

# PLAN DE RENFORCEMENT DE LA SECURITE DES SYSTEMES D'INFORMATION DE L'ÉTAT (2004-2007)

10 mars 2004

## SOMMAIRE

1. INTRODUCTION .....	2
2. QUATRE OBJECTIFS .....	4
2.1 Sécuriser les moyens de transmissions des Hautes Autorités .....	4
2.2 Sécuriser les systèmes d'information des administrations.....	4
2.3 Mettre en place les capacités opérationnelles de réponse aux attaques informatiques prévues dans les plans .....	4
2.4 Inscrire notre politique de sécurité des systèmes d'information dans le cadre de notre politique de sécurité au sein de l'Union européenne.....	4
3. DOUZE MESURES .....	5
3.1 Formation et compétences .....	5
3.2 Organisation.....	7
3.3 Equipements.....	10
3.4 Tissu industriel.....	12
3.5 Cadre juridique.....	14
4. MISE EN OEUVRE .....	14
ANNEXE 1 : LETTRE D'INSTRUCTIONS .....	17

## 1. Introduction

Depuis plusieurs années, les rapports annuels des départements ministériels sur l'état de la sécurité des systèmes d'information (SSI) font part des difficultés persistantes rencontrées pour améliorer la situation : compétences et capacités opérationnelles trop réduites et isolées, manque de sensibilité des décideurs aux enjeux, insuffisance de produits de sécurité dûment qualifiés combinée à des positions monopolistiques dans des segments importants du marché, prolifération d'interconnexions de réseaux mal sécurisées<sup>1</sup>, réglementation nationale difficilement applicable, dimension européenne mal coordonnée. Si certaines améliorations ponctuelles sont constatées, les efforts accomplis, pour méritoires qu'ils soient, n'ont pas été à la mesure de l'évolution rapide des technologies et des menaces.

Les événements du 11 septembre 2001 ont conduit à revoir l'ensemble des plans de vigilance et d'intervention face aux risques de terrorisme, à introduire une composante de sécurité des systèmes d'information jusque là absente et à prendre conscience de la nécessité d'acquérir rapidement la maîtrise de l'ensemble des circuits opérationnels concernés.

Le plan gouvernemental « RE/SO 2007 » prévoit de franchir une nouvelle étape en matière d'administration électronique. La réussite du plan stratégique élaboré dans ce but par l'ADAE<sup>2</sup> reposera largement sur la capacité à maîtriser les techniques et procédures d'authentification des interlocuteurs, à garantir l'intégrité des données échangées et le respect de leur confidentialité.

Une comparaison avec nos principaux partenaires occidentaux montre la diversité des organisations, des réglementations et des pratiques en sécurité des systèmes d'information. Une harmonisation à l'échelle européenne paraît à terme nécessaire.

Par lettre du 4 avril 2003 (cf. annexe 1), le Directeur du cabinet du Premier ministre a donné instruction aux départements ministériels et au Secrétariat général de la défense nationale de préparer d'ici pour octobre 2003 un plan d'action propre à « sécuriser les principaux réseaux gouvernementaux, aux échelons centraux et locaux, ainsi que ceux utilisés pour la gestion des infrastructures vitales ».

Ce plan d'action, dénommé « plan de renforcement de la sécurité des systèmes d'information de l'Etat » a été adressé au Cabinet du Premier ministre le 17 octobre 2003. Il a été débattu et approuvé au cours d'une réunion interministérielle le 16 décembre suivant et intégré dans le programme pour l'administration électronique (programme ADELE) lui-même approuvé lors d'une réunion interministérielle le 23 décembre.

Le plan de renforcement propose 4 objectifs (§1) et 12 mesures réparties en 5 domaines (§3)<sup>3</sup>. Le manque de moyens actuel dans nombre de ministères et la difficulté à répondre précisément à toutes les questions posées conduit à préconiser une action en deux temps.

---

<sup>1</sup> Une cartographie des déploiements et des interconnexions des réseaux sensibles reste à établir, dans le cadre de l'inventaire des infrastructures vitales lancé en 2002.

<sup>2</sup> Le Plan Stratégique pour l'Administration Electronique de l'ADAE vise notamment, d'ici 2007, une dématérialisation des télé-procédures (100%), des échanges entre usagers et administrations (66%) et entre administrations (100%).

<sup>3</sup> Dans le programme ADELE, les 12 mesures sont regroupées un peu différemment selon 4 domaines : la « mutualisation de services » y comprend les mesures O1 (sauf l'organisation conjointe pour le développement de produits), O2, O3 et J1 ; le « développement des compétences » comprend F1, F2, F3 ; la « mise à disposition de

Une première phase consistera à bâtir en trois ans un socle solide répondant à un premier niveau des objectifs visés (§4). Sur cette base, il sera possible d'évaluer plus précisément les ressources nécessaires à un deuxième phase à moyen terme conduisant à une sécurisation plus complète et durable des systèmes d'information de l'Etat.

Dans son discours du 9 février 2004, prononcé à Lyon à l'occasion du lancement du programme ADELE, le Premier ministre a officialisé le démarrage du Plan d'action pour l'administration électronique et du Plan de renforcement selon le financement prévu : 1,8 milliards d'euro, dont un dixième environ pour le plan de renforcement (voir § 4).

---

produits de sécurité » comprends l'organisation conjointe pour le développement de produit (extraite de O1), E2, I1, I2 et F4 ; l' « acquisition de produits » correspondant à E1.

## **2. Quatre objectifs**

### **2.1 Sécuriser les moyens de transmissions des Hautes Autorités**

Il est indispensable que les Hautes Autorités disposent en permanence de moyens de communication complètement sécurisés pour joindre leurs principaux interlocuteurs, nationaux ou étrangers, ainsi que certains réseaux interministériels réservés aux plus hauts responsables ministériels.

Cet objectif concerne tous les moyens de communication courants : liaisons téléphoniques (dans les bureaux ou en déplacement) et mobiles, télécopie et messagerie. Même s'il s'agit d'un marché faible en volume, il est très exigeant en terme de qualité.

