Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
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**

Madame la ministre, ma chère Fleur,
Monsieur le ministre, cher Kader,
Mesdames, Messieurs les présidents des commissions parlementaires de l'Assemblée nationale et du Sénat,
Mesdames, Messieurs les députés et sénateurs,
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, Messieurs,

Je suis très heureux d'être dans ces nouveaux locaux de l'Agence nationale de la sécurité des systèmes d'information. Vous le savez, c'est une structure jeune mais qui est en plein essor et c'était la moindre des choses de lui donner non seulement sur le plan matériel mais aussi sur le plan humain les moyens de son action. Cette action est nécessaire à notre sécurité et à la défense de nos intérêts, et elle prend chaque jour une importance nouvelle, parce que nos systèmes d'information sont des infrastructures vitales, ne cessent de croître, de se développer mais présentent aussi des risques. C'est cette révolution numérique que nous connaissons et qui va continuer à s'amplifier, qui impacte nos vies personnelles mais aussi professionnelles. C'est pourquoi le gouvernement a tenu à renforcer les moyens de la mission de sécurité pour protéger nos entreprises, protéger nos citoyens et leurs libertés et protéger aussi la compétitivité de notre pays.

C'est donc un enjeu stratégique que celui de la sécurité des systèmes d'information et c'est pourquoi il était important que les pouvoirs publics s'impliquent encore davantage.

D'abord contre la cybercriminalité. Cette cybercriminalité prend chaque jour des formes nouvelles : usurpation d'identité, escroquerie et même harcèlement. Cela suppose d'adapter les techniques d'enquête, le recueil et le traitement des plaintes, les sanctions aussi, l'organisation des services et les capacités d'investigation. C'est l'objet du groupe de travail interministériel sur la cybercriminalité qui est animé par le procureur général Marc ROBERT

et qui remettra ses propositions la semaine prochaine. À la fin du mois d'avril s'ajouteront les mesures du plan d'action qu'a demandé le ministre de l'Intérieur aux directeurs généraux de la gendarmerie et de la police nationales.

Quant aux instruments de notre réponse pénale et répressive, ils doivent être non seulement adaptés mais également renforcés. Tout cela est une nécessité mais, vous le voyez, ce n'est qu'un des volets de l'action à mener. Car au-delà de la lutte contre la cybercriminalité, la France doit se doter d'une capacité opérationnelle de réponse aux attaques contre les systèmes d'information eux-mêmes. Les instruments existent déjà mais il faut les renforcer et surtout les généraliser car nul n'est à l'abri, que ce soient les entreprises, les centres de recherche, les administrations, les personnes, les citoyens eux-mêmes. 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. C'est dire le risque, et ce risque ne se ralentit pas, il ne fait que s'amplifier.

Parce que les attaques ont des objectifs : s'emparer des informations du système visé, et s'agissant des informations personnelles, c'est inacceptable. La confidentialité doit être impérativement assurée. C'est inadmissible lorsque ces données constituent le cœur de la valeur ajoutée également de l'entreprise attaquée et que le défaut de sécurité aboutit à anéantir les investissements consentis et les efforts demandés aux salariés d'une entreprise. Les chefs d'entreprises qui sont là le savent très bien, et ils savent qu'ils ont en la matière une responsabilité particulière et accrue.

Mais un défaut de sécurité peut aussi avoir des conséquences plus redoutables encore, allant jusqu'à la paralysie ou même la destruction de l'activité des cibles visées. À l'été 2012, ce sont trente mille ordinateurs du premier exportateur mondial de pétrole, la société ARAMCO, qui 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 par exemple d'hôpitaux, de réseaux d'énergie, de transports, de banques, de communications, d'industries, de services de sécurité et de secours ou d'administrations publiques. Il y a donc des intérêts économiques à défendre, mais aussi la vie elle-même de notre concitoyen qui peut désormais être mise en danger du seul fait d'une attaque contre nos systèmes d'informations. Cela constitue une menace, une menace d'un nouveau genre dont chacun doit prendre totalement la mesure. C'est donc une question d'intérêt majeur et d'intérêt national qui concerne tous les citoyens, tous les Français, et c'est pourquoi il est important que le gouvernement s'engage totalement.

