PREMIER MINISTRE

Pôle Stratégie, Médias et Communication

Hôtel de Matignon, le 20 février 2014

**Discours de Monsieur Jean-Marc Ayrault, Premier ministre,
inauguration des nouvelles installations de
l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)**

jeudi 20 février 2014

Seul le prononcé fait foi

Madame la ministre, Monsieur le ministre,
Mesdames et Messieurs les parlementaires,
Monsieur le secrétaire général de la défense et de la sécurité nationale,
Monsieur le directeur général de l'agence nationale de la sécurité des systèmes d'information,
Messieurs les officiers généraux,
Mesdames et Messieurs,

Permettez-moi de vous souhaiter la bienvenue dans ces nouvelles installations. L'Agence nationale de la sécurité des systèmes d'informations est une structure encore jeune, en plein essor et qui trouve aujourd'hui un lieu à la hauteur de sa mission, qui prend chaque jour une importance nouvelle pour notre pays, celle d'assurer la sécurité des systèmes d'information des infrastructures vitales de notre pays.

Compte tenu des effets de la révolution numérique sur nos vies personnelles et professionnelles, cette mission est désormais essentielle à la sécurité de nos concitoyens et de nos entreprises et à la compétitivité du pays.

La sécurité des systèmes d'information est donc désormais un enjeu stratégique majeur, appelant une action résolue des pouvoirs publics.

D'abord contre la cybercriminalité, qui prend chaque jour des formes nouvelles : usurpations d'identité, escroqueries ou encore harcèlements. Cela suppose d'adapter les techniques d'enquête, le recueil et le traitement des plaintes, les sanctions, l'organisation des services et les capacités d'investigations. C'est l'objet du groupe de travail interministériel sur la cybercriminalité animé par le Procureur général Marc Robert qui remettra ses propositions dès la semaine prochaine.

S'y ajouteront, d'ici la fin du mois d'avril, les mesures du plan d'action demandé par le ministre de l'intérieur, Manuel Valls aux directeurs généraux de la gendarmerie et de la police nationales.

Les instruments de notre réponse pénale et répressive doivent être non seulement adaptés, mais renforcés. C'est une nécessité, mais ce n'est qu'un des volets de l'action à mener.

Car au-delà de la lutte contre la cybercriminalité, la France doit aussi se doter d'une capacité opérationnelle de réponse aux attaques contre les systèmes d'information eux-mêmes.
Les instruments existent déjà, mais ils doivent être renforcés et surtout généralisés, car nul n'est plus à l'abri, que ce soit les entreprises, les centres de recherche ou les administrations. Depuis 2010, c'est plus d'une centaine d'attaques de grande ampleur que l'ANSSI a été amenée à traiter. Bien des fois, les attaquants avaient pris le contrôle total du système d'information visé.

Ces attaques peuvent être destinées à s'emparer des informations du système visé. C'est inacceptable lorsqu'il s'agit d'informations personnelles dont la confidentialité doit impérativement être assurée. C'est inadmissible lorsque ces données constituant le cœur de la valeur ajoutée de l'entreprise attaquée, et que le défaut de sécurité informatique aboutit à anéantir les investissements consentis et les efforts demandés aux salariés. Les chefs d'entreprise qui m'écoutent le comprennent bien et savent qu'ils ont en la matière une responsabilité particulière.

Mais un défaut de sécurité peut avoir des conséquences plus redoutables encore, allant jusqu'à la paralysie ou la destruction de l'activité même des cibles visées. Le sabotage à l'été 2012 de 30 000 ordinateurs du premier exportateur mondial de pétrole, la société Aramco, en a donné un exemple saisissant, à une échelle encore inédite. Et c'est notre responsabilité d'en tirer toutes les conséquences pour assurer la sécurité de nos infrastructures vitales, qu'il s'agisse d'hôpitaux, de réseaux d'énergie, de transports, de banques, de communications, d'industrie, de services de sécurité et de secours ou d'administrations publiques. Au-delà de nos intérêts économiques, c'est la vie elle-même de nos concitoyens qui peut désormais être mise en danger du seul fait d'une attaque contre nos systèmes d'informations. Et cela constitue une menace d'un genre nouveau dont chacun doit prendre la mesure.

C'est ce qu'a fait le Gouvernement en décidant d'engager un effort sans précédent en faveur de la sécurité et de la défense de nos systèmes d'information.

Le Livre blanc sur la défense et la sécurité nationale présenté par le Président de la République en avril 2013, a placé le risque d'attaque contre les systèmes d'information au premier rang de nos priorités, juste derrière le risque de conflit armé et le terrorisme, et défini une stratégie de cybersécurité et de cyberdéfense.