L'objectif visé est de garantir en toutes circonstances la sécurité de l'ensemble des moyens de communication protégés à l'usage des Hautes Autorités, en s'appuyant sur une maîtrise d'ouvrage sous contrôle direct de la puissance publique.

### **2.2 Sécuriser les systèmes d'information des administrations**

Peu de ministères disposent aujourd'hui d'un document spécifique détaillant leur politique en matière de sécurité des systèmes d'information. Le plan de renforcement doit viser à :

- sécuriser les nouvelles fonctions de l'administration électronique, conformément au plan stratégique et au schéma directeur de l'ADAE.
- expliciter des politiques de sécurité et engager les plans d'action correspondants en termes d'organisation, de potentiel humain et de ressources matérielles et financières.

### **2.3 Mettre en place les capacités opérationnelles de réponse aux attaques informatiques prévues dans les plans**

La diversité des cibles possibles et la rapidité de propagation des attaques informatiques requièrent réactivité et efficacité.

L'objectif du plan de renforcement est ici que les mesures prévues par les plans Piranet et Vigipirate deviennent pleinement opérationnelles, avec

- d'ici la fin du premier trimestre 2004, la définition des déclinaisons ministérielles des plans Vigipirate SSI et Piranet ;
- d'ici fin 2004, la disponibilité des capacités opérationnelles correspondant à ces plans ministériels (disponibilité en toute circonstance de liaisons sécurisées, annuaire de correspondants, pleine maîtrise par tous les acteurs des mesures à appliquer, disponibilité d'équipes mobilisables sans délai et capables de mener 24h sur 24 un programme opérationnel dans la durée).

### **2.4 Inscrire notre politique de sécurité des systèmes d'information dans le cadre de notre politique de sécurité au sein de l'Union européenne.**

La stratégie française en matière de défense et de sécurité se place dans une perspective européenne. Sa déclinaison en matière de sécurité des systèmes d'information doit se situer aussi clairement dans cette perspective. A cet égard, la participation aux travaux du Conseil et de la Commission, tant sur les aspects réglementaires qu'institutionnels, reste une priorité tout comme l'implication de personnels français dans les structures européennes chargées de ces questions.

En ce qui concerne les aspects opérationnels, cette orientation doit se traduire par une mutualisation des outils, l'interconnexion des chaînes opérationnelles et la mise en place de mécanismes permettant une gestion des crises et des incidents plus efficace sur des sujets qui, par nature, ne se limitent pas aux cadres nationaux. Cette politique devrait permettre d'offrir aux acteurs économiques des perspectives plus vastes et de favoriser à l'échelle de l'Union une prise en compte plus large des questions de sécurité des systèmes d'information.

### **3. Douze mesures**

Pour atteindre les objectifs visés, les mesures à prendre se répartissent en cinq domaines :

- Formation et compétences
- Organisation
- Equipements
- Tissu industriel
- Cadre juridique

#### **3.1 Formation et compétences**

Faisant appel à des techniques très élaborées, la sécurité des systèmes d'information repose néanmoins sur la compétence des hommes et des femmes qui en sont les acteurs : au premier chef, les spécialistes et les experts en sécurité des systèmes d'information, mais aussi les utilisateurs, qui sont directement concernés, et les décideurs, dont le rôle est primordial pour faire accepter, voire imposer, les bonnes pratiques et les allocations de moyens.

Le développement des compétences en sécurité des systèmes d'information, au sein des administrations comme auprès de prestataires de confiance, est donc un facteur clé. Quatre mesures proposées ci-après visent à répondre à cette exigence.

<b>MESURE F1 : DEVELOPPER LES COMPETENCES EN SECURITE DES SYSTEMES D'INFORMATION AU SEIN DES ADMINISTRATIONS</b>
--

Le manque de spécialistes compétents en sécurité des systèmes d'information au sein des administrations est devenu particulièrement alarmant. L'acquisition de compétences nouvelles et la mise à niveau permanente de celles qui sont disponibles sont donc une impérieuse nécessité pour l'ensemble des administrations. Des besoins considérables de formation et de sensibilisation en résultent.

Quantitativement, les actions et moyens existants<sup>4</sup> ne sont pas à la mesure de ces besoins, malgré la qualité du travail accompli.

Il est donc proposé de mettre en place un plan interministériel de formation en sécurité des systèmes d'information. A caractère interdisciplinaire (scientifique, technique, juridique, économique), ce plan inclura des allocations d'étude afin de susciter des vocations très en amont, ainsi qu'un renforcement des formations continues en tirant le meilleur parti possible de l'enseignement en ligne. Un effort particulier sera fait en direction des étudiants se destinant à des carrières dans l'administration. Dans ce but, une convention sera passée entre le Centre de Formation en sécurité des systèmes d'information du SGDN, le ministère de l'Education nationale et le ministère du Travail (formation professionnelle).

---

<sup>4</sup> notamment le Centre de formation en SSI du SGDN/DCSSI, le site web ssi.gouv.fr, le site protégé de la DCSSI avec droit d'accès réservé aux administrations, etc.

Par ailleurs, dans un marché de l'emploi qui est et restera tendu dans ce domaine, il convient de tout mettre en œuvre pour conserver les compétences ainsi acquises. Il est donc proposé que ces compétences soient reconnues et valorisées au plan professionnel, grâce à un système de rémunération adapté et des déroulements de carrière fondés sur le mérite.

#### MESURE F2 : REALISER REGULIEREMENT DES EXERCICES CONFORMES AUX PLANS SUR LA SECURITE DES SYSTEMES D'INFORMATION

Les attaques visant les systèmes d'information se caractérisent par leur déclenchement inopiné, leur ubiquité et la rapidité avec laquelle leurs effets se propagent. Une attaque informatique d'origine terroriste pourrait avoir, de surcroît, des capacités de nuisance sans commune mesure avec celles, déjà considérables, des attaques quotidiennes à but ludique ou crapuleux. Il importe donc que tous les services concernés puissent réagir sans délai et sans hésitation face à une agression sur les systèmes d'information de l'Etat. Les plans relatifs à la sécurité des systèmes d'information doivent pouvoir être appliqués et mis en œuvre à l'état de réflexe.

