La cyberguerre ou la remise en question du rang de la France sur la scène internationale

cahier de la pensée mili-Terre

le Chef de bataillon Bruno EMPTAZ

publié le 04/06/2018

Sciences & technologies

En se basant sur des exemples variés et éloquents de cyberattaques, cet article démontre l'impérieuse nécessité de considérer la cyberguerre comme un fait acquis et non comme une hypothétique menace née de quelques esprits alarmistes. Il rappelle également les mesures concrètes prises par les pouvoirs publics français depuis le livre blanc de 2008, particulièrement au sein du ministère de la Défense. Une comparaison avec d'autres grandes nations révèle enfin l'ampleur de la menace et le chemin à parcourir pour garantir le rang de la France dans ce nouvel espace conflictuel.

Le cyberespace: «espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques».

Cette définition technique et restrictive, donnée par le SGDSN en 2011 dans sa stratégie de défense et sécurité des systèmes d'information, pourrait cantonner le cyberespace au rôle de cinquième champ de bataille évoqué par certains auteurs, après la terre, l'air, la mer et l'espace. Mais la cyberguerre, dans une approche moderne des rapports internationaux, basée bien davantage sur le smart power américain que sur les rapports de force conventionnels hérités de la guerre froide, prend une dimension transverse nettement plus importante. La guerre dans cet espace virtuel ne ressemble plus à une confrontation militaire classique entre États, mais se décline en actions multiples et bien réelles dans chaque secteur stratégique: la sécurité, l'économie, l'énergie, l'information…

Dès 2009, le président Obama s'en inquiétait en faisant de la cyberdéfense l'une des priorités de son mandat: «La menace cybernétique est l'un des plus importants défis auxquels doivent faire face les États-Unis, en matière économique et au regard de la sécurité nationale».

Les événements lui ont donné raison, tant la diversité et le nombre des attaques ont démontré que la cyberguerre ne relevait pas de la science-fiction. Dès lors, une course effrénée à la cyberdéfense a été engagée par les puissances mondiales afin de protéger leurs intérêts vitaux et conserver leur suprématie. La France n'a pas dérogé à la règle,

particulièrement dans le secteur de la défense, même si l'effort à réaliser dans ce domaine, gage du maintien de son rang sur la scène internationale, s'avère permanent et coûteux.

La guerre dans le cyberespace présente une grande variété de déclinaisons, tant par les techniques employées, les cibles visées, l'origine des actions et, accessoirement, leur motivation. Les cyberattaques visent ainsi les informations, mais aussi les systèmes d'information et de communication (SIC) qui les contiennent, et même certains équipements ou installations physiques. Les conséquences peuvent en être multiples: obtention de la primauté sur l'information, récupération de secrets industriels ou sécuritaires, neutralisation de systèmes d'armes, de moyens de communication et destruction d'infrastructures sensibles.

«La cyberguerre est bien déclarée»

Le phénomène le plus connu est sans doute le cyberespionnage, notamment suite à la retentissante affaire Snowden, le consultant de la National Security Agency (NSA) qui a révélé une vaste campagne d'espionnage orchestrée par cette agence par l'intermédiaire de grandes firmes américaines opérant dans le secteur de l'Internet. La découverte en mai 2012 par l'éditeur russe d'anti-virus Kaspersky Lab d'un logiciel malveillant particulièrement puissant, baptisé FLAME, a été moins médiatisée mais tout aussi significative[1].

Les cibles de cet espionnage moderne sont variées, le «cybercommander» américain, le Général Alexander, reconnaissant récemment que les systèmes du département de la défense étaient attaqués près de six millions de fois par jour. De graves intrusions dans les systèmes d'information du Pentagone, du département d'État ou encore de la NASA ont également été constatées ces dernières années et largement imputées au concurrent chinois.

La France et ses quelques deux cents «opérateurs d'importance vitale» (OIV) publics et privés, répertoriés notamment dans le secteur industriel, présentent également un grand intérêt pour les pirates. M. Le Drian, le ministre de la Défense, tient un langage sans ambiguïté à ce sujet: «C'est désormais l'atteinte aux intérêts stratégiques de l'État et à notre autonomie d'appréciation, de décision et d'action par menace cyber (…) qui est un enjeu majeur de défense et de souveraineté».

