Edito

Comme le note le Secrétariat Général de la Défense et de la Sécurité Nationale dans le cadre du document préparatoire à l'actualisation du *Livre blanc sur la défense et la sécurité nationale*[1], les cyber attaques semblent augmenter à la fois en raison de la progression du cyberespionnage et de la multiplication des attaques informatiques en direction des Etats, des institutions ou des entreprises posant des problèmes stratégiques importants pour toutes ces organisations. « *Plus d'un million de personnes sont victimes de cybercriminalité tous les jours* » d'après la commission européenne.

Les cyber menaces sont en premier lieu des actes de criminalité financière. L'usage généralisé des NTIC et d'Internet a permis à la délinquance de s'ouvrir à de nouveaux marchés et de toucher de plus en plus de monde. Internet favorise la recherche de clients ou de victimes dans le cadre d'escroquerie, de ventes de produits illégaux ou d'exploitation des êtres humains. Les attaques par déni de service (DDOS), qui sont souvent assimilées à de nouvelles formes de contestation (cf. l'article sur Anonymous de Frédéric Bardeau et Nicolas Danet), sont aujourd'hui de nature beaucoup plus criminelle qu'il n'y paraît, les auteurs de ces attaques utilisant maintenant leurs ressources pour extorquer des sommes aux entreprises.

Un deuxième type de menace est naturellement l'espionnage. Les attaques informatiques contre les systèmes d'information des Etats et des entreprises se seraient multipliées d'après le SGDSN. Une enquête réalisée par le CDSE en 2010 auprès de grands groupes internationaux montre que cette question constitue la troisième forme d'infractions perpétrées contre les entreprises (39% d'entre elles) derrière le vol de produits et la fraude interne mais devant la contrefaçon ou la corruption. Ces attaques visent les données sensibles de leurs cibles. Elles sont souvent de grande ampleur, fruits d'une longue préparation et d'un ciblage précis. Elles tirent profit de la difficulté à attribuer avec certitude leur origine.

Un troisième type de menace pourrait, à terme, concerner la destruction ou le contrôle des systèmes informatisés de production, les fameux systèmes SCADA. La découverte du ver informatique *Stuxnet* en juin 2010 a prouvé qu'un code informatique malveillant pouvait porter atteinte à des infrastructures critiques totalement isolées d'Internet, par une attaque de leurs systèmes d'information et de contrôle.

Le cyberespace, formidable source d'enrichissement pour les Nations, de connaissance et de mise en relation (2 milliards d'internautes), introduit également une sensibilité accrue aux défaillances accidentelles, aux malveillances internes ou externes ainsi qu'aux éventuelles opérations de désinformation ou de propagande. Rappelons les campagnes honteuses relatives au 11 septembre 2001.

Le cyberespace est un lieu de renforcement des capacités des acteurs non étatiques. Si ces pirates informatiques ne sont pas nouveaux, leurs attaques semblent de plus en plus nombreuses et virulentes à l'encontre des Etats et des entreprises, en particulier émanant de groupes « hacktivistes » cherchant à porter atteinte à la réputation de certaines d'entre elles. Ainsi d'Anonymous qui s'est attaqué à des intérêts économiques et institutionnels de premier plan au cours de ces derniers mois, divulguant à grande échelle des informations confidentielles. Pensons au cas de Stratfor, entreprise américaine dans le domaine du renseignement qui s'est vue dérober des données (mails, mots de passe cryptés...) sur ses membres dont une large partie vient du Département d'État et du Département de la Défense américains, ou encore des représentants de banques internationales, dont Bank of America et JP Morgan Chase, ou des géants de la technologie comme IBM et Microsoft. Quelles sont les conséquences en termes de réputation pour cette entreprise et, de manière indirecte, pour les entreprises et administrations membres ?

Derrière ce rapide panorama conclusif des menaces et des risques, il demeure une question en suspens. Est-on scientifiquement sûr de ces évolutions ? S'il est permis de se faire un idée des tendances en matière de cybercriminalité, du profil type des hackers, ainsi que des modes d'organisation, cela reste pour l'heure davantage de l'ordre des perceptions que des certitudes. Il y a naturellement des enquêtes et sondages réalisés par des grands cabinets américains. Mais quelle est la valeur de ces sondages, alors qu'ils sont réalisés par des fournisseurs de technologies de sécurité ? De même, si le S.G.D.S.N. constate dans le cadre du livre blanc une augmentation de ces différents phénomènes, laissant suggérer que le mal est plus profond qu'il ne l'était, le constat souffre d'un manque de précisions sur l'étendue des dégâts. De nombreuses interrogations subsistent qui résultent en partie, pour l'heure, de la faiblesse des recherches à l'échelle internationale dans le domaine de la cybercriminalité. En cela on ne peut que rejoindre les conclusions dans ce numéro de Franck Guarnieri et d'Eric Pryswa qui déplorent l'absence de centre de recherche universitaire directement ou indirectement dédié aux enjeux de cybercriminalité selon une approche pluridisciplinaire en sciences humaines et sciences sociales.

Nous ne pouvons donc conclure ce propos liminaire sans appeler de nos vœux à la fois au développement de recherches en matière de cybercriminalité et à l'émergence d'échanges interdisciplinaires sur le sujet. En cela, ce nouveau numéro de *Sécurité & Stratégie* permettre, nous l'espérons, d'alimenter de prochains débats qui s'annoncent à la fois très riches et très stimulants. ■

Olivier Hassid

[1] *Secrétariat général de la défense et de la sécurité nationale, La France face aux évolutions du contexte international et stratégique, Document préparatoire à l'actualisation du Livre blanc sur la défense et la sécurité nationale, http://www.sgdsn.gouv.fr/IMG/pdf/Doc_preparatoire_LBDSN-2012_.pdf*