Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

Création de l'Agence nationale de la sécurité des systèmes d'information

DOSSIER DE PRESSE

dossier de presse

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

SOMMAIRE

dossier de presse

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

COMMUNIQUÉ DE PRESSE

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009.

Le *Livre blanc sur la défense et la sécurité nationale* publié le 17 juin 2008 retient, parmi les menaces principales pesant sur le territoire national, les attaques informatiques. L'usage généralisé des technologies de l'information et de la communication ainsi que l'utilisation croissante des réseaux dans le fonctionnement de la société font de la prévention et de la réaction face aux attaques informatiques une priorité majeure de nos dispositifs de sécurité nationale. Cette nécessité a été soulignée par plusieurs rapports, notamment ceux du député Pierre LASBORDES et du sénateur Roger ROMANI.

Pour renforcer la cohérence et la capacité propre des moyens de l'État en matière de sécurité des systèmes d'information, à l'instar des principaux partenaires de la France, le *Livre blanc sur la défense et la sécurité nationale* prévoit la création d'une agence nationale de la sécurité des systèmes d'information (ANSSI). Cette agence, qui relève du Premier ministre, est rattachée au secrétaire général de la défense nationale.

Un an après la parution du *Livre blanc*, le décret publié au *Journal Officiel* le 8 juillet 2009 crée l'ANSSI à la suite d'une mission de préfiguration mise en place dès le 1er janvier 2009. Cette agence se substitue à la direction centrale de la sécurité des systèmes d'information (DCSSI) du secrétariat général de la défense nationale (SGDN) tout en en renforçant les compétences, les effectifs et les moyens.

La création de l'agence nationale de la sécurité des systèmes d'information est une étape marquante dans la mise en place progressive d'une capacité de protection renforcée des systèmes d'information sensibles français.

L'agence nationale de la sécurité des systèmes d'information a notamment pour missions :

- de détecter les attaques informatiques et de réagir au plus tôt, grâce à un centre opérationnel renforcé de cyberdéfense, actif 24 heures sur 24, chargé de la surveillance permanente des réseaux les plus sensibles de l'administration et de la mise en œuvre de mécanismes de défense adaptés ;
- de prévenir la menace : l'agence contribuera au développement d'une offre de produits et de services de confiance pour les administrations et les acteurs économiques ;
- de jouer un rôle permanent de conseil et de soutien aux administrations et aux opérateurs d'importance vitale ;
- d'informer régulièrement les entreprises et le grand public sur les menaces et les moyens de s'en protéger, en développant une politique de communication et de sensibilisation active.

Contacts presse : Marie NAUDON, SGDN (01 71 75 80 04) et Jérôme RABENOU, ANSSI (01 71 75 84 04)

dossier de presse

L'ANSSI : DES ATTRIBUTIONS ELARGIES

L'agence nationale de la sécurité des systèmes d'information (ANSSI) se substitue à la direction centrale de la sécurité des systèmes d'information (DCSSI) du secrétariat général de la défense nationale (SGDN) et ses attributions sont élargies.

Désormais, outre les missions assurées auparavant par la DCSSI, l'ANSSI assure la mission **d'autorité nationale en matière de sécurité des systèmes d'information**. A ce titre elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées.

Dans le domaine de la défense informatique, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. L'agence **va créer un centre de détection précoce des attaques informatiques**.

S'agissant des produits et des réseaux de sécurité, elle est chargée :

- **de développer et d'acquérir les produits essentiels** à la protection des réseaux non-militaires les plus sensibles de l'État ;
- de **mettre en œuvre les moyens gouvernementaux sécurisés de commandement et de liaison** interministériels, notamment le réseau téléphonique Rimbaud et l'intranet Isis.

Elle constitue un **réservoir de compétences** qui doit pouvoir mettre son expertise et son assistance technique au profit des administrations et des opérateurs d'importance vitale.

Elle est chargée de la **promotion des technologies**, des systèmes et des savoir-faire nationaux. Elle contribue au **développement de la confiance dans l'économie numérique**.

Elle assure la **tutelle du centre de transmission gouvernemental** chargé de mettre en œuvre les moyens sécurisés de commandement et de liaison nécessaires au Président de la République et au Gouvernement.

La gouvernance de l'agence s'exercera au travers d'un **comité stratégique** constitué de responsables de haut niveau de l'administration. La mission de ce comité sera d'orienter la stratégie de l'État en la matière et d'arrêter le programme annuel d'activité de l'agence.

