Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE
DES AFFAIRES ÉTRANGÈRES
ET DU DÉVELOPPEMENT
INTERNATIONAL

Réponse de la France à la résolution 68/243 relative aux « Développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale »

RESUME ANALYTIQUE

A titre préliminaire, la France souhaite rappeler qu'elle n'emploie pas le terme de « sécurité de l'information » auquel elle préfère le terme de « sécurité des systèmes d'information » ou encore de « cybersécurité ». Active dans la promotion du principe de liberté d'expression en ligne (Résolution 20/8 du Conseil des droits de l'Homme de 2012), la France n'estime pas que l'information en tant que telle puisse être un facteur de vulnérabilité contre laquelle il est nécessaire se protéger, hormis dans les conditions strictement établies par la loi, de manière proportionnée et transparente, conformément à l'article 19 du Pacte relatif aux droits civils et politiques.

Le fonctionnement de notre société dépend de manière croissante des systèmes d'information et des réseaux, notamment d'Internet. Une attaque réussie contre un système d'information critique pourrait donc entraîner des conséquences humaines ou économiques graves. C'est pourquoi la France a défini en 2011 une *Stratégie pour la défense et la sécurité des systèmes d'information*, érigeant ainsi la cybersécurité en véritable priorité nationale. Le *Livre blanc sur la Défense et la Sécurité nationale* de 2013 est venu affiner notre perception de la menace en identifiant deux dangers majeurs pour la Nation : le cyberespionnage et le cybersabotage d'infrastructures d'importance vitale.

Créée en 2009 pour répondre à ces défis, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a depuis connu un constant renforcement de ses moyens et de ses prérogatives. Elle porte aujourd'hui, au nom du Premier ministre, l'ensemble des missions de prévention et de réaction relatives à la cybersécurité de nos infrastructures critiques, y compris gouvernementales. Responsable de la sécurité de ses propres réseaux, le ministère de la Défense est également monté en puissance dans ce domaine, comme l'illustre la parution d'un ambitieux document stratégique en février 2014, le « Pacte Défense Cyber ».

En parallèle, la France s'est engagée activement à renforcer la coopération internationale en matière de cybersécurité, sans laquelle les efforts nationaux sont limités. Depuis le G8 de Deauville en 2011, elle est particulièrement attachée à renforcer la régulation internationale du cyberespace. Dans ce but, elle participe aujourd'hui activement aux travaux du GGE de l'ONU et de l'OSCE visant à mettre en place un cadre normatif international reposant sur le droit international existant, ainsi que des mesures de confiance et des normes de comportement spécifiques au cyberespace. Enfin, la France s'applique à mettre en œuvre l'objectif de renforcement international des capacités en matière de cybersécurité, au travers de programmes concrets initiés dans un cadre bilatéral ou multilatéral (UE, OTAN).

RAPPORT

La France salue l'opportunité qui lui est offerte de répondre à la résolution 68/243 de l'Assemblée générale des Nations Unies intitulée « Développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale ».

1. **Appréciation générale des problématiques de cybersécurité**

A titre préliminaire, la France souhaite rappeler qu'elle n'emploie pas le terme de « sécurité de l'information » auquel elle préfère le terme de « sécurité des systèmes d'information » ou encore de « cybersécurité ». Active dans la promotion du principe de liberté d'expression en ligne (Résolution 20/8 du Conseil des droits de l'Homme de 2012), **la France n'estime pas que l'information en tant que telle puisse être un facteur de vulnérabilité** contre laquelle il est nécessaire se protéger, hormis de manière proportionnée, transparente et dans les conditions strictement établies par la loi conformément à l'article 19 du Pacte relatif aux droits civils et politiques.

A l'inverse, le *Livre blanc de la défense et de la sécurité nationale de 2013* livre une appréciation détaillée de la menace pesant sur les **systèmes** d'information critiques au bon fonctionnement de l'Etat, des opérateurs d'importance vitale et des grandes entreprises nationales. Ces menaces peuvent relever de l'**espionnage**, mais également du **sabotage**, à travers la destruction ou la prise de contrôle de système informatiques critiques :

« *Le développement rapide des infrastructures numériques ne s'est pas toujours accompagné d'un effort parallèle de protection, de sorte que* ***les agressions de nature cybernétique sont relativement faciles à mettre en œuvre et peu coûteuses****. Leur furtivité complique l'identification de leurs auteurs qui peuvent être aussi bien étatiques que non-étatiques. Les agressions les plus sophistiquées requièrent néanmoins une organisation complexe. Une attaque d'envergure contre une infrastructure numérique repose sur une connaissance détaillée de la cible visée, connaissance qui peut s'acquérir par des attaques préalables de moindre ampleur destinées à tester la cible, ou par des renseignements obtenus par d'autres moyens.*