J'ai souhaité que cette stratégie se traduise en actes sans délai.

Ainsi, le plan Vigipirate rénové, que j'ai présenté la semaine dernière, comporte désormais un volet de cybersécurité robuste.

Ainsi encore, la loi de programmation militaire, adoptée dès la fin de l'année 2013 enrichie des travaux parlementaires, que je salue, confère au Premier ministre et à ses services des capacités accrues, pour fixer les règles de sécurité nécessaires à la protection des systèmes d'information critiques des opérateurs d'importance vitale et pour en assurer le contrôle, y compris grâce à des notifications systématiques d'incidents informatiques et à la mise en place d'un pilotage direct en cas de crise majeure.

Cet enjeu est commun à tous les ministères et à tous les secteurs concernés : c'est pourquoi cette politique transversale est directement pilotée par le Premier ministre, qui dispose pour cela du Secrétariat général à la défense et à la sécurité nationale et de l'ANSSI, qui lui est rattachée. Ils travaillent dès à présent à la mise en œuvre de ces mesures, en étroite concertation bien sûr avec les quelque 200 organismes et entreprises publics et privés identifiés comme opérateurs d'importance vitale.

Les nouvelles installations que j'inaugure aujourd'hui illustrent l'effort national que nous avons engagé. À sa création en 2009, l'agence comptait une centaine d'ingénieurs. Devant le développement de la menace, j'ai décidé dès ma prise de fonctions de porter cet effectif à 350 agents, niveau atteint aujourd'hui. Cet effort sera poursuivi : l'ANSSI comptera 500 agents à l'horizon 2015, ce qui la rapprochera de l'effectif de ses homologues étrangers, notamment anglais et allemand, à missions comparables.

Ces missions, c'est, en amont, définir les règles de protection, assister les administrations et les opérateurs pour leur mise en œuvre, labelliser les produits et les prestataires de sécurité, développer les formations et diffuser les bonnes pratiques. Et en défense, l'ANSSI met en œuvre une capacité permanente de veille, d'alerte et d'analyse. Son centre opérationnel de la sécurité des systèmes d'information, véritable pompier de l'internet, conduit ou coordonne, tous les jours, les opérations de cyberdéfense pour parer les attaques et restaurer les systèmes. Compte tenu du caractère souvent transnational de la menace cyber, cette action se fait aussi en coopération avec ses homologues internationaux, européens notamment.

Je tiens à saluer le travail des femmes et des hommes de l'ANSSI, qui remplissent dans la discrétion une mission éminente, au cœur d'un réseau dont ils contribuent, de façon déterminante, à assurer la sécurité.

Cœur de réseau, l'ANSSI doit aussi veiller à la coordination et à la mutualisation des efforts de l'Etat. Pour relever un défi collectif de cette ampleur, la coordination est en effet essentielle.

Elle est illustrée ici même par la colocalisation et l'excellente coopération entre le centre opérationnel de sécurité de l'ANSSI et le centre d'analyse de lutte informatique défensive du ministère de la défense, que j'ai également visité il y a quelques minutes.

Le ministère de la défense y participe pleinement, et il développe actuellement des capacités permettant de se défendre et, le cas échéant, de riposter dans le cyberespace grâce à une chaîne opérationnelle dédiée, et à la création d'une réserve citoyenne « cyber ».

Les ressources allouées par la loi de programmation 2014-2019 permettront à la Défense d'investir, sur cette période, près d'un milliard d'euros en faveur de la cybersécurité et de la cyberdéfense. Le « Pacte Défense Cyber », présenté par Jean-Yves Le Drian il y a quinze jours, synthétise les actions engagées à ce titre. Dans leur volet opérationnel, comme en matière de formation ou de développements industriels, ces actions profiteront à toute la communauté nationale de cyberdéfense et apportent une contribution majeure à la stratégie nationale mise en œuvre par le Gouvernement et coordonnée par l'ANSSI.

Cette stratégie repose aussi sur le renforcement de notre souveraineté industrielle et technologique et sur le soutien à l'offre française en matière de produits et services de sécurité.

La France peut s'enorgueillir de disposer d'un tissu industriel complet qui va des composants électroniques au logiciel, avec des champions dans chacun de ces domaines. Il suffit de regarder les succès de la carte à puce à l'étranger pour s'en convaincre. Aux côtés de grands industriels reconnus, nous avons également la chance de disposer d'un formidable tissu de startups particulièrement dynamiques. Les métiers de la confiance numérique représentent en France près de 50 000 emplois.