La technique de denial of service (DoS) attack est également courante. Elle vise à saturer les serveurs afin d'empêcher tout accès à certains services informatiques, notamment de sites institutionnels.

L'attaque massive contre le cyberespace géorgien qui a précédé l'intervention russe en Géorgie en 2008 en a été une illustration et le premier cas connu d'intégration d'une cyberattaque dans une manœuvre militaire globale.

Le risque d'un «cyber Pearl Harbor»

D'autres types d'attaques élèvent encore le niveau de menace en engageant concrètement la sécurité physique d'infrastructures et d'individus par une action directe sur les systèmes d'information et les logiciels d'équipements critiques dans les secteurs industriel, énergétique ou encore des transports. Leon Panetta, le secrétaire d'État américain à la défense, estime même que «certains pays seraient déjà capables de provoquer un cyber Pearl Harbor pire que le 11 septembre! Des assaillants pourraient faire dérailler un train de voyageurs ou un convoi de produits chimiques dangereux. Ou encore, contaminer les systèmes d'eau des grandes villes ou éteindre une grande partie du réseau électrique». L'ironie de ce constat est que son illustration la plus significative reste le virus informatique STUXNET, probable fruit d'une coopération américano-israélienne, qui a permis de retarder le programme nucléaire iranien en endommageant les centrifugeuses Siemens du site d'enrichissement d'uranium de Natanz.

Le secteur de la défense est bien évidemment une cible privilégiée de ces diverses attaques, alors que l'efficacité des systèmes d'information et de communication (SIC) est unanimement reconnue comme une des clés de la supériorité opérationnelle. La numérisation de l'espace de bataille (NEB), la complexité des systèmes d'armes et la recherche d'une interopérabilité croissante entre les SIC alliés (à l'exemple de l'Afghanistan mission network de l'ISAF) sont autant de sources de vulnérabilité. À titre d'exemple, une frégate multi-missions (FREMM) rassemble aujourd'hui près de 2.400 systèmes d'information.

La cyberguerre est d'autant plus pernicieuse que le flou juridique qui l'entoure et les balbutiements de la coopération internationale, notamment au sein de l'UE et de l'OTAN, ne permettent pas encore d'y apporter une réponse homogène et globale. La récente affaire Snowden démontre même que le cyberespace permet les coups les plus bas entre partenaires officiels et concurrents officieux.

Les rapports tendus dans ce domaine entre les États-Unis et la Chine en sont une manifestation paroxystique. L'empire du milieu est régulièrement accusé de recourir à un espionnage industriel et militaire massif, comme le démontre notamment le rapport très étayé de la société de sécurité Mandiant en février 2013.

Les récentes informations du Washington post sur l'accès de pirates aux plans des systèmes d'armes les plus perfectionnés de l'armée américaine, tels que le missile Patriot, le radar Aegis et le programme de développement du chasseur F-35, pourraient être lourdes de conséquences.

De plus, l'origine des cyberattaques ne se cantonne pas formellement aux services étatiques. Elle relève, notamment dans le cas chinois, d'officines privées agissant au profit de l'État, mais aussi de groupes d'activistes, de terroristes ou de criminels aux motivations financières ou idéologiques. Ces divers acteurs malveillants profitent de deux facilités

offertes par le cyberespace.

D'abord, nul besoin d'investissements humains et financiers conséquents pour engager une cyberattaque. Quelques ordinateurs connectés et des malware ou spyware (virus malveillants ou espions) performants, téléchargeables en ligne, permettent à une poignée de hackers, délocalisés et sans lien direct avec le service commanditaire, d'engager une cyberattaque.

Ensuite, la difficulté de localisation de l'assaillant, entretenue par le recours généralisé à des adresses IP piratées, à des logiciels d'anonymisation (de type TOR), à des ordinateurs «zombies» ou à un système de rebonds sur des serveurs situés dans différents pays, contribue à son impunité.