C'est la raison pour laquelle le gouvernement a décidé un effort sans précédent en faveur de la sécurité et de la défense de nos systèmes d'information. Le Livre blanc sur la Défense, auquel vous avez contribué, Mesdames et Messieurs les parlementaires, qui porte aussi sur les questions de sécurité nationale que le président de la République a arbitré et a présenté en avril 2013, a placé le risque d'attaque contre les systèmes d'information au premier rang de nos propriétés, juste derrière le conflit armé et le terrorisme, et défini une stratégie de cybersécurité et de cyberdéfense. J'ai donc souhaité que cette stratégie se traduise en actes le plus rapidement possible.

La semaine dernière, j'ai présenté le plan Vigipirate rénové avec le ministre de l'Intérieur et le ministre de la Défense. Désormais, il compte lui aussi un volet cybersécurité robuste. La loi de programmation militaire adoptée dès la fin de l'année dernière, enrichie par vos propositions que je tiens à saluer, Mesdames et Messieurs les parlementaires, 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. Il dispose pour cela du secrétariat général à la Défense et à la sécurité nationale et de l'ANSSI qui lui est rattachée. Il travaille dès à présent à la mise en œuvre de ces mesures, en étroite concertation bien sûr avec les quelque deux cents organismes et entreprises publics et privés identifiés comme opérateurs d'importance vitale. Aujourd'hui, ces nouvelles installations que j'inaugure avec vous 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 fonction de porter cet effectif à trois cent cinquante agents, niveau atteint aujourd'hui. Cet effort doit être poursuivi et il le sera. L'ANSSI comptera à l'horizon 2015 cinq cents agents, ce qui la rapprochera de l'effectif de ses homologues étrangers, notamment anglais et allemands, à missions comparables.

Ces missions, c'est d'abord 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, qui est un véritable pompier de l'internet comme vous l'avez rappelé Monsieur le directeur général, conduit ou coordonne tous les jours, je dirais heure par heure, les opérations de cyberdéfense pour parer les attaques et restaurer les systèmes. Et nous avons vus tout à l'heure, en visitant, une démonstration très éloquente. Compte tenu du caractère souvent transnational de la menace, cette action se fait aussi en coopération avec ses homologues internationaux, européens notamment. Vous nous avez montré une salle qui est secret-défense dans laquelle nous ne sommes pas entrés, où vous avez vos échanges et c'est extrêmement important.

Moi, je l'ai dit aux personnes que j'ai rencontrées, qui sont derrière leur écran, et qui est un travail exigeant, difficile, qui demande de la concentration et de la disponibilité, je leur ai dit directement mais je le dis à travers vous à tout le monde, à toutes les équipes : ces hommes et ces femmes 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. C'est donc une noble mission, difficile, mais que je tenais à saluer particulièrement parce qu'elle est conduite sous votre autorité, à la fois Monsieur le secrétaire général et Monsieur le directeur général, avec compétence et dévouement, au service des Français et des intérêts de la France.

Au cœur du réseau, l'ANSSI doit aussi veiller à la coordination et à la mutualisation des efforts de l'État. Pour relever un défi collectif de cette ampleur, la coordination est essentielle et elle est illustrée ici-même par la colocalisation et l'excellente coopération – Amiral, vous êtes là, j'espère ; vous nous avez accueillis tout à l'heure entre le centre opérationnel de sécurité de l'ANSSI et le centre d'analyse de lutte informatique défensive du ministère de la Défense, que nous venons de visiter il y a quelques minutes.

Le ministère de la Défense – je dois d'ailleurs excuser Jean-Yves Le Drian qui est en déplacement en Grèce, mais il est représenté aussi par le ministre délégué – le ministère de la Défense, dis-je, participe pleinement, et 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 ». Elle n'est pas encore très connue mais elle mérite d'être également saluée. Cet engagement citoyen, cette forme d'engagement citoyen, est extrêmement importante. Les ressources qui ont été allouées par la loi de programmation militaire 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 Cyber Défense, ou plutôt le Pacte Défense Cyber que Jean-Yves Le Drian a présenté il y a quinze jours, synthétise les actions qui sont 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 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. Oui, la France peut s'enorgueillir de disposer d'un tissu industriel complet qui va des composants électroniques aux logiciels, 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 des grands industriels reconnus, nous avons également la chance de disposer d'un formidable tissu de start-ups particulièrement dynamiques. Les métiers de la confiance numérique – de la confiance numérique ! - représentent en France près de cinquante mille emplois. Ce sont des emplois qui vont continuer à croître.