C'est pourquoi j'ai installé en octobre dernier le comité de la filière industrielle de sécurité : pour que tous ces acteurs jouent davantage encore en équipe, et pour favoriser le dialogue public/privé, au service de la sécurité du citoyen et de la compétitivité de l'industrie française. Pour appuyer cette démarche, nous avons choisi, avec Arnaud Montebourg et Fleur Pellerin, de consacrer à la cybersécurité l'un des 34 plans de la Nouvelle France industrielle. Mais une action transversale sera aussi menée car il ne suffit pas de soutenir les entreprises de ce secteur, c'est l'ensemble des entreprises françaises qui doivent être sensibilisées à cet enjeu.
Le Gouvernement soutient également la recherche et le développement, notamment au moyen du programme d'investissements d'avenir. L'appel à projets spécifiquement consacré à la cybersécurité lancé dans ce cadre l'an dernier a suscité dix-huit candidatures. Les lauréats bénéficieront d'un soutien de l'État. Compte tenu de la qualité de ces projets et de la priorité accordée à la cybersécurité, un nouvel appel à projets sera donc lancé en 2014.

Enfin, la France doit aussi mieux intégrer la cybersécurité aux formations informatiques et mieux répondre au besoin de spécialistes fortement exprimé par les entreprises et les administrations. J'ai donc demandé à Geneviève Fioraso, en partenariat avec les acteurs concernés, de prendre rapidement les mesures nécessaires pour développer la formation de spécialistes en cybersécurité et garantir sa prise en compte dans les formations informatiques supérieures.

L'actualité de ces derniers mois a montré que la menace contre les systèmes d'information était omniprésente. J'ai donc décidé de prendre des mesures supplémentaires destinées à en renforcer la sécurité.

J'ai notamment décidé que le chiffrement des réseaux de l'État devait devenir systématique. J'ai également demandé aux administrations de l'État de recourir à des produits et à des services de sécurité informatique labellisés par l'ANSSI. Nous devons pouvoir nous appuyer sur une offre industrielle pour traiter nos informations sensibles dans des conditions alliant, mieux qu'aujourd'hui, efficacité et sécurité. La labellisation de cette offre est d'ailleurs un atout qui doit en faciliter le développement en France et nous permettre d'exporter, au-delà de nos frontières, notre excellence industrielle dans le domaine de la cybersécurité.

Mesdames, Messieurs, l'effort que nous développons en faveur de la sécurité des systèmes d'information est aussi une des clés de la protection des libertés publiques et de la vie privée.

C'est pourquoi j'ai souhaité aujourd'hui le lancement d'une initiative forte et simple : que les offres nationales de messagerie électronique soient chiffrées par leurs fournisseurs et que les messages soient traités par des infrastructures situées sur le territoire national. Cette initiative concernera dans un premier temps les services de messagerie électroniques proposés par les fournisseurs d'accès à Internet – ces opérateurs qui vous fournissent des « box ». Puis tous les fournisseurs de messagerie électronique seront invités à s'y joindre. Je pense particulièrement à la messagerie « laposte.net », qui concerne des millions de nos concitoyens. Notre objectif est de garantir l'inviolabilité des correspondances, vieux principe républicain qu'il faut réaffirmer dans le monde numérique.

Nous devons aussi porter cette stratégie au niveau européen. Seule l'Europe peut nous permettre de créer les conditions propices à l'émergence de champions de taille mondiale, pour renforcer la protection de la vie privée et assurer la sécurité de l'hébergement des données des entreprises et des citoyens européens. C'est la condition indispensable, je dis bien indispensable, pour que notre continent puisse garantir sa souveraineté. Cette position, le Président de la République l'a portée lors du Conseil européen d'octobre dernier consacré au numérique et à l'innovation. Il faut poursuivre sur cette voie et nous nous employons à convaincre nos partenaires européens de se mobiliser en ce sens. Nous avons discuté de ces sujets hier lors du conseil des ministres franco-allemand et je me réjouis de constater la très forte convergence de vue entre nos deux pays.

Ce sont là des enjeux vitaux pour la France, des enjeux non pas seulement techniques mais politiques au sens fort du terme.

Le grand défi est désormais d'y faire participer la société tout entière car dans cet espace de réseaux, la puissance publique ne peut assurer seule la sécurité des intérêts du pays. Ce sont des menaces d'un genre nouveau que nous affrontons, dans un espace de réseaux lui-même en perpétuelle évolution. L'Etat a défini une stratégie et mobilisé les moyens appropriés. A chacun d'entre nous, responsables politiques, élus, chefs d'entreprise, chercheurs, cadres d'administration, salariés, de prendre maintenant ses responsabilités dans la nécessaire mobilisation du pays.

Je vous remercie.