Pour y parvenir, une politique et un programme d'exercices au niveau interministériel et au niveau des départements ministériels<sup>5</sup> est nécessaire. Une périodicité trimestrielle est envisagée pour l'ensemble de ces exercices.

Des exercices interministériels, à thème unique, à la fois simples et mobilisateurs pour les administrations, seront ciblés sur des objectifs précis et s'attacheront à tester, d'une part les chaînes de liaison, d'autre part la mise en application des mesures du plan d'intervention ainsi que la maîtrise par les différents acteurs des actions qui leur incombent. D'autres exercices interministériels, au niveau national ou international, en particulier au niveau européen, permettront d'activer l'ensemble des chaînes de commandement et de décision ; ils prendront en compte les aspects liés à la communication de crise et à la communication vers les populations et testeront la mise en œuvre des procédures liées à la coopération internationale.

Au niveau ministériel, seront évaluées la capacité des services opérationnels des unités à faire face aux attaques informatiques, ainsi que l'adéquation des moyens dont ils disposent. La DCSSI pourra être sollicitée en tant que de besoin afin d'assister les organisateurs de ces exercices ministériels.

#### MESURE F3 : SENSIBILISER LES HAUTS RESPONSABLES

L'expérience prouve que, pour bien des responsables de haut niveau, la sécurité des systèmes d'information est l'affaire de spécialistes. Cela tient au fait que cette discipline est d'apparence très technique et que, par ailleurs, la menace apparaît comme très diffuse et théorique.

Or, l'action des hauts responsables est déterminante pour favoriser, ne serait-ce que par le poids de l'exemple et l'effet d'entraînement, ou, si nécessaire, pour imposer la diffusion des bonnes pratiques contraignantes et souvent perçues comme injustifiées.

Pour convaincre ces hauts responsables (cabinets, directions centrales) et organismes en charge d'infrastructures vitales que les menaces sont bien réelles, et aussi qu'il est possible de s'en protéger, une sensibilisation périodique sera proposée, à raison, par exemple, de trois à quatre séminaires d'une demi-journée par an, pour traiter les principaux aspects de la sécurité des

---

<sup>5</sup> Les premiers exercices SSI, réalisés en mai et en septembre 2003, puis en février 2004, ont déjà montré les bénéfices à tirer de ce type de mesure.

systèmes d'information : menaces, parades possibles, moyens nécessaires, contexte international, calendrier d'action<sup>6</sup>.

#### MESURE F4 : QUALIFIER DES PRESTATAIRES PRIVES EN SECURITE DES SYSTEMES D'INFORMATION

L'externalisation peut contribuer à une meilleure maîtrise des dépenses publiques et sera donc favorisée pour les fonctions qui n'ont pas de caractère régalien, pour peu que puissent être garantis des niveaux adéquats de compétence et de sécurité.

Il est donc proposé, dans un premier temps, de procéder à un inventaire des processus de qualification des métiers de la sécurité des systèmes d'information. Cet inventaire sera mené en concertation entre le secteur public et le secteur privé, sous l'égide de l'AFNOR, voire du comité européen de normalisation. Il prendra en compte les projets en cours dans ce domaine.

Sur cette base, des procédures de qualification de prestataires seront ensuite définies<sup>7</sup>. Elles devront être opérationnelles pour les activités de conseil et d'audit à l'horizon 2006. Il faudra veiller par ailleurs à ce que cette qualification des prestataires puisse être requise pour la passation de marchés publics.

### **3.2 Organisation**

#### MESURE O1 : RENFORCER L'ORGANISATION DE LA SECURITE DES SYSTEMES D'INFORMATION AU SEIN DES MINISTERES ET DES INSTITUTIONS EUROPEENNES

La prise en compte des objectifs gouvernementaux en matière de SSI doit être effective à tous les niveaux de l'administration en termes d'objectifs, d'organisation et de ressources.

Il est proposé que chaque département ministériel rencontrant des difficultés dans la sécurisation de ses systèmes d'information analyse, au regard des objectifs gouvernementaux et de ses propres enjeux et objectifs de sécurité, la répartition optimale des différentes fonctions génériques dans ce domaine au sein de son organisation, et définisse et engage sans tarder un plan d'ajustement.

L'élaboration d'un schéma directeur prenant en compte la sécurité des systèmes d'information<sup>8</sup> permet de conduire avec succès une telle analyse<sup>9</sup> et de mettre au point un tel plan d'ajustement.

Aujourd'hui, la capacité de pilotage d'une telle démarche fait souvent défaut au sein des ministères. La première étape consistera alors à mettre en place une équipe minimale capable de prendre en charge ce pilotage en s'appuyant, en tant que de besoin, sur des assistances externes (DCSSI, prestataires privés).

---

<sup>6</sup> Un premier séminaire, centré sur les menaces en SSI, a été organisé par le SGDN en octobre 2001 à l'intention des membres des cabinets ministériels.

<sup>7</sup> en s'inspirant, par exemple, de l'agrément des Centres d'Evaluation en Sécurité des Technologies de l'Information (CESTI), tel que spécifié dans le décret 2002-535.

<sup>8</sup> La DCSSI met à disposition des départements ministériels qui le souhaitent, un soutien technique à l'élaboration de schémas directeurs, en particulier pour l'identification des fonctions à assurer.

<sup>9</sup> Dans certains départements ministériels, un schéma directeur SSI existe déjà, ou bien un schéma directeur plus général (schéma directeur informatique ou schéma directeur de sécurité) traite déjà les aspects SSI d'une façon qui s'avère, à l'usage, satisfaisante.

Par ailleurs, une meilleure inscription de la politique nationale en sécurité des systèmes d'information dans le cadre de notre politique de sécurité au sein de l'Union européenne nécessite une implication marquée d'experts français dans les structures mise en place au niveau européen.

On s'attachera donc particulièrement à ce que des experts français puissent être détachés au sein de l'Agence européenne chargée de la sécurité des réseaux et de l'information (AESRI), instituée à partir du 14 mars 2004 pour une période de 5 ans, par le règlement (CE) N°460/2004 du Parlement européen et du Conseil du 10 mars 2004.