Ces facilités auxquelles s'accommodent de mieux en mieux certains «rogue states» ou groupes terroristes ne font qu'amplifier les risques pour les États ciblés. Ainsi, le 20 avril 2013, le compte Twitter d'Associated Press était hacké, ce qui permit de diffuser de fausses informations concernant une attaque sur la Maison Blanche ayant blessé le président Obama. Cette action a ensuite été revendiquée par la Syrian Electronic Army, proche du régime d'El-Assad.

Selon James Clapper, directeur national du renseignement (DNI), le cyberterrorisme constitue la menace la plus grave à l'encontre des États-Unis, précisant que les groupes terroristes affiliés à Al-Qaïda commencent aussi à développer des capacités de cyberattaques perfectionnées.

La guerre dans le cyberespace ne peut donc plus être considérée comme une théorie hypothétique entretenue par quelques auteurs catastrophistes. Par l'étendue des domaines qu'elle concerne, la gravité des conséquences qu'elle est susceptible d'engendrer et le contexte très favorable dont elle bénéficie, elle doit au contraire être considérée comme un problème concret. C'est sans doute ce qu'estime Hamadoun Touré, secrétaire général de l'union internationale des télécommunications (UIT), quand il affirme solennellement: «La cyberguerre est bien déclarée».

L'indispensable maîtrise des armes de cyberguerre

Le Livre blanc sur la défense et la sécurité nationale de 2008 attestait déjà d'une prise de conscience de ce nouvel enjeu: «Dans les 15 ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude».

Cela aboutit à la création dès 2009 d'une autorité nationale rattachée au secrétaire général de la défense et de la sécurité nationale, l'agence nationale de la sécurité des systèmes d'information (ANSSI). Celle-ci publie en janvier 2011 une stratégie interministérielle en matière de défense et de sécurité des systèmes.

Du fait de ses spécificités, le ministère de la Défense développe parallèlement ses propres structures de cyberdéfense. Pour protéger ses systèmes d'information et de communication dédiés, il a édifié une chaîne de commandement opérationnel interarmées sous l'autorité du chef d'état-major des armées et intégrée au CPCO. En 2011, un «concept interarmées de cyberdéfense» est élaboré et un OG CYBER (officier général en charge de la cyberdéfense) est nommé, le Contre-amiral Coustillière. Conseiller du CEMA et des autorités du ministère, il conduit la lutte informatique défensive (LID) au moyen d'un dispositif réactif. Son bras armé, le centre d'analyse en lutte informatique défensive (CALID), surveille les réseaux et recherche les parades aux infections informatiques. Il s'intègre ainsi à Piranet, le plan interministériel de réaction aux cyberattaques, qui prévoit notamment l'engagement sur très court préavis de véritables commandos informatiques, les «groupes d'intervention rapide» (GIR).

Le travail collaboratif du CALID au sein et à l'extérieur du ministère est également un gage d'efficacité. Il s'appuie pour cela sur l'expertise technique qu'entretient la DGA sur son site «maîtrise de l'information» de Bruz, où sont notamment traquées d'éventuelles failles de sécurité sur les systèmes d'armes et les systèmes d'information des armées. Il bénéficie aussi d'une réserve citoyenne de cyberdéfense, constituée d'un noyau de volontaires accrédités par l'autorité militaire, dont une cinquantaine d'ingénieurs capables de renforcer le dispositif en cas de crise majeure.

Le «renseignement d'intérêt cyberdéfense», fourni en boucle courte par la DGSE, la DRM et la DPSD, complète le dispositif en anticipant certaines menaces.

Sur le plan interministériel, le CALID anime un réseau permanent d'échange d'informations techniques et opérationnelles. Il collabore étroitement avec le centre opérationnel de l'ANSSI (le COSSI), avec lequel il devait d'ailleurs être colocalisé d'ici à la fin de l'année 2013.

Depuis le Livre blanc de 2013 et la constatation de certaines lacunes, des efforts supplémentaires ont été consentis pour préparer l'avenir. Cela conduit au triplement des crédits consacrés à la recherche et au développement dans le domaine de la cyberdéfense, qui passeront à 30 millions d'euros par an. La promotion des compétences au profit de la défense est également renforcée par la montée en puissance du pôle d'excellence universitaire de la cybersécurité en Bretagne, dont dépend notamment la chaire de recherche «cyber» des écoles de Saint-Cyr Coëtquidan (soutenue par THALES). Enfin, la nouvelle loi de programmation militaire devrait prévoir une augmentation conséquente du personnel travaillant dans ce secteur: près de 20% en plus, pour approcher les 2.000 personnes au sein du ministère.

