Cybersécurité : le Royaume-Uni se dote d'une force de dissuasion militaire

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 30 juin 2011

Selon Nick Harvey, secrétaire d'Etat aux forces armées britanniques, le Royaume-Uni développerait un programme militaire offensif pour se prémunir d'une menace cyberterroriste. L'objectif est de doter le pays d'un arsenal informatique permettant de lancer des offensives sur le réseau.

L'utilisation des technologies de télécommunication serait soumise aux mêmes règles d'engagement que pour les moyens d'actions classiques de l'armée, telles qu'appliquées par les forces spéciales britanniques (British Special Forces). Pour Nick Harvey, ce programme ne rend pas la stratégie militaire britannique plus offensive, mais il constitue une nouvelle force de dissuasion face aux menaces grandissantes d'attaques informatiques envers un état. Que ce soient les infrastructures de transport ou d'approvisionnement en énergie ou les transactions bancaires et financières, le fonctionnement d'un pays est aujourd'hui dépendant du bon fonctionnement de son réseau Internet.

Le développement du programme de cybersécurité britannique est piloté par le Cabinet Office et par le Service de renseignements électroniques du gouvernement (GCHQ, Gouvernment Communication Headquarters). Pour répondre à ses nouveaux objectifs, l'armée britannique a lancé un vaste programme de recrutement pour attirer des experts en sécurité informatique. Depuis la publication en octobre 2010 de la Stratégie nationale de sécurité [1] (National Security Strategy), la cybersécurité fait partie des trois menaces traitées comme priorités par le gouvernement britannique. Un second rapport, la révision de la stratégie de défense et de sécurité (Strategic defence and security review) a convaincu le gouvernement d'allouer un budget de 650 M£ supplémentaire pour la cybersécurité.

Pour le professeur Peter Sommer, expert en cybersécurité à la London school of economics (LSE), toute nation qui cherche à développer des moyens de défense contre le cyberterrorisme développe par la même occasion des connaissances pour mettre en oeuvre des moyens d'attaque. Une attaque sur le réseau est peu coûteuse, facilement camouflable et peut sauver des vies. La question est alors de savoir quelles seront les règles d'intervention.

En mai 2011, le MI6, service de renseignements extérieurs du Royaume-Uni, associé au GCHQ, a piraté un site Internet utilisé par al-Qaeda pour diffuser des manuels sur la fabrication de bombes artisanales. L'attaque baptisée "Operation Cupcake" a consisté à remplacer le lien vers le manuel en ligne par un lien vers un livre de cuisine sur la préparation des cupcakes, qui sont des petits gâteaux anglais.

Les menaces de cybersécurité sont aujourd'hui prises très au sérieux par la plupart des grands pays. Selon le Wall Street Journal, le Pentagone américain devraient prochainement publier un document considérant les actes de piratage informatique contre un gouvernement comme des actes de guerre. En 2008, suite à des attaques informatiques contre le gouvernement estonien, l'OTAN a créé le Centre d'excellence en cyberdéfense (CCDCOE, Cooperative Cyber Defence Centre of Excellence) à Tallin. D'autres pays prennent des mesures plus draconiennes pour se prémunir des menaces sur le réseau. Après que ses installations nucléaires aient été infectées par le virus Stuxnet, l'Iran a annoncé vouloir créer son propre réseau national de télécommunication et se déconnecter progressivement du réseau Internet. Enfin, de nouvelles attaques informatiques au mois de mai 2011 sur des comptes Gmail sont venues raviver les tensions entre la Chine et Google.

Post-scriptum :

http://www.bulletins-electroniques....