L'ère de la cyberguerre est déjà bien entamée. Ce jeudi 15 février 2018, le ministère des Affaires étrangères britannique, soutenu par la Maison Blanche, vient d'accuser la Russie d'être derrière la cyberattaque NotPetya, au printemps 2017. Les cibles principales de cette attaque d'un nouveau genre? Les secteurs financiers, énergétiques et gouvernementaux ukrainiens. Sa «conception sans discernement a entraîné sa propagation» à travers le monde, accuse le Gouvernement britannique, multipliant ainsi les victimes collatérales.

Ces graves accusations de nos voisins d'outre-Manche s'appuient sur un rapport technique de son centre national de cybersécurité, une division du Government Communications Headquarters (GCHQ), l'un des services de renseignement spécialisés dans les interceptions. Pour ces derniers, c'est l'armée russe qui est responsable de cette attaque qui a coûté «des centaines de millions de livre sterling». Le quotidien *Le Monde* chiffre pour sa part les dégâts à plus d'un milliard d'euros. Le Gouvernement russe a démenti être responsable de cette attaque.

Des victimes en France

En France, le logiciel malveillant NotPetya a fait plusieurs victimes, le constructeur automobile Renault mais aussi l'industriel Saint-Gobain. Ce spécialiste du bâtiment a estimé l'impact de l'attaque à 250 millions d'euros sur ses ventes et à 80 millions d'euros sur le résultat d'exploitation ! Contrairement aux "Fives Eyes" (l'Australie, la Nouvelle-Zélande et le Canada se sont également associés à l'accusation britannique), la France n'a pas choisi d'aller sur le terrain délicat de l'attribution de cette attaque.

> «L'attribution des cyberattaques complexes demeure très difficile. Il est très ardu de récupérer une preuve scientifique formelle pour imputer l'attaque à quelqu'un ou une organisation. Nommer l'ennemi est un acte politique fort. Cela complexifie grandement les règles d'engagement.»
>
> Alexandre Papaemmanuel, directeur sécurité et renseignement intérieur chez Sopra Steria, à L'Essor.

Ce qui ne veut pas dire que les pouvoirs publics ne font rien. Ils mettent au contraire les bouchées doubles pour muscler la cyberdéfense. Coup sur coup, deux documents viennent de donner un coup de fouet à l'armée numérique française: la loi de programmation militaire et la *Revue stratégique de cyberdéfense*.

La loi de programmation militaire, présentée le 8 février 2018 en Conseil des ministres, donne la part belle à la cyberdéfense. 1,6 milliard d'euros seront consacrés à la lutte dans le cyberespace d'ici 2025 avec, comme objectif, de recruter 1000 cybercombattants de plus, pour arriver à un total de 4000 cybersoldats. En tout, 1500 recrutements pour la cyberdéfense et le numérique sont prévus dans les 6 ans à venir, soit un quart des hausses d'effectifs prévues.

L'Essor de la Gendarmerie nationale française, 22 février 2018.

Pour en savoir plus: https://lessor.org/france-muscle-cyberdefense/#iLYW9U9kL1sQiUEp.99