«Avons-nous été trop naïfs?...»

La question subsiste néanmoins: au regard des risques encourus dans le cyberespace, la France a-t-elle pris toutes les mesures nécessaires pour parer à une cyberguerre engageant ses intérêts vitaux? Jean-Yves Le Drian, le ministre de la Défense, s'interrogeait lui-même lors d'un colloque sur la cybersécurité en juin 2013: «Avons-nous

été trop naïfs, trop confiants dans le développement de l'Internet et, plus largement, des systèmes d'information?»

Ce questionnement revêt une acuité particulière au regard de la course au «cyberarmement» entrepris par certaines nations, qui durcissent simultanément leur doctrine d'emploi dans le cadre d'une cyberguerre.

Les Américains s'offrent ainsi des moyens à la hauteur des enjeux et de leur leadership incontestable dans le domaine. Ainsi, la cyberdefence constitue un des rares postes en hausse dans le budget de la défense américaine. La presse nationale évoque 10 milliards de dollars de budget annuel et des milliers de recrues. Rien que le cyber command devrait voir ses effectifs multiplier par cinq, pour atteindre à court terme 4.900 personnes.

Deux de nos alliés majeurs, la Grande-Bretagne et l'Allemagne, évoquent également un effort budgétaire conséquent à ce sujet.

La Chine, dotée d'un dispositif cybernétique nébuleux du fait d'un système de sous-traitance civile, compterait près de 20.000 personnes dédiées à ce secteur au sein du «troisième département de l'armée populaire de libération», renforcées d'un nombre conséquent d'instituts de recherche et de sociétés privées. Les moyens technologiques et les compétences humaines indispensables à l'efficience des armes numériques vont bien sûr de pair avec l'engagement financier de ces États.

On constate aussi un renforcement notable de la doctrine face aux cybermenaces. L'International strategy for cyberspace, publiée en mai 2011 par les États-Unis, assimile les attaques informatiques contre les infrastructures vitales du pays à des «actes de guerre» qui pourraient engendrer une riposte militaire ne se limitant pas au cyberespace. Dès lors, le Pentagone reconnaît sans détour, à l'instar d'autres pays, développer des capacités offensives dans le domaine informatique.

Treize «teams» seraient, selon le Général Alexander, déjà dédiées à cet aspect et engageables sur ordre du président en réaction à une attaque, mais aussi en prévention de celle-ci. Ces capacités s'inscrivent clairement dans un cadre de dissuasion, qu'elles soient utilisées de manière exclusive ou combinées avec d'autres armes, notamment nucléaires, et qu'elles s'opposent à une cyberattaque ou une attaque plus classique.

La France, dans le livre blanc de 2013, évoque également l'emploi d'une «capacité informatique offensive» si les intérêts stratégiques nationaux sont menacés. Elle la conditionne néanmoins à une capacité de renseignement indispensable à la caractérisation de la menace et à l'identification de son origine.

En effet, toute réponse offensive à une cyberattaque est conditionnée par cette identification formelle préalable, que le ministre de la Défense appelle «l'intime conviction que permettent des faisceaux d'indices convergents». Mais l'acquisition de ces indices reste particulièrement difficile. Outre la problématique des délais de détection de l'attaque, seuls des moyens conséquents de collecte et de traitement des données

informatiques peuvent permettre d'attribuer effectivement l'acte malveillant en retraçant son cheminement et en identifiant les auteurs. Le réseau d'interception américain Echelon de la NSA paraît pour l'instant être le seul à permettre cette traçabilité de manière quasi exhaustive.

Doit-on pour autant attribuer à un état la responsabilité d'une cyberattaque lancée depuis son territoire, sans démontrer qu'il en est formellement à l'origine? Le pas pourrait rapidement être franchi en s'inspirant de précédents relevant de guerres conventionnelles, telles que l'opération Enduring freedom. Celle-ci fut en effet conduite en 2001 par les Américains, avec le soutien d'une grande partie de la communauté internationale, pour sanctionner le régime taliban, hôte des terroristes d'Al-Qaïda qui venaient de détruire les Twin Towers.