C'est pourquoi j'ai voulu installer personnellement en octobre dernier le comité de la filière industrielle de sécurité. L'objectif est de mobiliser tous ces acteurs pour qu'ils jouent davantage encore en équipe, pour favoriser le dialogue public-privé, au service de la sécurité du citoyen et mais aussi de la compétitivité de l'industrie française.

Pour appuyer cette démarche, vous savez que le gouvernement a décidé de lancer l'organisation de trente-quatre plans pour la Nouvelle France industrielle. Ces plans sont peu à peu mis au point et sont quasiment tous terminés. Nous aurons l'occasion de les présenter, j'espère, dans quelques jours. Fleur Pellerin y travaille avec Arnaud Montebourg et il y a donc, sur ce secteur de la cybersécurité, une organisation qui est maintenant en marche et qui fait partie de ces trente-quatre plans de la Nouvelle France industrielle. Le gouvernement soutient également la recherche et le développement, notamment au moyen du programme d'investissements d'avenir. L'appel à projets qui est consacré spécifiquement à la cybersécurité va être lancé dans ce cadre – enfin, a été lancé dans ce cadre l'année dernière, a suscité dix-huit candidatures et les lauréats vont recevoir un soutien substantiel de l'État pour mettre en œuvre leur projet de recherche développement. Et compte tenu de la qualité de ces projets, de la priorité accordée à la cybersécurité, nous allons lancer un nouvel appel à projets cette année.

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 demandé à Geneviève Fioraso, ministre de l'Enseignement supérieur et de la recherche, en partenariat avec les acteurs concernés, de prendre rapidement des mesures pour développer la formation de spécialistes en cybersécurité et garantir sa prise en compte dans les formations informatiques supérieures. Voilà encore des perspectives non seulement de formations mais aussi d'emplois. Vous connaissez l'actualité de ces derniers mois. Elle 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 devrait 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 aussi d'exporter, au-

delà de nos frontières, notre excellence industrielle dans le domaine de la cybersécurité, qui est particulièrement appréciée. Dans tous les contacts internationaux que nous avons, tant au niveau du président de la République que de moi-même ou des membres du gouvernement, à l'évidence beaucoup de pays sont sensibilisés à cette question et vont lancer des marchés substantiels, ne serait-ce que d'assurer la sécurité aux frontières, ce qui n'est pas une mince affaire et dans certains pays.

Mesdames, Messieurs, l'effort que nous développons en faveur de la sécurité des systèmes d'information est aussi une des clefs de la protection des libertés publiques et de la vie privée. Je sais, Mesdames, Messieurs les parlementaires, que vous y êtes particulièrement attentifs, et vous avez raison. 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 électronique proposés par les fournisseurs d'accès à Internet – ces opérateurs qui 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, qui est un vieux principe démocratique, un vieux principe républicain, mais qu'il faut réaffirmer et actualiser dans le monde numérique.

Et cette stratégie, il nous faut la porter aussi 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, 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 totale souveraineté. Cette position, le président de la République l'a portée lors du Conseil européen d'octobre dernier qui était consacré au numérique et à l'innovation. Il y a encore du chemin à faire dans cette voie, et nous nous employons d'ailleurs à convaincre nos partenaires européens pour se mobiliser en ce sens. Nous avons d'ailleurs abordé cette question hier avec la chancelière Angela Merkel à l'occasion du conseil des ministres franco-allemand et je me réjouis de constater la très forte sensibilité de nos partenaires allemands à cette question, qui a été renforcée par l'actualité ces derniers mois, mais surtout la très forte convergence de vue entre nos deux pays. C'est très rassurant pour la vision stratégique que l'on doit avoir sur cette question essentielle.

Voilà donc des enjeux vitaux pour la France, mais pas seulement en termes 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'État a défini une stratégie, a mobilisé les moyens appropriés. C'est à chacun d'entre nous, responsables politiques, élus, chefs d'entreprise, chercheurs, cadres d'administration, salariés, de prendre maintenant toutes ses responsabilités dans la nécessaire mobilisation du pays, parce qu'il s'agit bien d'une mobilisation d'abord d'une sensibilisation, d'une éducation, d'une responsabilisation et aujourd'hui, en inaugurant l'ANSSI, nous démontrons la volonté du gouvernement, appuyé par de nombreuses compétences, appuyé par le parlement, pour réussir à relever ce défi et la France est bien placée pour y parvenir.