PACTE DÉFENSE CYBER : VERS UN RENFORCEMENT DE NOTRE POSTURE DE CYBERDÉFENSE

Par Jean-Marie BOCKEL
- ▶ Sénateur UDI-UC du Haut-Rhin
- ▶ Auteur d'un rapport d'information « Cyberdéfense : un enjeu mondial, une priorité nationale »
- ▶ Conseiller municipal de Mulhouse
- ▶ Président de La Gauche moderne

Ces dernières années, les attaques contre les systèmes d'information se sont multipliées en France, comme partout ailleurs dans le monde. Ces attaques informatiques, qu'elles aient pour objectif d'espionner, de saturer, voire de détruire, sont susceptibles de mettre en cause notre défense et notre sécurité nationale. C'est pourquoi, conformément aux recommandations de mon rapport du Sénat de 2012, le Livre blanc de 2013 et la loi de programmation militaire 2014-2019 font de la cyberdéfense une priorité nationale.

Le ministère de la Défense, responsable des systèmes d'information et de communication stratégiques, liés à la dissuasion nucléaire ou au déploiement de nos forces armées, est particulièrement concerné par cette cyber-menace. Il a d'ailleurs été victime en 2013 de 780 incidents informatiques significatifs, soit près du double qu'en 2012. Si certaines dispositions ont déjà été prises, à l'image de la création d'un poste d'officier général à la cyberdéfense et la mise en place d'un Centre d'analyse en lutte informatique défensive (Calid), beaucoup reste à faire.

Dans ce contexte, je me réjouis du lancement début février du « Pacte Défense Cyber » par le ministre de la Défense. Ce Pacte vise avant tout à renforcer le niveau de sécurité et de résilience des réseaux du ministère. Cela se traduira notamment par une augmentation des moyens humains affectés à la cyberdéfense. Les effectifs du centre Maîtrise de l'information de la Direction générale de l'Armement (DGA) à Bruz atteindront près de 400 spécialistes de très haut niveau d'ici 2017, et une unité projetable en opération extérieure sera créée. Sans parler de la cyber-réserve – citoyenne aujourd'hui et à vocation opérationnelle demain – qu'il convient d'encourager.

En outre, cette montée en puissance de notre politique de cyberdéfense passe par le développement d'une industrie souveraine dans le domaine de la sécurité des systèmes d'information. L'enjeu est de constituer une véritable base industrielle et technologique en matière de cybersécurité, avec une dimension européenne indispensable. Pour structurer cette filière, le Pacte, qui préconise l'utilisation d'équipements et de logiciels souverains « partout où cela est nécessaire » au sein de la Défense, entend ainsi soutenir plus activement les PME-PMI du secteur, en appui aux efforts de l'Agence nationale de la sécurité des systèmes d'information (Anssi) et du « plan 33 » de la « Nouvelle France industrielle ».

Le Ministère de la Défense, responsable des systèmes d'information et de communication stratégiques, [...] a été victime en 2013 de 780 incidents informatiques significatifs, soit près du double qu'en 2012

Enfin, il existe aujourd'hui peu d'ingénieurs spécialisés dans la protection des systèmes d'information. Aussi, parallèlement à la sensibilisation et la formation du personnel de la Défense aux règles de cybersécurité, le Pacte envisage la création en 2015 d'un pôle d'excellence en cyberdéfense à Rennes, dédié à la formation et à la recherche mais aussi à l'entraînement à la gestion de cyberattaques. Ces initiatives vont dans le bon sens car elles devraient permettre de voir émerger à terme au sein de nos armées une culture de la cyberdéfense...

En définitive, à travers les actions concrètes de ce « Pacte Défense Cyber », il ne s'agit pas de prétendre à une protection absolue mais de durcir la sécurité des réseaux et des infrastructures les plus sensibles tout en améliorant leur résilience. S'il s'adresse en premier lieu à la communauté de Défense, l'objectif du Pacte me semble bien *in fine* de créer une dynamique, avec 1 milliard d'euros investis d'ici 2019, pour renforcer notre posture globale de cyberdéfense. ●