LES MISSIONS DE L'ANSSI

La Direction de l'ANSSI est constituée d'un directeur général assisté par un directeur général adjoint. Une cellule de communication lui est rattachée.

L'Agence est organisée en quatre sous-directions et un centre de formation qui reflètent ses principales missions :

1. Cyberdéfense
2. Stratégie et réglementation
3. Assistance, conseil et expertise
4. Développement des systèmes d'information sécurisés
5. Formation

1. Cyberdéfense

Le centre opérationnel de la sécurité des systèmes d'information (COSSI) assure un service permanent de veille, de détection et d'alerte en cas d'incidents ou de vulnérabilités susceptibles d'affecter la sécurité des systèmes d'information de l'État et plus largement de la société de l'information. Il coordonne la réaction à ces incidents.

Il est chargé de la planification des mesures de réponse aux attaques informatiques et conduit des exercices afin de mesurer le degré de préparation de l'État et d'entraîner les personnels concernés.

Pour l'accomplissement de ses missions, le COSSI entretient des relations opérationnelles avec ses homologues notamment étrangers, les industriels du secteur des technologies de l'information et de la communication, les opérateurs de communications électroniques et les opérateurs d'importance vitale.

Il dispose d'une capacité d'audit pour évaluer la sécurité des systèmes d'information des services de l'État. Cette capacité peut également être utilisée dans le cadre du contrôle qu'exerce l'État sur les opérateurs d'importance vitale. Elle vient renforcer la capacité de gestion de crise en cas de besoin.

2. Stratégie et réglementation (SR)

L'agence coordonne la mise en œuvre de la fonction d'autorité nationale dans le domaine de la sécurité des systèmes d'information. A ce titre elle est chargée de :

- la gouvernance, la préparation de la stratégie nationale, l'animation interministérielle ;
- la préparation des textes réglementaires ;
- la labellisation de produits et de services ;
- l'organisation et le suivi des relations internationales et industrielles ;
- l'instruction des dossiers de déclaration et d'autorisation relatifs aux produits réglementés.

3. Assistance, conseil et expertise (ACE)

L'agence apporte son concours aux administrations et aux opérateurs d'importance vitale pour la sécurisation de leurs systèmes d'information.

Elle est également chargée de définir les recommandations générales, les référentiels techniques et les guides méthodologiques.

Elle dispose de laboratoires techniques de haut niveau, aptes à anticiper les évolutions technologiques et à les sécuriser (cryptologie, réseaux, composants, signaux...).

4. Développement des systèmes d'information sécurisés (SIS)

L'agence est chargée de la conception, de la réalisation et des évolutions de systèmes d'information sécurisés et de produits de sécurité.

Elle veille notamment à la mise à disposition de moyens sécurisés de communication électronique, disponibles en toutes circonstances pour les plus hautes autorités gouvernementales, ainsi que pour les autorités publiques et les organismes associés à la gestion des situations d'urgence et des crises.

5. Formation

L'agence dispose d'un centre de formation à la sécurité des systèmes d'information (CFSSI). Ce dernier dispense des enseignements spécialisés qui vont de la sensibilisation à la formation d'experts en cryptologie ou en systèmes. Il dispense la formation d'expert en sécurité des systèmes d'information (ESSI), sanctionnée par un titre de niveau I (Bac +5). Chaque année, il forme plus de 1500 agents publics.

LES MOYENS DE l'ANSSI

De quels moyens l'ANSSI dispose-t-elle ?

Effectifs

Les effectifs de l'agence nationale de la sécurité des systèmes d'information (ANSSI) seront sensiblement renforcés au cours des prochaines années. A l'horizon 2012, l'agence devrait compter 250 personnes, soit un doublement des effectifs actuels.

Le soutien de l'agence est assuré par le secrétariat général de la défense nationale (SGDN). Hors les fonctions de direction et de secrétariat, la totalité de l'effectif est affectée à l'activité directement productive de l'agence.

Moyens financiers

La création de l'agence s'accompagne d'un effort financier destiné, d'une part, à créer le centre de détection des attaques informatiques, et d'autre part, à permettre l'accroissement des compétences et des moyens humains. Les crédits d'investissement, de masse salariale et de fonctionnement courant connaîtront ainsi une progression significative, en cohérence avec cette montée en puissance, pour atteindre une somme d'environ 90 millions d'euros en 2012.