Les menaces qui se développent dans le cyberespace sont de plusieurs ordres. Au plus bas niveau, elles sont une forme nouvelle de criminalité, qui ne relève pas spécifiquement de la sécurité nationale : vol d'informations personnelles à des fins de chantage ou de détournements de fonds, usurpation d'identité, trafic de produits prohibés, etc. Relèvent en revanche de la sécurité nationale les ***tentatives de pénétration de réseaux numériques à des fins d'espionnage,*** *qu'elles visent les systèmes d'information de l'État ou ceux des entreprises.* ***Une attaque visant la destruction ou la prise de contrôle à distance de systèmes informatisés*** *commandant le fonctionnement d'infrastructures d'importance vitale, de systèmes de gestion automatisés d'outils industriels potentiellement dangereux, voire de systèmes d'armes ou de capacités militaires stratégiques pourrait ainsi avoir de graves conséquences.*

Le cyberespace est donc désormais un champ de confrontation à part entière. ***La possibilité d'une attaque informatique majeure contre les systèmes d'information nationaux dans un scénario de guerre informatique*** *constitue, pour la France et ses partenaires européens, une menace de première importance.* »

2. Efforts entrepris pour renforcer la cybersécurité au niveau national et promouvoir la coopération internationale dans ce domaine.

a. Au niveau national

Les orientations stratégiques prises ces dernières années au plus haut niveau de l'Etat français **ont consacré la cybersécurité comme l'une des priorités de l'action gouvernementale**. Pour faire face au défi croissant que représentent les cyberattaques et maintenir un Internet ouvert, sécurisé et fiable, **l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée en 2009** afin de mener et de coordonner les efforts réalisés dans ce domaine au niveau national.

En février 2011, la première stratégie française de défense et de sécurité des systèmes d'information a été publiée. Elle fixe les objectifs suivants :

- être une puissance mondiale de cyberdéfense et appartenir au premier cercle des nations majeures dans ce domaine tout en conservant son autonomie ;
- garantir la liberté de décision de la France par la protection de l'information de souveraineté ;
- renforcer la cybersécurité des infrastructures vitales nationales ;
- assurer la sécurité dans le cyberespace.

Devenue en 2011 **autorité nationale** en matière de sécurité et de défense des systèmes d'information, l'ANSSI continue aujourd'hui de monter en puissance avec **380 employés, et 500 prévus à l'horizon 2015**. La dernière loi de programmation militaire (2014-2019) du 18 décembre 2013 est venue **renforcer les outils juridiques** dont elle dispose pour mener ses missions, notamment en matière de régulation des secteurs d'activités d'importance vitale.

En **février 2014**, le **ministère de la Défense** a publié un « **Pacte Défense Cyber** », qui implique à la fois des mesures visant à accroître la mobilisation de l'ensemble du ministère de la Défense en matière de cybersécurité, ainsi que des actions destinées à soutenir les initiatives innovantes émanant aussi bien du secteur public que privé : collectivités locales, grands groupes, PME/PMI, opérateurs de formation. **Six axes et cinquante mesures** constituent ce pacte :

- **Axe 1** : durcir le niveau de sécurité des systèmes d'information et les moyens de défense et d'intervention du ministère et de ses grands partenaires de confiance.
- **Axe 2** : préparer l'avenir en intensifiant l'effort de recherche tant technique et académique qu'opérationnel, tout en soutenant la base industrielle.
- **Axe 3** : renforcer les ressources humaines dédiées à la cyberdéfense et construire les parcours professionnels associés.
- **Axe 4** : développer le Pôle d'excellence en cyberdéfense en Bretagne au profit du ministère de la défense et de la communauté nationale de cyberdéfense.
- **Axe 5** : cultiver un réseau de partenaires étrangers, tant en Europe qu'au sein de l'Alliance Atlantique et dans les zones d'intérêt stratégique.
- **Axe 6** : favoriser l'émergence d'une communauté nationale de cyberdéfense en s'appuyant sur un cercle de partenaires et les réseaux de la réserve

Conformément aux orientations du Livre blanc sur la défense et la sécurité nationale, la Loi de programmation militaire 2014-2019 prévoit une **augmentation substantielle des moyens alloués à la cyberdéfense, et en particulier des effectifs**.

En outre, un **pôle d'excellence en cyberdéfense** chargé de répondre aux besoins du ministère de la défense et d'autres institutions se développe en Bretagne, où se situent de nombreux centres d'expertises militaires et civils et des écoles de formation.

b. Au niveau international

- *Au niveau technique*

Dans sa **Stratégie de défense et sécurité des systèmes d'information de 2011**, la France reconnaît que « *la sécurité des systèmes d'information repose en partie sur la qualité de l'échange d'informations entre les services compétents des divers États* ». C'est pourquoi l'Agence nationale de sécurité des systèmes d'information (ANSSI) cherche à établir « *un large tissu de partenaires étrangers afin de favoriser le partage des données essentielles, comme, par exemple, les informations concernant les vulnérabilités ou les failles des produits et services* ».

L'ANSSI entretient donc des contacts avec ses homologues de nombreux pays. Dès lors qu'un organisme national possède un mandat clair et semble fournir des services utiles et visibles, il est susceptible de devenir un partenaire pour l'ANSSI.