#### MESURE O2 : ASSURER LES PERMANENCES OPERATIONNELLES EN CAS D'APPLICATION DES PLANS PIRANET ET/OU VIGIPIRATE

Le plan Vigipirate, aux niveaux rouge et écarlate, et le plan Piranet prévoient la mise en place de centres opérationnels fonctionnant 24 heures sur 24 et 7 jours sur 7, au SGDN et dans les ministères.

Il faut donc garantir la disponibilité en toutes circonstances de ressources humaines compétentes et suffisantes pour constituer ces équipes opérationnelles dans le centre de coordination du SGDN ainsi que dans les centres de crise ministériels.

A l'heure actuelle, le personnel existant ne suffit pas toujours à constituer, même aux heures ouvrables, les équipes opérationnelles complètes<sup>10</sup> prévues par les plans. Le personnel supplémentaire, mobilisé de façon exceptionnelle, devra provenir des ressources nouvelles mises en place pour la réalisation d'autres mesures du plan de renforcement, en veillant à l'adaptation des compétences aux spécificités opérationnelles.

#### MESURE O3 : MUTUALISER UN ENSEMBLE DE SERVICES EN SECURITE DES SYSTEMES D'INFORMATION

La mutualisation de services est une manière pragmatique de satisfaire les besoins communs des ministères tout en réduisant les dépenses publiques et en optimisant les ressources humaines. Les actions suivantes y contribueront :

##### Mettre en place une organisation conjointe de développement de produits de sécurité

Les besoins des administrations qui ne peuvent être satisfaits par les produits du marché doivent être pris en charge par une organisation capable de définir les besoins communs, de gérer les priorités, d'établir les spécifications, de mobiliser les budgets correspondants, de passer et de suivre les contrats et de mettre en œuvre des procédures d'acquisition au meilleur coût<sup>11</sup>.

Une telle organisation unifiée sera mise en place en s'appuyant sur la CISSI (expression des besoins communs, répartition des contributions budgétaires, plan de développements prioritaires) et sur le ministère de la défense (conduite des projets de développement et d'acquisition de produits de sécurité de haut niveau, conception des algorithmes de chiffrement et maîtrise étatique des moyens de conception des composants et des produits). Les spécifications techniques correspondant aux niveaux de sécurité recherchés seront établies par concertation entre les services compétents des ministères et du SGDN. Les travaux de qualification des équipements seront pris en charge par les équipes habilitées (cf. infra).

<sup>10</sup> surveillance de réseaux, gestion des incidents, réaction aux attaques...

<sup>11</sup> comme cela a été fait, par exemple, aux Pays-Bas.

La mise en place de cette organisation conjointe amènera à revoir ou compléter certains textes réglementaires<sup>12</sup>.

#### Coordonner les infrastructures de gestion de clés (IGC) ministérielles

La disponibilité de clés authentifiant les acteurs dans les ministères et inter-opérables entre les ministères est une étape essentielle du développement de l'administration électronique<sup>13</sup>.

Une infrastructure interministérielle de gestion de clés sera mise en place pour permettre le dialogue entre et avec les différents services ministériels.

Sous réserve d'une demande de plusieurs ministères, une infrastructure mutualisée de gestion de clés devra pouvoir être mise à leur disposition.

#### Organiser les retours d'expérience interministériels

La veille et l'alerte sont des fonctions capitales pour la résolution d'incidents, *a fortiori* pour le déclenchement au moment opportun des mesures des plans de vigilance et d'intervention. L'analyse des signaux perturbateurs sur les réseaux reste aujourd'hui empirique et dispersée.

Un gain opérationnel important résultera de la mise en place d'une mutualisation des connaissances et des remontées d'incidents, et d'une harmonisation des procédures, du vocabulaire et des modes de travail.

#### Harmoniser les gestions de passerelles ministérielles d'interconnexion

L'exploitation des passerelles d'interconnexion est particulièrement exigeante en termes de ressources humaines alors que les besoins augmentent avec le développement des réseaux.

Dans un premier temps, il faudra auditer les différentes passerelles des ministères<sup>14</sup> puis harmoniser leurs modes de fonctionnement et d'organisation.

Une étude d'opportunité et de faisabilité sera ensuite réalisée en vue d'une offre de télé-administration des passerelles ainsi harmonisées. Cette mutualisation pourra comprendre l'administration d'une passerelle commune d'accès à Internet, complétée le cas échéant d'une surveillance permanente du réseau Internet.

#### Mettre en place auprès des préfets de zone de défense une structure de formation et de conseil en sécurité des systèmes d'information

Ces structures zonales doivent rendre les actions de soutien plus facilement accessibles aux services déconcentrés et aussi améliorer la remontée des signaux précurseurs d'incidents, renforçant ainsi la capacité à déclencher les plans de vigilance et/ou d'intervention au moment opportun.

Ces structures, placées auprès des préfets de zone, auront une vocation interministérielle affirmée, étant entendu que les activités et pratiques de chaque service ministériel déconcentré resteront sous la responsabilité des services centraux correspondants.

---

<sup>12</sup> notamment la directive interministérielle 4201 et l'instruction interministérielle 77/CD du 13 avril 1995, qui confie au ministère de la défense une responsabilité de « maîtrise d'œuvre » pour le développement des équipements destinés à protéger les « systèmes d'information gouvernementaux » (i.e. « qui gèrent des informations classifiées de l'Etat (défense, diplomatie, sécurité de l'Etat) »).

<sup>13</sup> voir notamment le Plan Stratégique de l'Agence pour le Développement de l'Administration Electronique (ADAE).

<sup>14</sup> ces audits de passerelles ont commencé dans plusieurs ministères.

La mise en place de deux équipes locales (zone Est et zone Ouest) a permis d'acquérir de l'expérience et un modèle d'organisation (deux personnes minimum par structure).

L'action proposée consiste à étendre progressivement les zones couvertes au rythme d'une à deux structures par an.