LES NOUVELLES MENACES

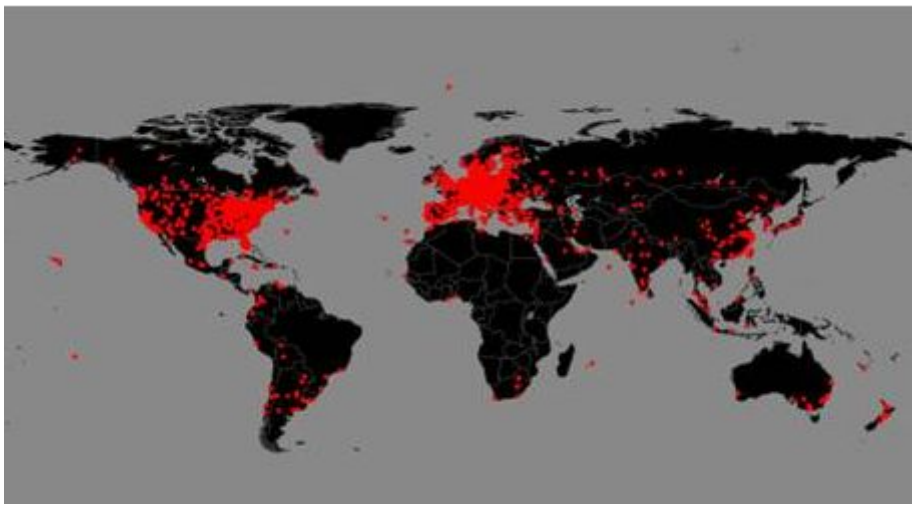
Depuis sa création, le centre opérationnel de la sécurité des systèmes d'information (COSSI) identifie chaque année un nombre croissant d'attaques. Même si les messages non sollicités (spam) et les défigurations de sites Internet constituent les attaques les plus visibles, ils ne forment en fait que le bruit de fond de l'Internet. De nouvelles formes de cybercriminalité, telles que les réseaux de *botnet* et les attaques ciblées (furtives ou non), constituent de véritables menaces stratégiques.

La généralisation des attaques ciblées

L'utilisation de codes malveillants (chevaux de Troie…) dans le but de dérober des informations sensibles ne se limite pas au champ des activités sensibles des États. Elle touche l'ensemble des activités dans lesquelles la compétition existe, entre États ou entre entreprises, qui constituent une cible de choix pour les pirates. Le glissement observé d'attaques massives, au moyen de virus informatiques médiatisés, vers des attaques plus ciblées et plus discrètes, est le résultat d'une importante professionnalisation des pirates informatiques, désormais motivés par le gain et non plus par la reconnaissance de leur savoir-faire. Ceux-ci peuvent également mettre à disposition des officines, des entreprises, voire des États, moyennant rétribution, leurs moyens techniques ou leur savoir faire.

Des réseaux de *botnets* aux capacités redoutables

Les *botnets*, vastes réseaux d'ordinateurs infectés contrôlés à distance, offrent aux agresseurs des capacités d'attaques sans limite. Aujourd'hui essentiellement utilisés pour diffuser massivement des messages non sollicités, ils peuvent également servir à mener des opérations de blocage (déni de service). Ainsi les attaques menées contre l'Estonie en 2007 ont été très largement réalisées par le biais de réseaux de *botnets*. Lorsque l'on sait que les plus gros réseaux ont atteint le million de machines compromises et que les attaques en Estonie ont été réalisées à partir de quelques milliers d'ordinateurs, on comprend mieux la menace représentée par ces réseaux.



Exemple d'un réseau de *botnets*

dossier de presse

L'utilisation systématique des attaques informatiques comme moyen de protestation

En 2006, suite à la publication des caricatures du prophète Mahomet dans les journaux *France Soir* et *Charlie Hebdo*, des sites Internet français ont été défigurés. De nombreux autres l'ont été lors des débats puis de l'adoption par l'Assemblée nationale de la proposition de loi visant à sanctionner la négation du génocide arménien en octobre 2006.

Cette évolution a atteint un niveau jamais observé auparavant à l'occasion des attaques informatiques subies par l'Estonie en 2007. Les cyber-attaques ont été lancées entre le 27 avril et le 10 mai 2007, après la décision des autorités estoniennes de déplacer du centre de Tallin un mémorial de guerre datant de l'époque soviétique. Cet évènement a provoqué des émeutes et différentes attaques informatiques visant des sites Internet gouvernementaux et privés (médias, banques) estoniens. Ces attaques visaient à rendre inaccessibles les sites Internet gouvernementaux mais également à rendre inutilisable l'ensemble de l'Internet estonien.