Par ailleurs, le CERT-FR, au sein de l'ANSSI, est actif au sein de plusieurs **réseaux multilatéraux** (FIRST, TF-CSIRT, EGC) grâce auxquels il créé des contacts avec des CERTs du monde entier.

- *Au niveau juridique*

La France a ratifié la **Convention de Budapest de 2001**, qui prévoit des **moyens flexibles et modernes de coopération internationale en matière de lutte contre la cybercriminalité** (ex : mise en place d'un **réseau 24/7** pour accélérer les procédures d'assistance entre Etats parties). La France plaide aujourd'hui pour une **universalisation de la Convention de Budapest**.

Au niveau européen, la France est actuellement en cours de transposition en droit national des dispositions de la **directive 2013/40/UE relative aux attaques contre les systèmes d'information**. Cette directive, qui vise à combattre la cybercriminalité, a été adoptée le 12 août 2013. Elle fixe des règles minimales concernant la définition des infractions pénales et des sanctions en matière de cyberattaques (en dehors de celles menées par les Etats). En outre, elle **améliore la coopération transfrontalière entre les autorités judiciaires et la police des différents Etats membres de l'Union européenne**. Les Etats membres devront veiller à disposer d'un point de contact national opérationnel. Ils devront également recourir au réseau existant de points de contact opérationnels.

Le **point de contact international** opérationnel français en matière de lutte contre la cybercriminalité est **l'Office centrale de lutte contre la criminalité lié aux technologies de l'information et de la communication** (OCLCTIC), qui dépend de la direction générale de la police judiciaire au sein de la direction générale de la police nationale (ministère de l'Intérieur).

- *Au niveau diplomatique*

Outre les **consultations bilatérales** menées régulièrement avec ses grands partenaires, la France s'est distinguée par un **engagement précoce et constant en faveur d'une meilleure régulation internationale du cyberespace** :

- Lors du G8 de Deauville en 2011, la France a ouvert la voie à une réflexion sur la mise en place de normes de comportement responsables pour les Etats dans le cyberespace ;

- La France a participé activement aux derniers groupes d'experts gouvernementaux (GGE) sur la cybersécurité et se félicite de la reconnaissance par le dernier groupe de l'applicabilité du droit international au cyberespace. Les travaux du nouveau GGE doivent désormais bâtir sur ce succès en réfléchissant à la définition de nouvelles mesures de confiance et de normes de comportements spécifiques au cyberespace.

- Par ailleurs, la France participe activement aux travaux du groupe de travail de l'OSCE sur la cybersécurité. Elle se félicite de l'adoption en décembre 2013 d'une liste initiale de 11 mesures de confiance visant à renforcer la transparence entre les Etats et figure parmi les premiers pays à avoir publié un document exhaustif de mise en œuvre de ces mesures.

3. Concepts internationaux pertinents visant à renforcer la cybersécurité globale

- **Applicabilité du droit international**

La France estime que la création d'un nouvel instrument spécifique au cyberespace est prématurée, sans pour autant préjuger de la pertinence de disposer d'un tel instrument sur le long terme. A ce stade, elle se félicite de la reconnaissance par le dernier GGE de l'applicabilité du droit international au cyberespace, et notamment des corpus juridiques suivants : Charte des Nations Unies, Déclaration universelle des droits de l'Homme, droit des conflits armés, droit de la responsabilité internationale des Etats.

- **Normes de comportement et mesures de confiance**

La France soutient le développement de mesures de confiance et de normes de comportement spécifiques au cyberespace, quoique basées sur le droit international existant. En renforçant la transparence, la coopération et la stabilité, ces instruments s'avèrent indispensables à la prévention les conflits dans le cyberespace. Ils doivent en particulier être fondés sur les principes de souveraineté territoriale et de responsabilité internationale des Etats dans le cyberespace.

- **Renforcement des capacités**

La France soutient l'objectif de renforcement international des capacités en matière de cybersécurité, qui constitue un moyen pour lutter contre les interdépendances critiques dans le cyberespace. La France contribue à la réalisation de cet objectif grâce à des projets menés de manière bilatérale ou dans un cadre européen, en Afrique ou dans les Balkans.

4. Mesures qui pourraient être prises par la communauté internationale pour renforcer la cybersécurité au niveau global

La France estime que les mesures suivantes pourraient être prises pour renforcer la cybersécurité au niveau international :

- poursuite par le GGE des travaux visant à mieux réguler le cyberespace et à proposer un cadre de coopération internationale propre à réduire le risque de cyberconflits ;

- universalisation de la Convention de Budapest pour renforcer la coopération internationale en matière de lutte contre la cybercriminalité ;

- renforcement de l'échange de bonnes pratiques et du renforcement des capacités visant à doter tous les Etats d'un dispositif performant de cybersécurité :

    - mise en place d'une stratégie de cybersécurité ;
    - définition cadre législatif pour la lutte contre la cybercriminalité ;
    - création d'un CERT ;
    - mise en place de procédures pour coopérer avec le secteur privé ;
    - définition d'un cadre de protection des infrastructures critiques dans le cyberespace.