### 3.3 Equipements

#### MESURE E1 : ACQUERIR UNE SERIE D'EQUIPEMENTS PRIORITAIRES

Le plan de renforcement SSI de l'Etat comporte un important effort d'acquisition d'infrastructures et de moyens techniques adaptés aux enjeux nouveaux de la sécurité de l'information. Cet effort se répartit en trois volets

#### La mise à niveau des moyens propres de l'Etat pour la sécurité de ses communications et la continuité de son action en cas de crise.

Il est indispensable en premier lieu de porter au niveau de sécurité souhaitable les moyens de communication protégés mis à la disposition des hautes autorités et de les y maintenir dans la durée, conformément aux objectifs suivants :

- protection de l'information contre toute menace d'atteinte à sa confidentialité ou à son intégrité ;
- disponibilité permanente des moyens ;
- accès facile et ergonomique ;
- interopérabilité entre les différents systèmes ;
- fonctionnement en mode fixe ou mobile ;
- capacité de projection dans des délais très courts (quelques heures).

Plusieurs projets seront lancés dans ce cadre.

La refonte de l'architecture de la planification (plans de vigilance et d'intervention, plans de secours, plans spécialisés) et de la doctrine des exercices appelle le renforcement des systèmes de communication gouvernementale de crise. Fiables et disponibles en toute circonstance, ces systèmes doivent pouvoir acheminer très rapidement les informations avec une assurance d'intégrité et de confidentialité cohérente avec les exigences particulières de la situation de crise.

Le réseau Rimbaud sera maintenu à un haut niveau de sécurité, notamment en ce qui concerne la téléphonie chiffrée. Une messagerie gouvernementale sécurisée devra lui être associée. Elle devra pouvoir être interconnectée avec les réseaux spécialisés des ministères. A cet effet, la passerelle d'interconnexion du Centre de Transmissions gouvernemental sera modernisée afin d'assurer une interconnexion des messageries sécurisées nationales (gouvernementales, et ministérielles : Intérieur, défense, Affaires étrangères), et un accès contrôlé à des systèmes de même niveau de l'UE et de l'OTAN, dans des conditions plus efficaces.

#### Sécuriser les nouveaux outils de l'administration électronique

L'administration électronique ne tiendra toutes ses promesses que si elle inspire confiance aux différents interlocuteurs, confiance fondée en particulier sur la capacité d'identification réciproque sans ambiguïté possible et d'authentification des messages électroniques qu'ils échangent. Il est donc proposé de considérer comme prioritaire l'attribution à chaque agent

public d'une carte professionnelle dotée d'une capacité de signature électronique et d'authentification « forte »<sup>15</sup>.

Il conviendra aussi de développer les outils permettant à une infrastructure interministérielle de gestion de clés de faire se reconnaître entre elles les signatures des différents services ministériels (outils de datation, de comparaison des politiques ministérielles de gestion de clés, de publication des clés valides et des clés révoquées, etc.). Ceci permettra de mettre en place une gestion des droits d'accès des différents acteurs aux différents types de données (gestion des privilèges).

Pour compléter les besoins de l'administration électronique, il est enfin proposé de développer des outils de signature électronique correspondants aux différents niveaux de confiance souhaités<sup>16</sup>. Un effort particulier sera aussi mené pour le développement d'outils et d'architecture propres à sécuriser les interconnexions des réseaux inter-administrations (sécurisation du réseau AdER, en particulier).

#### Acquérir ou développer des outils de conception, de sécurisation et de surveillance des réseaux

L'acquisition d'une gamme cohérente d'outils de supervision et d'audit de la sécurité des réseaux et des systèmes et leur intégration progressive dans les infrastructures nationales devra donner à l'Etat et à ses partenaires, intérieurs et extérieurs, une assurance suffisante de leur capacité de défense et de réponse face aux menaces nouvelles pesant sur l'intégrité, la disponibilité ou la confidentialité de ces infrastructures. Dans nombre de ministères, un effort particulier devra être fait pour compléter ou renouveler les parcs en moyens de filtrage et de chiffrement.

<b>MESURE E2 : ACCROITRE RAPIDEMENT LE NOMBRE DE PRODUITS QUALIFIES EN SECURITE</b>
---

La qualification d'un produit de sécurité (dans une échelle à trois niveaux : standard, renforcé et élevé) résulte de sa capacité à résister à des menaces plus ou moins fortes. Cette qualification est fondée sur l'adoption de spécifications techniques présumées représentatives de la résistance à un certain niveau de menaces, sur une évaluation reconnue de la conformité à ces spécifications, et sur le niveau de confiance qui aura pu être établi vis-à-vis des équipes de conception et de développement<sup>17</sup>.

Ces nouvelles règles doivent permettre d'accroître rapidement la gamme de produits qualifiés, pour peu que les spécifications techniques associées aux différents niveaux de menaces soient disponibles et puissent être intégrées dans la conception des produits par des prestataires de confiance.

La mesure proposée consiste à élaborer, pour les différents types de produits et niveaux de sécurité, des spécifications techniques s'appuyant sur l'expertise de produits existants et sur des travaux de R&D, en particulier ceux définis par la structure de coordination mise en place par le

---

<sup>15</sup> Le déploiement de cartes nationales d'identité électronique (CNIE) ayant la même capacité est aussi un projet de première importance, mais n'entre pas dans le cadre du plan de renforcement de la sécurité des systèmes d'information dans l'Etat.

<sup>16</sup> Tels que définis dans la Politique de Référencement Intersectorielle de Sécurité (PRIS).

<sup>17</sup> cf. les nouvelles orientations de la doctrine en SSI, approuvées par le Cabinet du Premier ministre à l'automne 2002 (n°1884/SGDN/DCSSI/DA/E/DR)

Comité interministériel pour la société de l'information (CISI du 10 juillet 2003<sup>18</sup>). Des coopérations européennes permettront d'élargir la portée des travaux<sup>19</sup>.

Une concertation avec le secteur industriel<sup>20</sup> précèdera la validation de ces spécifications techniques en vue d'une prise en compte dans les appels d'offre des marchés publics<sup>21</sup>.

