Assises de la Sécurité, P. Pailloux (DCSSI) revient sur le Livre blanc 'Défense et sécurité nationale'

Silicon.fr:*Une nouvelle agence doit prendre le relais de la DCSSI dans les prochains mois. Quel est le contexte de cette évolution de structure? Quelle place occupe la cyber sécurité ?*

Patrick Pailloux: Le Président de la République a souhaité que la France se dote d'une nouvelle doctrine en matière de défense et de sécurité nationale. Il a confié cette mission à une commission réunissant des personnalités de tous horizons. Les travaux qu'elle a menés ont conduit à la publication, le 17 juin dernier, du , expression de la nouvelle doctrine française en la matière.

Ce Livre blanc retient le risque d'une attaque informatique contre les infrastructures nationales comme une des menaces majeures des 15 prochaines années. C'est dans ce contexte qu'il identifie un certain nombre de mesures à prendre afin de contrer ce risque. Parmi les mesures, il faut noter : la création d'une capacité de détection précoce des attaques informatiques, le recours accru à des produits et des réseaux de sécurité de haut niveau et la mise en place d'un réservoir de compétence au profit des administrations et des opérateurs d'infrastructure vitale.

Pour mener à bien cette stratégie, le gouvernement a décidé la création d'une agence nationale qui sera chargée de la sécurité des systèmes d'information. Cette agence reprendra, en les renforçant sensiblement, les moyens et les effectifs de la DCSSI.

Cette agence aura également pour objectif d'assurer une mission de conseil auprès du secteur privé et plus largement de la population française.

Silicon.fr: ***Dans le cadre de la présidence de l'Union Européenne, la France dispose-t-elle de propositions en la matière dans ses cartons ?***

Patrick Pailloux: Dans le domaine de la cyber sécurité, il est illusoire d'imaginer pouvoir travailler uniquement au niveau national. C'est la raison pour laquelle la stratégie nationale en la matière repose sur deux principes: le développement d'une part de coopérations étroites avec nos principaux partenaires notamment dans le domaine de la défense contre les attaques informatiques et, d'autre part, d'une politique de sécurité des réseaux de communication à l'échelle européenne.

Dans ce domaine la France compte, durant sa présidence, lancer un débat, dans le cadre des travaux qui vont être menés sur l'avenir de l'agence européenne de sécurité des réseaux de l'information (ENISA), sur les priorités et la stratégie européennes en matière de sécurité des systèmes d'information. Elle compte notamment insister sur la nécessité de développer un niveau minimum de règles de sécurité que devront appliquer les opérateurs de communication électroniques.

Silicon.fr : ***Certains acteurs de l'univers Internet se plaignent régulièrement des procédures***

juridiques françaises et plaident dans les journaux pour « un modèle ouvert » (cf. la tribune publiée dans Le Monde du 8 juillet par les dirigeants de Google France, Price Minister, Exalead… (« notre principal message aux pouvoirs publics serait, paradoxalement, d'en faire le moins possible »). Où doit commencer et s'arrêter une politique publique en matière de sûreté et de sécurité sur Internet? **Patrick Pailloux:** On ne peut pas éternellement opposer liberté et sécurité. Il ne vient à l'idée de personne de remettre en cause le bien-fondé du code de la route et du permis de conduire qui ont été créés lorsque l'utilisation de l'automobile s'est répandue. Personne de raisonnable aujourd'hui ne considère que ces règlementations bride les libertés individuelles. On peut assez simplement faire le parallèle avec les autoroutes de l'information chères à Gérard Théry. L'internet, comme le récent rapport du sénateur Romani sur la cyber défense l'a très justement souligné, est porteur d'un certain nombre de risques, qu'il est de la responsabilité des Etats et des organisations internationales de prendre en compte.

Les réseaux et notamment Internet, s'insèrent chaque jour de plus en plus dans nos sociétés et par la même nous en devenons de plus en plus dépendants. La résilience des réseaux va devenir une condition essentielle du maintien de nos modes de vie.

En parallèle se développent à grande vitesse de nouvelles formes de criminalité que les Etats, faute de manquer à leurs devoirs essentiels, ne peuvent pas laisser prospérer. Evidemment les nations ne doivent et ne peuvent pas agir seules. Les industriels, les opérateurs et tous les utilisateurs doivent, chacun à leur niveau, veiller à une utilisation rationnelle des technologiques de l'information et de la communication.