En 2009, en Iran, plusieurs défigurations de sites gouvernementaux ont été constatées suite à la publication des résultats de l'élection présidentielle du 12 juin.

La vulnérabilité des systèmes de commande et de contrôle industriels

Apparus dans les années 1960, les systèmes SCADA (*Supervisory Control and Data Acquisition*) sont utilisés dans la plupart des processus industriels pour assurer en temps réel l'acquisition des données, la supervision et le contrôle des processus. Ils sont présents dans de nombreux secteurs d'activités d'importance vitale, comme le transport et la production d'énergie, la transformation de produits chimiques et d'hydrocarbures, le contrôle de la qualité de l'eau et des effluents. Ces systèmes, conçus pour optimiser la disponibilité et l'efficacité des processus industriels, peuvent présenter des vulnérabilités qui pourraient être exploitées à des fins malveillantes.

Quelques chiffres

En 2008, près d'un million de sites Internet ont été défigurés dans le monde.

Le filoutage (phishing) qui consiste à jouer de la crédulité des internautes afin de dérober des informations confidentielles ou sensibles explose littéralement depuis 2005. Les établissements bancaires et les opérateurs de télécommunications électroniques sont très régulièrement touchés.

En 2008, le centre opérationnel de la sécurité des systèmes d'information (COSSI) a ainsi fait fermer plus de 2200 sites de filoutage, contre 400 en 2006.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

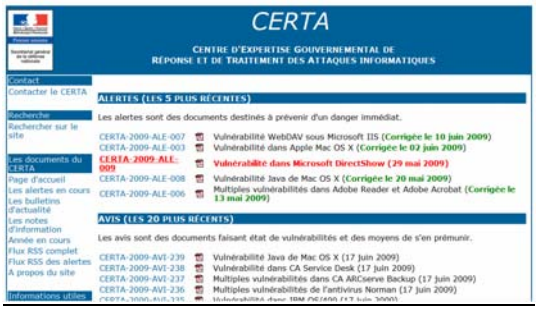
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

LES SITES INTERNET DE L'ANSSI

Le nouveau site de l'ANSSI
http://www.ssi.gouv.fr

(L'ancien site reste disponible pendant la durée de son transfert)

Le site du Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA)
http://www.certa.ssi.gouv.fr



Le portail de la sécurité informatique
http://www.securite-informatique.gouv.fr

dossier de presse

EXTRAITS DU *LIVRE BLANC SUR LA DEFENSE ET LA SECURITE NATIONALE*

Page 53

Attaques informatiques majeures

« Les moyens d'information et de communication sont devenus les systèmes nerveux de nos sociétés, sans lesquels elles ne peuvent plus fonctionner. Or le « cyberespace », constitué par le maillage de l'ensemble des réseaux, est radicalement différent de l'espace physique : sans frontière, évolutif, anonyme, l'identification certaine d'un agresseur y est délicate.

La menace est multiforme : blocage malveillant, destruction matérielle (par exemple, de satellites ou d'infrastructures de réseau névralgiques), neutralisation informatique, vol ou altération de données, voire prise de contrôle d'un dispositif à des fins hostiles.

Dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une *certitude*. Certaines d'entre elles pourront être de grande ampleur.

S'agissant des *attaques d'origine étatique*, plusieurs pays ont déjà défini des stratégies de lutte informatique offensive et se dotent effectivement de capacités techniques relayées par des pirates informatiques. Dans ce contexte, les tentatives d'attaques dissimulées sont hautement probables. Des actions massives, menées ouvertement, sont également plausibles.

L'évolution des technologies et l'interconnexion des réseaux rendent les seules stratégies de défense passive et périmétrique (de « ligne ») de moins en moins efficaces, même si elles restent nécessaires. *Le passage d'une stratégie de défense passive à une stratégie de défense active en profondeur, combinant protection intrinsèque des systèmes, surveillance permanente, réaction rapide et action offensive, impose une forte impulsion gouvernementale et un changement des mentalités.*

L'expertise de l'État en sécurité des systèmes d'information doit être fortement développée, entretenue et diffusée auprès des acteurs économiques et notamment des opérateurs de réseaux.
La nature immédiate, quasi imprévisible, des attaques exige aussi de se doter d'une capacité de gestion de crise et d'après-crise, assurant la continuité des activités et permettant la poursuite et la répression des agresseurs. »

Pages 182-183

Protéger les systèmes d'information sensibles

« Face à une menace croissante d'origine étatique ou non étatique, la France doit se doter à court terme d'une capacité réactive de défense de ses systèmes d'information.

