Préface au numéro hors-série "Cybersécurité"

Par le vice-amiral Arnaud Coustillière

En janvier dernier, suite aux attaques terroristes contre le journal *Charlie Hebdo* et l'épicerie casher de Vincennes, la France subissait une vague d'attaques informatiques visant plusieurs milliers de sites Internet institutionnels et privés français. En 2010, l'attaque *Stuxnet* contre le SCADA[1] d'une centrifugeuse nucléaire iranienne révélait le cyberespace comme un champ de confrontation pour les États. Désormais, les attaques informatiques quotidiennes contre des sociétés et leur impact financier confèrent à la lutte contre les cybermenaces une dimension stratégique pour tous les acteurs, aussi bien étatiques que privés. En 2015, le rapport annuel du Forum économique mondial sur les risques globaux classait la menace cyber parmi les risques les plus importants en termes de probabilité et d'impact sur les dix prochaines années, tandis qu'en France, selon une étude récente conduite auprès de 29 grandes sociétés, le coût annuel moyen de la cyber-criminalité est évalué à 4,8 millions d'euros par entreprise.[2] Afin de lutter contre les menaces dans le cyberespace, la France a fait le choix d'une stratégie nationale cohérente fondée sur le *continuum défense-sécurité* afin de protéger les infrastructures vitales tout en préservant notre industrie. L'État français a mis en œuvre un effort national parmi les plus avancés dans le monde : en 2011, une stratégie nationale de cybersécurité a été adoptée, et l'Agence nationale de sécurité des systèmes d'information (ANSSI) a été mise en place afin de coordonner la politique de cybersécurité en France.

Les technologies de l'information et de la communication innervent notre quotidien, les activités humaines ont en effet été largement numérisées. La diversification des supports numériques, la multiplication des objets connectés et des échanges dématérialisés (réseaux sociaux notamment) constituent un champ d'action nouveau pour une entité cherchant à exploiter des failles à des fins de renseignement ou d'action. Il est désormais possible de perturber le fonctionnement d'un système, de voler des données, de causer des dysfonc-tionnements dans des systèmes industriels, tout en étant à distance. Ces modes d'action peuvent être exploités par des acteurs divers : États, *hackers*, "hacktivistes", individus isolés, ou encore entreprises, comme l'a illustré *Sony Pictures Entertainment* en décembre 2014 en lançant une attaque par déni de service suite au vol de données sur ses réseaux.

Le sentiment d'une vulnérabilité importante liée à la dépendance de nos activités aux systèmes d'information et de communication (SIC) et aux menaces portées par le cyberespace a encouragé les États à prendre en compte le sujet de façon prioritaire dans la mesure où ce nouveau champ d'action est un support pour la diffusion de visions

[1] Supervisory Control And Data Acquisition : système de contrôle et de mesure à distance d'installations techniques.

[2] Ponemon Institute (en partenariat avec Hewlett-Packard), "2014 Cost of Cyber Crime Study : France".

Publié in *Res Militaris* (http://resmilitaris.net)**, hors-série** "**Cybersécurité**", **juillet 2015**

politiques, voire idéologiques : François Chauvancy présente cette dimension dans son article. Tandis que les nations occidentales (États-Unis, Royaume-Uni, France) visent à assurer la sécurité des systèmes sans en contrôler le contenu, d'autres États (Chine, Russie) défendent la protection des contenus, et donc leur contrôle. La France a pleinement intégré la menace cybernétique dans le champ de sa diplomatie et est impliquée dans les réflexions en cours au sein de l'ONU, de l'OTAN et de l'Union européenne sur le cyberespace.

Le *Livre Blanc sur la Défense et la Sécurité Nationale* de 2013 définit la cyber-défense comme un enjeu de sécurité nationale et de souveraineté, il désigne le cyberespace comme un champ de confrontation à part entière[3] et érige la cyberdéfense au statut de nouvelle donne stratégique. Désormais, les menaces cybernétiques constituent une menace stratégique pour la France au même titre qu'une agression commise par un autre État, une attaque terroriste, une atteinte au potentiel scientifique et technique de la nation, la criminalité organisée, ou encore une crise majeure résultant de risques naturels, sanitaires, technologiques, industriels ou accidentels.[4] Le ministère de la Défense a intégré le combat dans l'espace numérique dans ses procédures opérationnelles : les articles d'Aymeric Bonnemaison, Gaëtan Sciacco et du général Denis Mercier présentent les évolutions dans la conduite des opérations militaires et la combinaison des opérations numériques avec le champ de bataille traditionnel. Il doit répondre à l'impératif suivant : garantir l'efficacité opérationnelle des Forces pour accomplir les missions ordonnées par les autorités politiques en toutes circonstances, même dans un contexte de crise cybernétique, tout en garantissant le bon fonctionnement du ministère. Les moyens cyber militaires sont pleinement inclus dans le champ des capacités militaires dont dispose la Force, le cyberespace est désormais considéré comme un environnement de combat au même titre que la terre, l'air, la mer et l'espace et les opérations numériques sont placées au cœur du combat.

Si les forces armées ne sont pas toujours en première ligne, elles peuvent apporter une contribution décisive en soutenant la communauté nationale de cyberdéfense. Le général Watin-Augouard démontre la pertinence du continuum défense-sécurité dans le cyberespace. L'ensemble des contributions à ce numéro de la revue ***Res Militaris*** alimentent la réflexion sur le cyberespace comme nouvel espace de combat, et plus généralement au rôle des États dans la lutte contre les cybermenaces. Cette réflexion collective est indispensable à la formulation de réponses innovantes aux nouveaux enjeux que soulève le cyberespace.

---

[3] *Livre Blanc sur la Défense et la Sécurité Nationale*, 2013, p.45.
[4] *Ibid*., p.10.