La France doit renforcer la défense de ses systèmes d'information

Publié le 29 avril, le Livre blanc sur la défense et la sécurité nationale, qui fixe les orientations stratégiques des quinze prochaines années et servira de socle à la future loi de programmation militaire (2014-2019), contient naturellement un volet sur les menaces numériques qui, comme le terrorisme, la prolifération nucléaire et les pandémies *« se sont amplifiées »* depuis 2008, aux dires de **François Hollande** cité par *ITespresso.fr*. Aux yeux du Président de la République, *« cette situation nous impose d'augmenter très significativement le niveau de sécurité et les moyens de défense des systèmes d'information »*.

Un effort significatif sera conduit pour développer dans le cyberespace les capacités du pays à détecter les attaques, à en déterminer l'origine et, lorsque les intérêts stratégiques sont menacés, «*à riposter de manière adéquate*».

Marge de manoeuvre

Ce qui laisse une marge d'interprétation et de manoeuvres pour recourir à des dispositifs offensifs dans le cyberespace. Mais le flou subsiste.

Des mesures législatives et réglementaires devraient renforcer les obligations qui incombent aux opérateurs de service et d'infrastructure d'importance vitale pour détecter, notifier et traiter tout incident informatique touchant leurs systèmes sensibles.

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) a néanmoins précisé la portée du Livre blanc. Les opérateurs devront ainsi respecter les référentiels de sécurité à appliquer, mettre en place de «dispositifs de défense adaptés», avoir obligation de déclarer les incidents. En retour, l'Etat doit s'assurer de la conformité des dits niveau de sécurité de ces systèmes et «*en cas de crise grave, d'imposer les mesures nécessaires*».

Les sous-traitants touchés

Selon l'ANSSI, le Livre blanc souligne également l'importance du maintien d'une «*industrie nationale capable de produire en toute autonomie certains équipements de sécurité*». Les cœurs de réseaux télécoms en font partie.

Le fournisseur français de solutions de sécurité Netasq a déjà pris position: «*Avec la proposition faite d'obligation de protection des systèmes d'information pour les opérateurs d'importance vitale et l'obligation de notifier la moindre attaque informatique, c'est aussi tout le tissu industriel de sous-traitance qui sera vraisemblablement concerné*», a déclaré **François Lavaste**, le président de l'entreprise.

Voir aussi

Silicon.fr étend son site dédié à l’emploi IT
Silicon.fr en direct sur les smartphones et tablettes