Dans le cas des niveaux renforcé ou élevé, en particulier pour des équipements protégeant la confidentialité, la concertation sera limitée à certains industriels de confiance et les spécifications seront protégées, voire classifiées.

Un élément important du dispositif sera l'établissement d'une politique cryptographique interministérielle précisant quel type d'algorithme cryptographique peut être utilisé pour quelle catégorie d'utilisateurs. Corrélativement, une action sera menée pour disposer des bibliothèques cryptographiques de référence et les mettre à la disposition des industriels.

### 3.4 Tissu industriel

#### MESURE II : GARANTIR UNE DIVERSITE D'APPROVISIONNEMENT EN PRODUITS DE SECURITE

Face à un marché des technologies de l'information caractérisé par des positions dominantes aux plans logiciel et matériel, une série d'actions vise à maintenir une diversité d'approvisionnements en produits de sécurité.

Stimuler le développement de produits industriels innovants et répondant à des besoins identifiés, en favorisant la prise en compte de spécifications techniques correspondant au niveau de sécurité standard, soit dans la conception de produits nouveaux, soit dans l'adaptation de produits existants. Cette démarche comporte le soutien aux étapes préalables à l'industrialisation de produits (prototypes, pré-séries, travaux d'évaluation).

Cette action s'adressera à un tissu d'industriels de confiance, qu'elle contribuera à entretenir et élargir, en particulier parmi les PME.

Pour accorder des « subventions d'investissement accordées par l'État » et/ou des « avances remboursables », il est proposé d'identifier un fonds interministériel, géré par le SGDN selon les orientations fixées par la CISSI.

Promouvoir le développement<sup>22</sup> et l'utilisation de produits sous licence libre au sein des administrations

Les produits sous licence libre offrent une alternative intéressante aux positions dominantes acquises par certains produits dont des industriels possèdent tous les droits.

<sup>18</sup> CISI 4 (créer un climat de confiance/agir sur l'offre) : une structure placée sous l'égide du ministère de la Recherche et de l'Industrie définira les thèmes prioritaires dans le domaine de la R&D en sécurité des systèmes d'information.

<sup>19</sup> une première coopération de ce type est envisagée entre l'Allemagne (BSI), les Pays-Bas (NLNCSA) et la France (DGA, DCSSI), sur le projet SINA de sécurisation du poste de travail.

<sup>20</sup> un séminaire public s'est tenu à l'Ecole militaire en février 2002 sur les IGC. Un atelier ouvert aux industriels a été organisé par le SGDN le 16 septembre 2003 sur les interconnexions.

<sup>21</sup> par exemple sous forme de normes homologuées au sens de l'AFNOR (décret 84-74 du 2 janvier 1984).

<sup>22</sup> avec des contributions d'équipes et agents publics, sous réserve d'une clarification des conditions juridiques.

Eviter la consolidation de positions commerciales dominantes, a fortiori l'émergence de mécanismes d'exclusion.

Les relations avec les industriels bénéficiant de situations notablement dominantes se limiteront à des contacts techniques pour améliorer la connaissance de leurs produits et des risques associés, et mettre à la disposition des administrations des guides de bonnes pratiques, tout en mettant en garde ces industriels contre toute démarche hégémonique.

## MESURE I2 : ADAPTER LES CAPACITES D'EVALUATION ET DE CERTIFICATION AUX BESOINS

L'évaluation/certification, actuellement encadrée par le décret 2002-535, est une composante essentielle de la qualification des produits

Longtemps léthargique, le marché de l'évaluation/certification connaît depuis quelques années une forte croissance qui demande une adaptation des structures et des capacités. Il s'agit de créer les conditions qui pourraient permettre, à l'horizon 2007, de rendre obligatoire pour l'administration l'acquisition de produits de sécurité évalués et certifiés.

Adapter les normes d'évaluation et développer les compétences des Centres d'Evaluation de la Sécurité des Technologies de l'Information (CESTI)

L'emploi de nouvelles normes d'évaluation, notamment Outre-Atlantique<sup>23</sup>, conduit de plus en plus les fournisseurs français à faire évaluer leurs produits à l'étranger. Pour que les équipes nationales restent des acteurs reconnus en matière d'évaluation et de certification, il faut que ces normes soient maîtrisées aussi bien par les équipes d'évaluation (prestataires privés reconnus comme CESTI<sup>24</sup>) que par les instances de certification (Centre de certification implanté au SGDN).

Dans toute la mesure du possible, la qualification des CESTI sera aussi étendue à l'habilitation des équipes et des personnes afin qu'ils puissent participer à l'évaluation de produits visant à protéger des informations classifiées.

Réviser l'organisation de l'activité de certification

La certification est actuellement assurée par une instance publique unique implantée au SGDN (Centre de certification). Pour répondre à la demande croissante en matière de certificats, sans pour autant accroître les charges de la puissance publique, il convient de démultiplier les capacités de certification au sein de structures combinant souplesse de gestion et contrôle d'une activité sensible.

Ceci pourra être obtenu en déléguant, par exemple, une responsabilité de certification à une autre instance administrative ou à un organisme sous tutelle, dans des domaines technologiques qui sont déjà de leur compétence.

Mieux utiliser les capacités de mesure des signaux compromettants

Longtemps réservée à la protection des informations classifiées, cette activité nécessite des investissements lourds. Entièrement prise en charge par la puissance publique (DGA/CELAR,

---

<sup>23</sup> tel que le FIPS 140-2 ou Federal Information Processing Standard : Security requirement ro cryptographic modules.

<sup>24</sup> Centres d'Evaluation de Sécurité en Technologie de l'Information, qui sont des instances privées agréées par le Centre de Certification.

SGDN/DCSSI), elle pâtit aujourd'hui d'un retard dans la rationalisation des moyens mis en place, alors que le développement des liaisons sans fil accroît les besoins de mesure des signaux.

L'action consistera, grâce à une meilleure gestion des moyens humains, à rechercher des gains de productivité en optimisant l'utilisation des moyens de mesure existants (CELAR, DCSSI et certains départements ministériels). Elle consiste aussi à examiner les possibilités de partage, voire de mutualisation, de cette activité avec certains partenaires nationaux ou européens.

