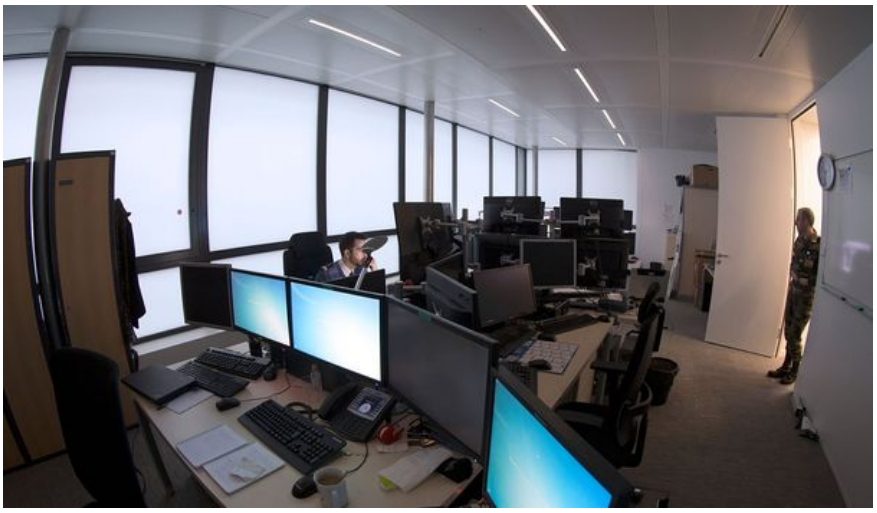
Cyberdéfense: la guerre de demain a déjà commencé

	Cyberdéfense: la guerre de demain a déjà commencé

Paris – A l'heure des cyberattaques en série, notamment après les dernières caricatures du prophète Mahomet, le Calid, « gendarme » des systèmes informatiques de l'armée française, est sur le pied de guerre, derrière la façade discrète d'un immeuble parisien.

Installé devant un rideau d'écrans, un cybersoldat en treillis scrute attentivement les informations qui défilent. Soudain une mention « SUSPICIOUS » (suspect) se détache en rouge sur l'un des ordinateurs.
« J'ai relevé une alerte sur un site, un utilisateur qui essaie d'aller sur un serveur cloud », lâche le sous-officier qui, avec une trentaine d'autres militaires, surveille 24 heures sur 24 les réseaux du ministère de la Défense, à l'affût du moindre intrus mal ou très mal intentionné.
« Ce qu'on cherche à détecter, c'est un pic de réseau anormal, un trafic important de messagerie. On dispose pour cela de +capteurs+ sur les entrées vers nos réseaux, les postes de travail », explique le cybersoldat, qui préfère garder l'anonymat.
Et les ennemis invisibles ne manquent pas. Le 6 janvier, le site du ministère a été piraté par le groupe Anonymous. Ces derniers jours, l'armée a été la cible d'une dizaine de cyberattaques visant notamment des régiments. Le 12 janvier encore, des pirates se réclamant de l'organisation Etat islamique (EI) prenaient brièvement le contrôle des comptes Twitter et Youtube du commandement militaire américain au Moyen-Orient (Centcom).
« Les gens de Daech (acronyme de l'EI en arabe) ont de l'argent, recrutent des informaticiens. Ils manquent peut-être de réseaux de renseignement sur les cibles mais sont capables assez rapidement de bloquer des sites », relève le vice-amiral Arnaud Coustillière, responsable Cyberdéfense à l'état-major des armées.
« C'est de la gesticulation. Mais dans la guerre de l'image, ce peut être très intéressant », ajoute ce spécialiste. Les jihadistes n'ont pas en revanche les moyens, selon lui, de mener des attaques d'envergure.
Le Calid (Centre d'analyse de lutte informatique défensive) surveille aussi les cyberattaques qui peuvent paralyser des systèmes d'armes ou détourner de l'information sur les moyens et les cibles des forces. Il envoie pour cela des équipes au coeur des théâtres d'opération.
Car plus que les attaques de sites internet, voilà bien le véritable cauchemar des états-majors: que des missiles soient stoppés net dans leur course, des drones, piratés, des frégates, détournées à distance au beau milieu d'une intervention militaire.

– 'Dans la peau de l'attaquant' –
En Afrique, l'opération antijihadiste française Barkhane a ainsi été la cible d'une tentative d'attaque cyber, confie-t-on au ministère de la Défense. « Cela peut se faire à partir d'un ordinateur et d'un téléphone ».
Depuis longtemps déjà, James Bond fait des émules. Lors du raid israélien contre de présumées installations nucléaires syriennes en 2007, une attaque numérique a ainsi trompé les défenses adverses en renvoyant une image radar tronquée.
Dans l'affaire Stuxnet, un ver informatique, espionnant et reprogrammant des automates industriels, s'est attaqué aux centrifugeuses iraniennes soupçonnées de faire de l'enrichissement d'uranium à des fins militaires.
Les systèmes sont d'autant plus vulnérables qu'ils sont de plus en plus interconnectés. Sur un navire, navigation, propulsion, combat et communications sont intégrés. Faute de sécurisation, il sera bientôt possible de bloquer le bateau en pleine mer ou de l'empêcher de combattre.
Derrière le Calid, des dizaines de chercheurs de la Direction générale de l'armement (DGA) s'emploient à anticiper cette cyberguerre de demain.
« On se met dans la peau de l'attaquant et on voit quelles attaques on peut mener sur nos propres systèmes d'armes pour voir quelles menaces sont crédibles », raconte Frédéric Valette, chef du pôle sécurité des systèmes d'information à la DGA.
Face à une menace de plus en plus pressante, la France s'est dotée d'un budget cyberdéfense d'un milliard d'euros sur la durée de la loi de programmation militaire (2014-2019). Le Calid doit doubler de taille dans les cinq ans à venir et 400 spécialistes être recrutés.
La France reste loin derrière les Etats-Unis, la Chine et Israël, à un niveau comparable avec la Grande-Bretagne ou la Russie, selon le ministère de la Défense.
« L'idée c'est d'arriver à un niveau de sécurité suffisant. Il n'y a pas de sécurité absolue. Il faut savoir anticiper, mettre en place des niveaux de protection adaptés et être capables de réagir en cas d'attaque », résume M. Valette.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lexpress.fr/actualites/1/societe/cyberdefense-la-guerre-de-demain-a-deja-commence_1642214.html