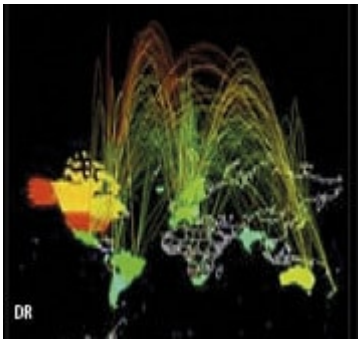

Cyberdéfense : placer l'excellence militaire au service de la nation

Monde à part entière, le cyberespace a pris une dimension stratégique, où interviennent souveraineté nationale, espionnage, aspects juridiques, relations internationales et accélération technologique.

Officier général « cyberdéfense » à l'État-major des armées, le contre-amiral Arnaud Coustillière, a fait le tour de la question au cours d'une conférence-débat organisée, le 11 mars 2014 à Paris, par l'Association région IHEDN Paris Ile-de-France.

Domaine militaire. Coordinateur des mesures pour développer la cybersécurité au sein du ministère de la Défense, l'amiral est responsable de la conduite des opérations en cas de crise cybernétique. A ce titre, il fait partie de l'équipe dirigeante du Centre de planification et de conduite des opérations (CPCO) de l'État-major des armées. Le CPCO a une vision transverse de tous les moyens et organisations militaires. Il assure la planification opérationnelle des effets des frappes dans la profondeur ou du ciblage et collecte des renseignements d'intérêt civil et militaire. Il établit la cartographie des points forts et des faiblesses de la France en matière de cyberdéfense. Tous les organismes sont visés par la « cyberpollution » et les « cyberdivisions » frappent les sites du ministère de la Défense. En 10 jours, 6.000 sites français ont fait l'objet d'attaques venues de l'Algérie : un drapeau algérien apparaissait sur l'écran ! Acte technique contre un objectif stratégique, la cyberattaque est modulable selon l'effet recherché. En France, un cadre juridique garantit aux autorités politiques la possibilité de capacité offensive, après identification de l'origine de l'acte et en limitant autant que possible les effets collatéraux, comme pour le lancement d'un missile. « *On*

ne dira pas comment on fait », précise l'amiral. Le ministère de la Défense va installer un pôle de cybersécurité en Bretagne (Rennes), où se trouve déjà le centre d'expertise de la Délégation générale pour l'armement (DGA). Il s'agit de former des opérationnels d'un niveau Master « bac + 6 » et non plus « bac + 4 ». Quelque 400 postes seront créés pour la formation à des actes techniques. Un centre de formation à la gestion de crises cybernétiques sera ouvert à l'École spéciale militaire de Coëtquidan et accessible aux étudiants civils. Pour disposer de ressources humaines conséquentes, une filière sera instaurée pour garantir un plan de carrière aux militaires spécialisés. L'armée américaine a déjà créé un corps de cyberdéfense au sein de l'artillerie. « *Plus ça avance, plus on se rapproche du cœur des opérations, afin de déterminer qui fait quoi et quelles sont les zones dangereuses* », explique l'amiral Coustillière. Il s'agit de constituer un réseau de partenaires de confiance dans le cadre de coopérations bilatérales et de relations internationales (diplomatie d'influence). Le Livre Blanc 2013 de la défense et de la sécurité nationale ainsi que la Loi de programmation militaire 2014-2019 prévoient un budget de 1 Md€ et la création de 550 postes pour les armées et la DGA. Des centres de formation seront également établis à Grenoble et Limoges.

Monde civil. La cybersécurité, enjeu de souveraineté, protège les infrastructures vitales (banques et transports) et les données industrielles. Ce secteur crée des emplois de proximité dans une zone de confiance et qui ne sont pas délocalisables en Inde ou en Chine. L'État français est peu présent dans la conduite de l'internet, indique l'amiral Coustillière. Mais depuis 2014, des textes législatifs l'engagent au niveau des ministères de l'Intérieur (gendarmerie et police) et de la Défense pour la réorganisation de l'action interministérielle. Le plan de cybersécurité inclut des recommandations pour les petites et moyennes entreprises (PME) et les grands groupes qui, comme le franco-allemand EADS et l'américain Boeing, ont des sous-traitants communs. En 2014, les investissements dans les projets de recherche et développement sont multipliés par trois par rapport à 2012, dont 15-20 % du financement peut être pris en charge par la DGA dans la cadre du dispositif RAPID (Régime d'appui PME pour l'innovation duale civile et militaire). La Loi de programmation militaire (LPM) 2014-2019 encadre les rapports entre l'État et 200 organismes d'intérêt national avec notamment la déclaration des incidents, la certification d'audits et la validation des matériels de télécommunications par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Faute de capacité technique, les PME sont souvent mal

défendues. L'attaquant recherche le maillon faible : frapper l'administration du réseau pour atteindre le niveau financier en envoyant une pièce jointe dangereuse qui, par réaction en chaîne, téléchargera des données. La protection commence par l'éducation du personnel : 90 % des attaques sont contrées par des mesures simples, comme le changement fréquent de mot de passe. Opérationnelle depuis 2011, l'ANSSI comptera 1.500 personnes en 2015. Le plan de cybersécurité sera mis à jour en 2017.

Relations internationales. « *Il n'y a ni allié ni ami dans la guerre économique* », rappelle l'amiral. Il s'agit de protéger les secrets industriels nationaux face à la multiplication des services de renseignement (SR). Contrairement au droit anglo-saxon, flou en la matière, le cadre juridique français sépare les entreprises qui travaillent dans le cyberespace et les organismes qui les protègent. Les entreprises françaises ont tendance à donner facilement leurs données, enjeux pourtant majeurs qui nécessitent une démarche européenne lors des négociations de libre-échange avec les États-Unis. Alors que la Chine et les États-Unis s'affrontaient depuis longtemps en matière d'espionnage, ces derniers se sont retrouvés en position d'accusés après les révélations, en mai 2013, de l'informaticien américain Edward Snowden sur les programmes britanniques et américains, dont ceux de la NSA, de surveillance et d'écoute de masse. Comme lors du conflit russo-géorgien en 2008, des éléments pro-russes ont perpétré des cyberattaques en Ukraine en février et mars 2014, pour déstabiliser la société et prendre le contrôle des installations cybernétiques du pays. La guerre de l'information et des signaux s'est poursuivie par des cyberattaques pro-ukrainiennes contre des installations pro-russes. Enfin, selon l'amiral Coustillière, les mafias ukrainiennes sont redoutables en matière de cybercriminalité.

Loïc Salmon

Cyberespace : nouveau terrain d'affrontement international

Nouvelles armes informatiques pour des attaques mieux ciblées

La doctrine française de cyberdéfense repose sur deux volets complémentaires. Le premier porte sur la mise en place d'une posture robuste et résiliente de protection des systèmes d'information de l'État, des opérateurs d'importance vitale et des industries stratégiques, couplée à une organisation opérationnelle de défense de ces systèmes, coordonnée sous l'autorité du Premier ministre. Le

second consiste en une capacité de réponse gouvernementale globale et ajustée, face à des agressions de nature et d'ampleur variées, faisant en premier lieu appel à l'ensemble des moyens diplomatiques, juridiques ou policiers, sans s'interdire l'emploi gradué de moyens relevant du ministère de la Défense, si les intérêts stratégiques nationaux sont menacés.