Seront développés, à cette fin, nos moyens de détection précoce des attaques informatiques en mettant sur pied un centre de détection chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre de mécanismes de défense adaptés.

Afin de prévenir la menace, le recours à des produits de sécurité et à des réseaux de confiance sera généralisé. Ce besoin implique de disposer de capacités industrielles nationales suffisantes, développant une offre de produits de très haute sécurité totalement maîtrisés pour la protection des secrets de l'État, ainsi qu'une offre de produits et de services de confiance labellisés à laquelle recourront les administrations et qui seront largement accessibles au secteur économique.

Des dispositions réglementaires seront également prises pour que les opérateurs de communications électroniques mettent en œuvre les mesures techniques et d'organisation nécessaires à la protection de leurs réseaux contre les pannes et les attaques les plus graves. À ce titre, le réseau Internet devra être considéré comme une infrastructure vitale et un effort important devra être mené pour améliorer sa résilience.

Pour renforcer la cohérence et la capacité propre des moyens de l'État, une agence chargée de la sécurité des systèmes d'information sera créée. Relevant du Premier ministre et de la tutelle du SGDSN, elle reprendra, tout en les renforçant sensiblement, les effectifs et les moyens de la direction du SGDN qui est actuellement chargée de cette mission. Elle mettra en œuvre une capacité centralisée de détection et de défense face aux attaques informatiques. Elle sera dotée des moyens de faire développer et d'acquérir les produits de sécurité essentiels à la protection des réseaux les plus sensibles de l'État. Elle sera également chargée d'assurer une mission de conseil du secteur privé, notamment dans les secteurs d'activité d'importance vitale, et de participer activement à la diffusion de la sécurité dans la société de l'information. Le développement de sites Internet dédiés à cette mission et accessibles à tous fera partie de ses missions.

Plus généralement, l'État améliorera son expertise, en renforçant les moyens humains spécialisés des ministères et en créant, au sein de l'agence, un réservoir de compétences au profit des administrations et des opérateurs d'infrastructures vitales.

Compte tenu de la dimension internationale des menaces qui pèsent sur les réseaux de communication, l'agence assurera une liaison étroite avec nos principaux partenaires, notamment européens, et elle encouragera le développement d'une politique de sécurité des réseaux de communication à l'échelle européenne. »

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Décret nº 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »

NOR : *PRMD0914748D*

Le Premier ministre,

Vu le code de la défense, notamment ses articles R. 1332-2, R. 2311-1 et suivants, D.* 1132-10 et D. 2321-7 ;

Vu le code des postes et des communications électroniques, notamment son article L. 32-1 ;

Vu l'ordonnance nº 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment ses articles 9 et 10 ;

Vu le décret nº 87-389 du 15 juin 1987 modifié relatif à l'organisation des services d'administration centrale ;

Vu le décret nº 92-604 du 1er juillet 1992 modifié portant charte de la déconcentration ;

Vu le décret nº 97-464 du 9 mai 1997 modifié relatif à la création et à l'organisation des services à compétence nationale ;

Vu le décret nº 2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;

Vu le décret nº 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;

Vu le décret nº 2006-672 du 8 juin 2006 modifié relatif à la création, à la composition et au fonctionnement de commissions administratives à caractère consultatif ;

Vu le décret nº 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie ;

Vu l'avis du comité technique paritaire spécial du secrétariat général de la défense nationale du 26 mai 2009 ;

Vu l'avis du comité technique paritaire des services du Premier ministre du 25 juin 2009,

Décrète :

Art. 1er. – Il est créé un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». Ce service est rattaché au secrétaire général de la défense nationale.

Art. 2. – L'Agence nationale de la sécurité des systèmes d'information assiste le secrétaire général de la défense nationale dans l'exercice de ses attributions dans le domaine de la sécurité des systèmes d'information, notamment celles prévues par l'article D.* 1132-10 du code de la défense.

Art. 3. – L'Agence nationale de la sécurité des systèmes d'information est l'autorité nationale en matière de sécurité des systèmes d'information.