### **3.5 Cadre juridique**

Un ensemble de textes (lois, codes, instructions interministérielles, directives, guides) constitue le cadre juridique de la sécurité des systèmes d'information. Les nouvelles orientations de la doctrine de l'automne 2002<sup>25</sup> et la mise en œuvre des mesures ci-dessus nécessitent aujourd'hui de reprendre certains de ces textes pour les compléter (cadre de l'homologation de systèmes, procédures d'agrément de produits), ou pour les amender (organisation unifiée de développement de produits de sécurité, qualification de produits).

#### **MESURE J1 : ADAPTER LES TEXTES REGLEMENTAIRES AU NOUVEAU CONTEXTE**

La mesure proposée conduira à expliciter la politique interministérielle de sécurité des systèmes d'information et à lui donner une assise réglementaire cohérente et solide, de façon à ce que chaque département ministériel puisse en déduire une politique de sécurité propre à son cadre spécifique.

Ce travail sera mené sous l'égide de la CISSI, par exemple sous forme d'un groupe de travail spécifique s'appuyant, le cas échéant, sur des études confiées à des prestataires extérieurs.

## **4. MISE EN OEUVRE**

Au regard de la situation actuelle, l'ambition des objectifs retenus pour le renforcement de la sécurité des systèmes d'information de l'Etat rend très difficile un chiffrage précis des ressources nécessaires : seule une approche analytique menée au sein de chacun des départements ministériels, notamment sous forme d'un schéma directeur, peut fournir de tels éléments. Mais dans de nombreux cas, l'insuffisance de personnels qualifiés, les retards dans l'inventaire des systèmes et applications sensibles et la faiblesse de l'organisation ne permettent pas de le faire.

Il est donc proposé de procéder en deux temps :

- d'abord, engager les mesures proposées en mobilisant un volume de ressources correspondant à un premier noyau d'objectifs. Ce « noyau dur » du plan de renforcement doit permettre, en trois ans, d'obtenir des résultats significatifs et de déterminer dans tous les départements les besoins nécessaires à une réalisation complète du plan ;
- ultérieurement, sur la base de l'expérience acquise et des nouvelles estimations, allouer les ressources complémentaires permettant d'accroître systématiquement le niveau de sécurité des systèmes d'information de l'Etat, conformément aux objectifs prévus.

Pour chacun des cinq domaines de mesures, il est possible de préciser les ressources à mobiliser sur la période de 2004 à 2006 et les résultats attendus.

---

<sup>25</sup> n° 1884/SGDN/DCSSI/DA/E/DR du 3 octobre 2002.

En matière de développement des compétences et pour la DCSSI, les objectifs de maîtrise des procédures d'application des plans de vigilance et d'intervention, de définition et de gestion des procédures de qualification de prestataires pour les métiers de conseil et d'audit, associés à une stimulation des vocations en sécurité des systèmes d'information et à un effort de formation devraient représenter un effort de 5 M€ et 5 postes.

Au plan de l'organisation, le noyau dur représente une soixantaine de postes (équivalents temps plein) au sein des ministères, une douzaine de postes au niveau interministériel et un coût d'une dizaine de M€ sur la période. Cet effort doit permettre d'élaborer des schémas directeurs partout où c'est nécessaire, d'assurer un premier niveau de renforcement des capacités de support et de contrôle au sein des ministères, d'affirmer la présence d'experts français au sein des instances de l'Union européenne consacrées à la sécurité des systèmes d'information, et de mettre en place une série de services mutualisés (développement de produits, notamment).

En cas de déclenchement des plans Vigipirate rouge/écarlate ou Piranet, ces ressources humaines permettront de mobiliser dans les services centraux le minimum de capacité opérationnelle requis dans la durée.

L'acquisition d'équipements de sécurité constitue le coût le plus important du plan proposé. Un montant de 151 M€ sur la période vise à couvrir les besoins de modernisation et sécurisation des moyens de communication essentiels de l'Etat.

<b>Produits de sécurité</b>	<b>Coût (M€)</b>
Communication des hautes autorités Passerelles sécurisées Moyens de chiffrements dédiés RIM	5
Liaisons de crise Pérennisation Rimbaud Messagerie sécurisée Passerelles	28
Equipements pour la défense Authentification par carte à puce Détection et suivi des incidents	55
Equipements pour le MISILL Chiffreurs de réseau Carte d'agent public	33
Equipements pour les autres ministères	30

Simultanément, une action forte devrait être engagée (8 M€, 10 postes interministériels) pour accroître le nombre de produits de sécurité.

Ce renouvellement et cette extension du parc de produits de sécurité doivent permettre de mieux sécuriser les transmissions des hautes autorités. Elles vont aussi créer une confiance accrue dans les nouvelles étapes de l'administration électronique, améliorer les conditions de déclenchement des plans de vigilance et d'intervention, et renforcer la position de la France dans le contexte européen.

La consolidation du tissu industriel appellera des dépenses de stimulation de l'innovation et de maîtrise de nouvelles normes d'évaluation (pour 12 M€) ainsi que 17 postes au niveau interministériel (mesures de signaux, travaux de certification, promotion des logiciels libres). Ceci doit permettre de mieux garantir la diversité des approvisionnements en produits de sécurité

et le contrôle de leur qualité, tout en maîtrisant au mieux la charge correspondante pour la puissance publique.

Enfin, l'adaptation des textes réglementaires au nouveau contexte aidera à la mise en œuvre de la plupart des mesures et va apporter une contribution générale aux objectifs poursuivis. Ne demandant pas de ressource nouvelle notable, cette mesure fait partie du noyau dur qu'il est proposé d'engager de 2004 à 2006.