L'intervention israélienne au Liban en 2006 est encore plus significative, le gouvernement de Beyrouth se démarquant des terroristes du Hezbollah qui menaient les attaques contre Israël à partir de son territoire.

Le Vice-amiral Coustillière reconnaît la détention par la France de tels moyens offensifs, sans s'étendre sur leur nature et leur capacité. Ces armes, du ressort exclusif du ministère de la Défense et de la DGSE, relèvent en effet du secret défense. Contrairement à l'armement conventionnel, elles peuvent difficilement faire l'objet de «show of force» puisque leur principal atout est de surprendre techniquement l'ennemi. De plus, des dommages collatéraux liés à la propagation virale de l'attaque ne sont pas à exclure. Le virus STUXNET, après avoir réalisé son effet sur les centrales atomiques iraniennes, avait par exemple infecté le réseau militaire Intradef en Afghanistan.

Préparer l'avenir de façon ambitieuse

Sans angélisme ni alarmisme excessifs, la France s'est donc mise en ordre de marche pour affronter la cyberguerre qui ébranle de façon croissante les relations internationales, bien au-delà des rapports de force conventionnels. Elle ne tiendra néanmoins son rang dans ce nouvel espace de bataille qu'au prix d'une adaptation permanente et d'investissements conséquents. Il s'agira pour la défense d'améliorer sans cesse ses compétences et ses capacités spécifiques, notamment offensives, face à cette menace très évolutive. Plus largement, il s'agira pour les pouvoirs publics de sensibiliser chaque acteur national, d'optimiser la coopération interministérielle et d'impliquer la société civile et les acteurs économiques dans ses efforts, tout en préservant son indépendance industrielle dans les secteurs les plus sensibles.

Enfin, la communauté internationale, à l'exemple de la création par l'OTAN d'un centre d'excellence de cyberdéfense en Estonie ou de la coordination européenne des Computer emergency response teams (CERT)[2], doit se doter des outils législatifs et des procédures contraignantes propres à endiguer l'usage malveillant de cet espace sans

limites géographiques et technologiques. C'est à cette seule condition que l'effort individuel de chaque État pourra s'atténuer au profit d'une cyberdissuasion collective. Cela aussi, la France l'a bien compris en soutenant explicitement les initiatives internationales, notamment dans le dernier livre blanc de défense et de sécurité nationale.

[1] Le malware FLAME, décrit comme le plus puissant jamais rencontré, offrait un panel de fonctionnalités remarquable et semblait sévir depuis plusieurs années sur la toile. Outre la capacité classique d'infiltrer un ordinateur à l'insu de son utilisateur pour en prendre le contrôle, collecter des informations ou effacer des fichiers, il était en mesure de lire les courriels, mémoriser les frappes sur le clavier, réaliser des captures d'écran, enregistrer les conversations et filmer l'environnement en activant lui-même le micro de l'ordinateur ou la webcam.

[2] Différents pays européens, dont la France, ont mis en place des Computer emergency response team (CERT). Ces structures indépendantes informent les organismes qui s'y sont rattachés (administrations, centres de recherche, entreprises) sur les vulnérabilités et les moyens de s'en prémunir. L'European Government Computer Security Incident Response Team (EGC) complète ce panel en regroupant certains CERT gouvernementaux

Titulaire d'un master en droit, spécialisé dans le multimédia et les systèmes d'information, le Chef de bataillon EMPTAZ évolue depuis plus de dix ans dans le domaine de la guerre électronique. À ce titre, il a dirigé le centre d'analyse et d'exploitation du renseignement du centre de guerre électronique et mené plusieurs missions opérationnelles spécialisées. Admis à l'enseignement militaire supérieur, il est actuellement projeté au sein de l'agence européenne de défense à Bruxelles.

Titre : le Chef de bataillon Bruno EMPTAZ

Auteur(s) : le Chef de bataillon Bruno EMPTAZ

Date de parution 01/06/2018