A ce titre :

– elle conçoit, fait réaliser et met en œuvre les moyens interministériels sécurisés de communications électroniques nécessaires au Président de la République et au Gouvernement ;
– elle anime et coordonne les travaux interministériels en matière de sécurité des systèmes d'information ;
– elle élabore les mesures de protection des systèmes d'information proposées au Premier ministre. Elle veille à l'application des mesures adoptées ;
– elle mène des inspections des systèmes d'information des services de l'Etat ;
– elle met en œuvre un système de détection des évènements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat et coordonne la réaction à ces évènements. Elle recueille les informations techniques relatives aux incidents affectant les systèmes d'information de l'Etat ;

– elle délivre des agréments aux dispositifs et aux mécanismes de sécurité destinés à protéger, dans les systèmes d'information, les informations couvertes par le secret de la défense nationale ;
– elle participe aux négociations internationales et assure la liaison avec ses homologues étrangers ;
– elle assure la formation des personnels qualifiés dans le domaine de la sécurité des systèmes d'information.

Art. 4. – L'Agence nationale de la sécurité des systèmes d'information se prononce sur la sécurité des dispositifs et des services, offerts par les prestataires, nécessaires à la protection des systèmes d'information.

L'agence est en particulier chargée, par délégation du Premier ministre :

– de la certification de sécurité des dispositifs de création et de vérification de signature électronique prévue par le décret du 30 mars 2001 susvisé ;
– de l'agrément des centres d'évaluation et de la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information prévus par le décret du 18 avril 2002 susvisé ;
– de la délivrance des autorisations et de la gestion des déclarations relatives aux moyens et aux prestations de cryptologie prévues par le décret du 2 mai 2007 susvisé.

L'agence instruit les demandes d'autorisation présentées en application de l'article 226-3 du code pénal.

Art. 5. – L'Agence nationale de la sécurité des systèmes d'information apporte son concours aux services de l'Etat en matière de sécurité des systèmes d'information.

Elle apporte son soutien :

– au ministre chargé des communications électroniques dans le domaine de l'intégrité et de la sécurité des réseaux de communications électroniques ouverts au public ;
– aux ministres coordonnateurs des secteurs d'activité d'importance vitale pour la protection de la sécurité des systèmes d'information des installations d'importance vitale.

Art. 6. – L'Agence nationale de la sécurité des systèmes d'information favorise la prise en compte de la sécurité dans le développement des technologies de l'information et de la communication.

Elle participe à l'orientation de la recherche, des études et du développement des dispositifs et des technologies de la sécurité des systèmes d'information.

Elle contribue à la promotion des technologies et des savoir-faire nationaux en matière de sécurité des systèmes d'information.

Art. 7. – Il est institué auprès du secrétaire général de la défense nationale un comité stratégique de la sécurité des systèmes d'information. Ce comité propose les orientations stratégiques en matière de sécurité des systèmes d'information et en suit la mise en œuvre.

Outre le secrétaire général de la défense nationale qui en assure la présidence, le comité comprend :

– le chef d'état-major des armées ;
– le secrétaire général du ministère de l'intérieur, de l'outre-mer et des collectivités territoriales ;
– le secrétaire général du ministère des affaires étrangères et européennes ;
– le délégué général pour l'armement ;
– le directeur général de la sécurité extérieure ;
– le directeur général des systèmes d'information et de communication ;
– le directeur général de la modernisation de l'Etat ;
– le directeur central du renseignement intérieur ;
– le vice-président du Conseil général de l'industrie, de l'énergie et des technologies ;
– le directeur général de l'Agence nationale de la sécurité des systèmes d'information.

Le secrétaire général de la défense nationale peut convier des personnalités qualifiées.

L'Agence nationale de la sécurité des systèmes d'information assure le secrétariat du comité.

Art. 8. – L'Agence nationale de la sécurité des systèmes d'information dispose, sur les crédits gérés par le secrétariat général de la défense nationale, des moyens nécessaires à l'accomplissement de ses missions.

Art. 9. – Dans toutes les dispositions à caractère réglementaire, la référence à la direction centrale de la sécurité des systèmes d'information est remplacée par la référence à l'Agence nationale de la sécurité des systèmes d'information.

Art. 10. – Le décret n° 2001-693 du 31 juillet 2001 créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information et l'article D. 1132-9 du code de la défense sont abrogés.

Art. 11. – Le ministre du budget, des comptes publics, de la fonction publique et de la réforme de l'Etat est chargé de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 7 juillet 2009.

FRANÇOIS FILLON

Par le Premier ministre :

Le ministre du budget, des comptes publics, de la fonction publique et de la réforme de l'Etat,
ERIC WOERTH