l'Opinion

Sécurité nationale

Cyberdéfense : la France va se doter d'une armée de réserve

En cas d'attaques informatiques graves, de jeunes informaticiens volontaires seraient mobilisés par l'Etat au sein d'une nouvelle formation

Publié le mercredi 19 juin 2013 à 20h22 - Mis à jour le vendredi 21 juin 2013 à 20h30
Par Jean-Dominique Merchet, Journaliste

Les faits - Le président de la République a annoncé, fin mai, la création prochaine d'une nouvelle réserve militaire pour la cyberdéfense, qui ferait appel à de jeunes professionnels volontaires. Plusieurs milliers de personnes pourraient être concernées, alors que l'Etat renforce ses moyens d'actions dans les armées, avec un commandement opérationnel ou grâce à l'Agence nationale de sécurité des systèmes d'information dont les effectifs augmentent fortement. Un projet de loi renforçant les obligations d'un millier d'établissements définis comme «opérateurs d'importance vitale» est en préparation.

La France va se doter d'une nouvelle "armée de réserve" pour la cyberguerre. Des milliers de volontaires pourraient être mobilisés en cas d'attaques informatiques graves contre notre pays. Ce projet, dont la mise en oeuvre sera précisée au cours des prochains mois, a reçu l'aval de l'Elysée. S'exprimant devant l'Institut des hautes études de défense nationale (IHEDN), le 24 mai, François Hollande a fait part de son intention d'«ajouter» à la réserve militaire actuelle «une branche nouvelle pour la cyberdéfense dont l'objectif sera de mobiliser de jeunes techniciens et informaticiens» sur la base du volontariat.

Après les armées de terre, de mer et de l'air, l'armée du web ? La France semble en prendre le chemin à grands pas. La menace d'attaques informatiques est prise très sérieux, comme en témoigne le récent Livre blanc de la défense et de la sécurité nationale, où le préfixe "cyber" apparaît 37 fois. «Le cyberespace est 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 une menace de première importance», lit-on dans ce document officiel.

Tout un dispositif de défense est progressivement mis en place avec la création d'une Agence nationale de sécurité des systèmes d'information (Anssi) et un commandement spécialisé dans les armées, le cocyber. Parallèlement, la DGSE (Direction générale de la sécurité extérieure) se dote de moyens d'action offensive (lire ci-après).

A quoi ressemblerait cette future «cyberarmée de réserve» ? L'idée de cette garde nationale informatique est née au sein du réseau Réserve citoyenne cyberdéfense, qui réunit près de 80 personnes sous la direction d'un professionnel du secteur, Luc-François Salvador, PDG du groupe de services informatiques Sogeti. Selon les premières réflexions, il s'agirait de disposer de plusieurs centaines de personnes dans chaque région ou zone de défense. «Pas forcément des spécialistes de la cybersécurité, mais des informaticiens ou des gestionnaires de réseaux intéressés par la défense ou la sécurité. Il nous faudra un maillage territorial», indiquent les initiateurs de projet.

Ceux-ci se souviennent d'une attaque massive bien réelle contre les ordinateurs du ministère des Finances à Bercy, fin 2010. Dans un premier temps, il avait fallu une trentaine d'ingénieurs pour comprendre et parer l'attaque, mais pas moins de 300 informaticiens, mobilisés durant tout un weekend, pour redéployer les milliers d'ordinateurs vérolés... La cyberdéfense a besoin de gros bataillons ! Dans l'esprit des concepteurs de ce projet, une mobilisation de cyber-réservistes permettrait de disposer de suffisamment de main d'oeuvre qualifiée pour faire repartir des systèmes attaqués dans un ministère, un hopital, une entreprise de transport ou d'énergie. «Ce projet dépasse donc largement le ministère de la Défense», explique l'amiral Arnaud Coustillière, en charge de la cybersécurité à l'état-major des armées.

Les militaires font déjà appel à un nombre limité de réservistes, recrutés pour leur expertise dans des domaines pointus de la cybersécurité. Ils sont aujourd'hui une quinzaine et pourrait atteindre la cinquantaine. Ces militaires à temps partiel signent un engagement à servir dans la réserve (ESR) opérationnelle et sont appelés plusieurs semaines par an, durant lesquelles ils percoivent une solde comme les militaires d'active.

Les armées ont créé en 2011 leur propre commandement opérationnel de cyberdéfense (cocyber), une petite structure installée au coeur de l'état-major, au Centre de préparation et de conduite des opérations (CPCO) boulevard Saint-Germain, à Paris. Environ 1600 militaires - soit l'effectif d'un très gros régiment - sont aujourd'hui impliqués dans la cybersécurité au sein du ministère de la défense. Le Cocyber dispose d'un bras armé : le Centre d'analyse en lutte informatique défensive (Calid), qui surveille les réseaux de la Défense, détecte les attaques et intervient pour les contrer. La quarantaine de militaires qui y sont affectés ne chôme pas : ils ont traités 420 attaques en 2012, plus du double de l'année précédente (196). Ces attaques sont en général bénignes - le site le plus visé étant... le portail internet du ministère (www.defense.gouv.fr) ou, ces dernières semaines, le site du 1er régiment de chasseurs parachutistes. Rien qui ne mette en péril la sécurité nationale.

Le Calid doit déménager cet été pour s'installer dans un immeuble du front de Seine,

dans la XVème arrondissement de Paris, ou il sera colocalisé avec l'Agence nationale de sécurité des systèmes d'information (Anssi). Créée en 2009, cette agence dépend du Premier ministre. Au sein de la fonction publique, son directeur Patrick Pailloux est un homme heureux : il embauche. «L'Anssi recrute beaucoup. Nos effectifs auront été quasiment quintuplés en cinq ans, passant d'une centaine à 500 en 2015».

L'Anssi se préoccupe des «opérateurs d'importance vitale», dont la cybersécurité est considérée comme relevant de la sécurité nationale. La liste précise de ces opérateurs, qui peuvent être des entreprises, des administrations ou des services publics, relève du secret-défense. Environ un millier d'établissements dans douze secteurs d'activité (santé, transport, banques, etc), sont concernés. Une loi est en préparation pour obliger ces opérateurs à «signaler» à l'Anssi les attaques dont ils sont l'objet et à renforcer leur protection selon des normes contrôlées par l'Etat.

Car en France, la cybersécurité n'est pas optimale, confirme un bon connaisseur du dossier : « C'est assez laborieux de convaincre le management de dépenser de l'argent pour cela. De manière générale, la situation est très perfectible». Or, les attaques se multiplient : «En matière de cyberespionnage, le volume est absolument considérable et le cybersabotage se développe à tour de bras. Les attaques concernent tous les secteurs, mais la France n'est pas plus visée que d'autres» poursuit-il. «Nous devons développer nos capacités d'identification de l'origine de la menace. Dans la plupart des cas, nous avons de sérieuses présomptions, sans avoir de preuve». La Chine est dans tous les esprits...

La cyberdéfense «ne peut s'appréhender qu'en multinational» constatait début juin le ministre de la défense Jean-Yves Le Drian, lors d'un colloque à Rennes. La France coopère étroitement, et discrètement, avec les Etats-Unis, le Royaume-Uni et l'Allemagne, mais également avec Singapour ou le Maroc, avec lequel un accord fin mai. Paris a également rejoint le centre spécialisé de l'Otan à Tallin (Estonie), pays qui avait été l'objet d'attaques de grande ampleur en 2007.