\*\*\*

### **Synthèse des ressources nécessaires pour mettre en œuvre la première étape du plan de renforcement sur trois ans**

<b>Ressources</b>	<b>Formation/ compétences</b>	<b>Organisation</b>	<b>Equipements</b>	<b>Tissu industriel</b>	<b>Total</b>
<b>Postes<sup>26</sup> interministériels</b>	5	13	10	17	<b>45</b>
<b>Postes ministériels</b>	0	62	0	0	<b>62</b>
<b>Coût (M€)</b>	5	10	159	12	<b>186</b>

La synthèse des ressources correspondant au noyau dur du plan de renforcement fait apparaître un coût de l'ordre de 186 M€ sur trois ans avec une centaine d'équivalents temps plein (ETP) à répartir entre les différents départements ministériels (62 ETP) et les services interministériels (45 ETP).

Dans une certaine mesure, les ressources humaines ministérielles nouvelles pourront se traduire par de la sous-traitance ou provenir du redéploiement de compétences existantes. Certaines allocations budgétaires peuvent aussi provenir de redéploiements découlant d'une meilleure prise en compte de la sécurité dans les projets de développement.

Enfin, il est prévu que des outils de suivi des moyens alloués (existants et nouveaux) et de la progression vers les objectifs du plan de renforcement seront mis en place. En particulier des tableaux de bord, en cours d'élaboration, permettront à chaque ministère d'assurer à son niveau un suivi (indicateurs) des investissements (humains, matériels, financiers). Un référentiel sera proposé pour ces tableaux de bord ministériels afin qu'ils facilitent l'élaboration d'une synthèse (par exemple, pour le rapport annuel à l'intention du Premier ministre) et d'un bilan régulier de l'avancement du plan de renforcement.

---

<sup>26</sup> exprimés en « équivalents temps plein »

## Annexe 1 : Lettre d'instructions

PREMIER MINISTRE  
LE DIRECTEUR DU CABINET

Le 04 AVR. 2003

LE PREMIER MINISTRE

À

MESDAMES ET MESSIEURS LES MINISTRES ET SECRÉTAIRES D'ETAT  
A l'attention de Mesdames et Messieurs les Directeurs de Cabinet

MONSIEUR LE SECRÉTAIRE GÉNÉRAL DE LA DÉFENSE NATIONALE

Objet : Sécurité des systèmes d'information.

La sécurité des systèmes d'information de l'Etat est un enjeu de première importance pour les pouvoirs publics. Elle doit faire l'objet d'une attention particulière de la part des autorités ministérielles.

Le rapport que m'a transmis le Secrétaire général de la défense nationale, sur ce dossier, et dont vous avez été rendus destinataires pour la partie qui concerne votre département, dresse un constat préoccupant. Si certains progrès sont signalés, les vulnérabilités demeurent, voire s'accroissent. Certains départements ministériels n'ont en effet pas encore mis en place de chaîne de responsabilité opérationnelle en ce domaine ; les inventaires de réseaux à caractère sensible restent très incomplets ; peu de schémas directeurs existent, ni même sont en cours d'élaboration ; enfin, les personnels nécessaires à cette fonction font défaut au sein des administrations centrales.

Or, trois facteurs viennent donner une acuité supplémentaire à ce sujet :

- le passage à la deuxième phase de l'administration électronique, celle de la dématérialisation des procédures, ne sera possible que sur la base d'une confiance partagée, entre administrations et administrés ;
- une nouvelle étape de la construction européenne est engagée, caractérisée par l'ouverture généralisée sur la société de l'information, ainsi que par de nouvelles dimensions géographiques et politiques ; il est indispensable, que ces échanges soient, à terme rapproché, entièrement sécurisés ;

- enfin, les systèmes d'information, sur lesquels repose le bon fonctionnement de nos infrastructures vitales, apparaissent comme une cible particulière, au regard du terrorisme. A ce titre, le nouveau plan Vigipirate définit des actions de protection, qui visent à sécuriser rapidement, les systèmes d'information prioritaires et essentiels de l'Etat.

Le Premier ministre demande, donc, qu'un plan « sécurité des systèmes d'information de l'Etat » soit engagé dans les plus brefs délais pour sécuriser les principaux réseaux gouvernementaux, aux échelons centraux et locaux, ainsi que ceux utilisés pour la gestion des infrastructures vitales.

A court terme, il s'agira d'assurer les liaisons entre tous les responsables opérationnels, ainsi que de renforcer, si nécessaire, les chaînes fonctionnelles.

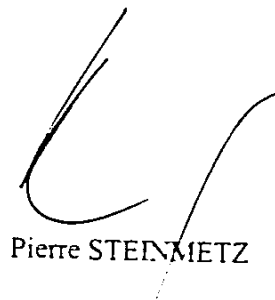
A moyen terme, il conviendra d'aboutir à une prise en compte généralisée des questions de sécurité, par les administrateurs et les utilisateurs des systèmes d'information. L'objectif final sera de disposer, au plus tard en 2006, d'une gamme étendue d'équipements de haute sécurité et d'une réglementation harmonisée dans un cadre européen.

Sur la base de l'analyse de la situation dans les administrations, dont vous avez la charge, je vous demande, par conséquent, de répertorier sans délai, les données, les applications informatiques et les réseaux à protéger. Vous élaborerez un plan sur trois ans, visant à assurer leur sécurité. Il portera sur le renforcement des chaînes fonctionnelles et des liaisons opérationnelles, l'établissement d'un schéma directeur et d'une politique de sécurité, le développement des compétences, l'identification des types d'équipement de sécurité à acquérir. Ce plan devra inclure, si nécessaire, les besoins des services déconcentrés et les échanges existants ou prévisibles à l'échelle européenne. Il fournira, enfin, une estimation des ressources humaines et budgétaires nécessaires à sa réalisation.

Par ailleurs, je donne instruction, au Secrétariat général de la défense nationale, de mener un travail équivalent, pour ce qui concerne les réseaux interministériels.

Enfin, une synthèse de ces plans ministériels et interministériels sera élaborée dans le cadre de la Commission interministérielle pour la sécurité des systèmes d'information, de façon à constituer un plan global. Je souhaite que ce plan me soit soumis d'ici le 1<sup>er</sup> Octobre.

Vous ne manquerez pas de me tenir informé de toute difficulté rencontrée, dans l'application de ces instructions.



Pierre STEINMETZ