivité des entreprises et la nécessité pour l'État d'être en mesure d'intervenir dans le sens de l'intérêt supérieur de la Nation.

- S'agissant des opérateurs de communications électroniques, la transposition en droit français des directives européennes va permettre d'édicter de nouvelles règles de protection des systèmes d'information et d'alerte des autorités gouvernementales en cas d'incident.
- En ce qui concerne les autorités publiques, la mise en œuvre du « référentiel général de sécurité » (RGS) et son évolution permettront de relever significativement le niveau de protection de leurs systèmes d'information, notamment dans leurs relations avec les usagers.

6. Développer nos collaborations internationales

La sécurité des systèmes d'information repose en partie sur la qualité de l'échange d'informations entre les services compétents des divers États. La France cherchera à établir un large tissu de partenaires étrangers afin de favoriser le partage des données essentielles, comme, par exemple, les informations concernant les vulnérabilités ou les failles des produits et services.

Elle renforcera également ses échanges avec ses partenaires en matière de lutte contre la cybercriminalité.

De la même manière, les relations fortes entre alliés sont la base d'une cyberdéfense efficace. La France construit un cercle très restreint de partenaires de confiance avec lesquels des échanges opérationnels très approfondis seront menés.

7. Communiquer pour informer et convaincre

La sécurité des systèmes d'information repose tant sur la vigilance personnelle que sur l'organisation, les choix et mesures techniques portés par les entreprises et l'action des États.

Devant les conséquences potentielles d'une attaque majeure contre les systèmes d'information sur la vie du pays et de ses citoyens, la sensibilisation et la motivation des personnes et des organisations doivent être assurées.

Or, en France, l'information et le débat public sur les menaces que font peser les atteintes à la sécurité des systèmes d'information sur la défense et la sécurité nationale

ou, plus simplement, sur notre vie quotidienne, restent très largement à développer.

- Un soutien ciblé sera apporté par l'ANSSI aux décideurs afin de les aider à élaborer les mesures et à prendre les décisions nécessaires en matière de sécurité des systèmes d'information essentiels au bon fonctionnement de leurs organisations et à la protection de leur patrimoine technique, scientifique, commercial ou financier.
- Plus largement, une communication appropriée sera développée par l'ANSSI vers le grand public et les entreprises.

Glossaire

Botnet

Un *botnet*, autrement dit un réseau de robots, est un réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son maître de transmettre des ordres à tout ou partie des machines du *botnet* et de les actionner à sa guise.

Remarques : certains réseaux peuvent atteindre un nombre considérable de machines (plusieurs millions). Celles-ci peuvent faire l'objet de commerce illicite ou d'actions malveillantes contre d'autres machines.

Cryptanalyse

Processus de déchiffrement de données protégées au moyen de cryptographie sans être en possession des clés de chiffrement.

Cryptographie

Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification ne passe inaperçue et/ou d'empêcher leur utilisation non autorisée (ISO 7498-2).

Cryptologie

Science englobant la cryptographie et la cryptanalyse.

Cybercriminalité

Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Cyberdéfense

Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

Cyberespace

Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

Cybersécurité

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Faille

Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Information classifiée

L'article 413-9 du code pénal indique que « les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation ou auxquels l'accès est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale » font l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.

Nétiquette

Charte établie en 1995 par l'Internet Engineering Task Force (IETF) présentant les règles de bienséance recommandées pour les échanges ayant lieu dans le cyberespace (voir charte : http://tools.ietf.org/html/rfc1855 ou http://www.sri.ucl.ac.be/rfc1855.fr.html pour une traduction française).

Glossaire

Opérateur d'importance vitale (OIV)

L'article R. 1332-1 du code de la défense précise que les opérateurs d'importance vitale sont désignés parmi les opérateurs publics ou privés mentionnés à l'article L. 1332-1 du même code, ou parmi les gestionnaires d'établissements mentionnés à l'article L. 1332-2.

Un opérateur d'importance vitale :
- exerce des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale ;
- gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.

Produit de sécurité

Dispositif matériel ou logiciel conçu pour protéger la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que les systèmes d'information offrent ou qu'ils rendent accessibles.

Résilience

En informatique, capacité d'un système d'information à résister à une panne ou à une cyberattaque et à revenir à son état initial après l'incident.

Référentiel général de sécurité (RGS)

Ensemble des règles établies par l'ANSSI et prévues par l'ordonnance n° 2005-1516 du 8 décembre 2005 « relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives » que doivent respecter certaines fonctions contribuant à la sécurité des informations, parmi lesquelles la signature électronique, l'authentification, la confidentialité ou encore l'horodatage. Les règles formulées dans le RGS s'imposent et sont modulées en fonction du niveau de sécurité retenu par l'autorité administrative dans le cadre de la sécurisation des services en ligne dont il est responsable. Ses conditions d'élaboration, d'approbation, de modification et de publication sont fixées par le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance citée relative à la sécurité des informations échangées par voie électronique. (voir http://www.ssi.gouv.fr/rgs).

Sécurité des systèmes d'information

Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Système d'information

Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information.

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence 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.

Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Février 2011

Agence nationale de la sécurité des systèmes d'information

ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr