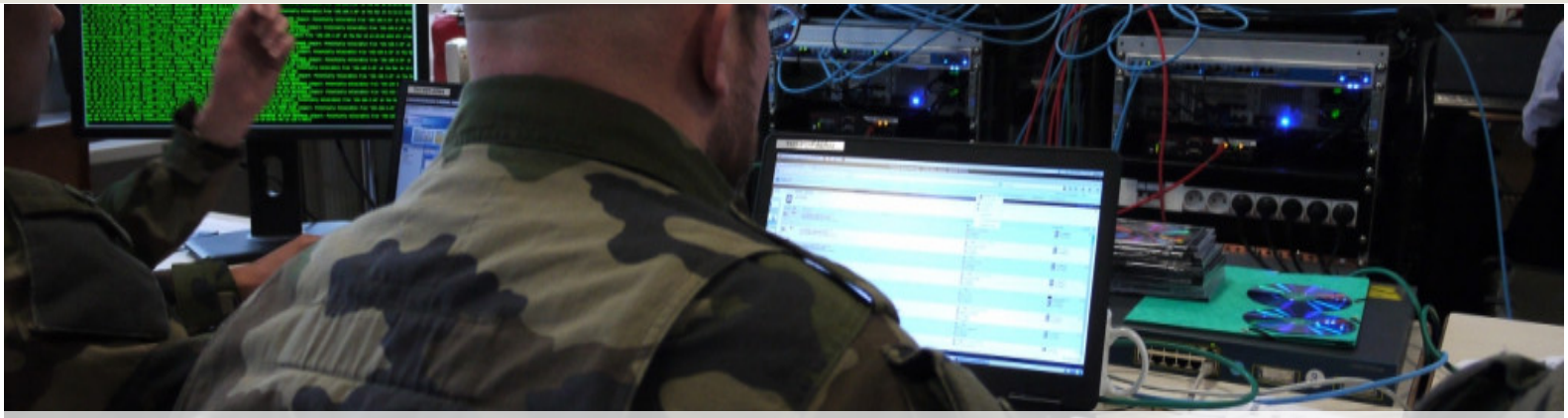

L'informatique est une arme: j'utilise mon arme

cahier de la pensée mili-Terre

le chef de bataillon Guillaume DELAVEAU

publié le 11/06/2018

Sciences & technologies

L'arme informatique est caractéristique de l'hybridation des conflits actuels, au cours desquels les mondes virtuels et physiques ne sont plus hermétiques. Cette arme peut potentiellement causer de nombreux dommages, y compris chez l'adversaire. Pratiquer la lutte informatique offensive dans les forces faciliterait grandement la diffusion de l'esprit cyber et offrirait à la France une capacité d'attaque supplémentaire, adaptée au monde actuel.

«Un beau matin les hommes découvriront avec surprise que des objets aimables et pacifiques ont acquis des propriétés offensives et meurtrières».

Qiao Liang et Wang Xiangsui, «La guerre hors limites»

L'offensive de la Russie en Géorgie en 2008 a provoqué une prise de conscience chez de nombreux stratèges et responsables politiques et militaires. L'attaque éclair classique avions/chars avait en effet été précédée de cyberattaques redoutablement efficaces.

Depuis, la France a bien pris en compte l'ampleur de la menace et a mis en place une organisation de cyberdéfense opérationnelle. Dans un contexte de restriction budgétaire, le livre blanc de 2013 préconise même de développer les capacités de cyberdéfense. En revanche, les capacités offensives de cyberguerre sont peu évoquées. Elles sont citées comme servant à caractériser la menace et comme étant une «option possible à disposition de l'État»[1].

La préférence française pour l'approche directe et l'aspect technique de l'informatique n'incite pas le commandement militaire à s'intéresser en priorité au domaine cyber.

Pourtant, l'arme informatique est caractéristique de l'hybridation des conflits actuels, au cours desquels les mondes virtuels et physiques ne sont plus hermétiques. Cette arme peut potentiellement causer de nombreux dommages, y compris chez l'adversaire. Dès lors, pourquoi ne pas s'entraîner à l'employer?

Une arme invisible et redoutable

Les attaques informatiques, ou cyberattaques, visent à entraver le fonctionnement d'un système d'information ou à voler des informations. Depuis la première, identifiée en 1988, elles se sont multipliées, complexifiées et amplifiées.

On fait historiquement débuter la «cyberguerre» en 1999, lorsque des hackers serbes ont attaqué les intranets de l'OTAN pour protester contre les bombardements. Une prise de conscience s'est réellement opérée suite à la paralysie de tous les services administratifs de l'Estonie en 2007[2]. Le conflit russo-géorgien de 2008 a achevé de donner une dimension belliqueuse aux attaques informatiques, les actions conventionnelles de l'armée russe ayant été précédées et accompagnées de nombreuses cyberattaques[3].

Écoutes, intrusions, destructions, falsifications, prises en main de systèmes: la diversité des actions de piratage informatique fait peser de lourdes menaces. Parce qu'elles n'ont pas encore causé la mort d'hommes, elles n'ont pas dans l'opinion l'impact d'actes terroristes. Pire, le hacking[4] offre un visage contrasté. Les cyberattaques sont surtout traitées en termes de criminalité. Elles dérangent les gens quand leur sphère privée est atteinte, mais elles recueillent de la sympathie lorsque le faible s'attaque au fort ou au fou, en attestent les actions des Anonymous.

Elles constituent pourtant une menace majeure et à fort impact potentiel, surtout pour un État développé comme la France. C'est le paradoxe du fort: plus on est moderne, plus on est dépendant de ses réseaux informatiques, et plus on offre de cibles à d'éventuels agresseurs.

Pour la France, la menace s'est clairement amplifiée. La multiplicité des systèmes, leur interconnexion grandissante, la complexité des architectures et l'open source rendent les vulnérabilités de plus en plus nombreuses et le travail de supervision de plus en plus difficile. Il faut ajouter au registre des menaces l'usage militaire particulier du spectre radioélectrique: liaisons radio, faisceaux hertziens, liaisons satellites. Ceci constitue un vecteur d'intrusion non négligeable. Certes, la plupart des systèmes d'information des forces armées sont cloisonnés par rapport à Internet, et lorsque Internet est utilisé, il est nominalement fourni par la DIRISI (Direction interarmées des systèmes d'information). Mais l'urgence opérationnelle ou le manque d'hygiène numérique conduisent parfois à l'adoption de comportements à risques.

Sont donc à redouter: l'infection virale (du type Conficker, qui a touché les armées[5]), l'intrusion sur un réseau, la cyberagression après capture d'un poste d'un système d'arme,

une cyberattaque utilisant le spectre radioélectrique, ou les effets d'une crise cybernétique majeure, Internet étant devenu vital[6] pour notre société.

En outre, la menace d'États cyberagressifs pratiquant la lutte informatique active (LIA) est à prendre très au sérieux. La récurrence actuelle des intrusions (appelées APT, advanced persistent threats), qui nécessitent des moyens que seuls des États peuvent fournir, laisse penser que des informations sont méthodiquement collectées pour rendre possible, dans une situation de conflit, une attaque de grande envergure. Le livre blanc de 2013 précise à ce sujet qu'en «paralysant des pans d'activité du pays, en déclenchant des catastrophes technologiques ou écologiques, une telle attaque pourrait constituer un véritable acte de guerre»[7]. La découverte du programme malveillant Stuxnet[8] en 2010, qui s'est attaqué au programme nucléaire iranien, puis celle du ver Flame en 2012, rendent bien compte de ce type d'affrontement nouveau: à des fins stratégiques, des États conduisent une véritable course à l'armement et augmentent le niveau général de la menace, devenue très professionnelle. Une menace d'autant plus forte que l'arme informatique prolifère rapidement et en quasi-totale impunité.

Le retard français se comble pas à pas

Parallèlement à l'augmentation de la menace, les pouvoirs publics ont pris conscience de l'importance de garantir et d'adapter la sécurité des systèmes d'information (SSI).

En 2008, le livre blanc sur la défense et la sécurité nationale consacre la SSI «enjeu de souveraineté nationale». Celui de 2013 va plus loin. Il reconnaît le cyberespace comme «un champ de confrontation à part entière»[9], et annonce qu'un effort significatif sera conduit pour améliorer notre défense, détecter les attaques et pouvoir «riposter de manière adéquate»[10].

- De la parole aux actes

La volonté politique ici affirmée s'est d'abord traduite par la création, en 2009, de l'ANSSI, l'agence nationale de la sécurité des systèmes d'information. De niveau gouvernemental, cette autorité unique pour la protection et la défense des systèmes d'information possède un mandat vis-à-vis des ministères, mais aussi vis-à-vis des opérateurs d'importance vitale (les OIV). Auprès d'elle, le ministère de la Défense joue un rôle primordial, notamment en cas de crise majeure[11].

Concrètement, au niveau des armées, une organisation opérationnelle est venue renforcer la chaîne fonctionnelle existante de protection des SI. Une doctrine militaire[12] a été promulguée et un cybercommandement mis en place. Pour faire face au tempo des attaques, l'unicité et la rapidité de décision d'une chaîne de commandement adossée à celle de la conduite et de préparation des opérations était nécessaire. C'est pourquoi l'officier général cyberdéfense, actuellement le Contre-amiral Coustillière, est rattaché au chef d'état-major des armées (CEMA)[13]. Il conduit la lutte informatique défensive du ministère de la Défense et des armées, et peut agir à travers le centre de planification et de conduite des opérations (CPCO) en cas de crise cybernétique majeure. Il a autorité sur

le centre d'analyse en lutte informatique défensive (CALID), véritable bras armé spécialisé de la cyberdéfense. Le CALID, qui fonctionne en permanence, effectue une veille technologique ciblée, émet et contrôle des mesures de LID (lutte informatique défensive). Il assure le pilotage de cinq groupes d'intervention rapide du ministère, les GIR[14], qui renforcent les groupes de premier niveau des différents opérateurs en cas d'attaque, et peut agir directement le cas échéant. Pour restaurer un SI infecté, un groupe de deuxième niveau, composé de 200 spécialistes, peut aussi être appelé en renfort. En plus de renforcer sa protection, la France a donc adopté une posture proactive de recherche et de détection d'attaque, ce que l'on nomme la «cyberdéfense en profondeur».

-

Les forces armées ont ensuite décliné à leur niveau la doctrine de cyberdéfense.

Au niveau des forces terrestres, une directive s'emploie ainsi à définir les fonctions, les ressources et les conditions de préparation opérationnelle pour la mise en œuvre de la cyberdéfense[15]. Pour autant, à ce jour, par manque de moyens, la chaîne cyber est un simple renfort de la chaîne fonctionnelle SSI existante, ce qui revient à donner un vernis opérationnel à la protection des SI. Quant à la préparation opérationnelle, elle est en phase d'expérimentation. L'objectif est de détenir pour 2015 des modules cyber entraînés et projetables pour contrer des cyberattaques.

Si la cyberdéfense française est au point au niveau politico-stratégique, la France détenant désormais une capacité de réaction en temps réel et une capacité de gestion de crise, elle n'est pas au point au niveau tactique.

- Des efforts marqués

Des efforts financiers et humains conséquents sont consentis pour la cyberdéfense, mais ils profitent avant tout à l'expertise et au renseignement.

200 emplois vont ainsi être créés au sein de la direction générale de l'armement, branche maîtrise de l'information (DGA/MI), afin que les domaines techniques de la cybersécurité soient parfaitement couverts. Cette entité est un expert technique de référence, notamment dans le domaine de la cryptologie. Elle veille à ce que les composants les plus sensibles des programmes d'armement restent sous maîtrise nationale et travaille au développement de solutions techniques inédites. Au niveau du renseignement, et par extension de la lutte informatique offensive[16], les services secrets français détiennent de fortes compétences. Un supercalculateur, ordinateur le plus puissant de France, fourni par la société Bull, avait d'ailleurs défrayé la chronique[17]. En termes de formation, un effort est porté sur trois domaines: le hacking éthique, la capacité à répondre aux crises, et ce que l'on nomme le «forensic», la préservation de preuves pour analyse ultérieure. Enfin, le ministère de la Défense entend mobiliser la réserve[18]. Aux côtés de la réserve citoyenne[19], la mise en place d'une réserve opérationnelle, dédiée au traitement des crises informatiques majeures, est à l'étude, ce qui apparaît pertinent dans ce monde de réseaux.

- A la recherche de synergies

À juste titre, la France recherche les synergies. La dilution des frontières et la forte dualité civilo-militaire qui caractérisent l'espace cyber imposent en effet de les renforcer.

Au niveau national, le pilotage gouvernemental et la collaboration avec l'industrie et les opérateurs d'infrastructures vitales sont effectifs. De même, la France entend maintenir une recherche académique de qualité. L'offre de formation ne répondant pas à la demande croissante d'experts, le ministère de la Défense soutient le projet de pôle d'excellence de cyberdéfense autour de Coëtquidan, avec la participation des acteurs étatiques, académiques et industriels. Au niveau international, les relations sont étroites avec l'OTAN, qui a mis l'accent sur la cyberdéfense dans son concept stratégique de 2010. La France a depuis rallié définitivement le centre informatique estonien de Tallinn, pôle de compétences otanien du domaine cyber. Au niveau européen, l'ENISA (European Network for Information Security Agency), créée en 2004, soutient utilement les États en retard, mais son efficacité est discutée car elle n'a pas de responsabilité opérationnelle et n'obéit pas à une stratégie européenne.

Si la coopération en termes de sécurité, face au banditisme par exemple, semble possible, les désaccords restent profonds, notamment au sujet de la gouvernance d'Internet, et les enjeux de souveraineté nationale prédominent.

L'accent est donc à porter avant tout sur les mécanismes de coopération public-privé à l'échelle nationale, voire européenne si les initiatives se concrétisent, pour structurer un écosystème industriel compétent, mais trop éclaté et fragile financièrement.

En conséquence, les principales recommandations du livre blanc de 2013 sont prises en compte: la collaboration est étroite avec le renseignement, la recherche amont et l'expertise sont prises en compte par la DGA et l'organisation de cyberdéfense est intégrée aux forces. Le retard de la France se comble. Il est néanmoins légitime de s'interroger sur les fameuses «capacités offensives qui doivent préparer ou accompagner les opérations militaires»[20]. Naturellement couvertes par le secret, elles devraient tout de même pouvoir être à disposition des chefs tactiques et opératifs pour leur entraînement, ou a minima leur enseignement.

Dans le cyberespace comme ailleurs, la meilleure défense, c'est l'attaque

Le livre blanc de 2013 annonce que la capacité offensive enrichit la palette des options à la disposition de l'État et qu'elle comporte différents stades, plus ou moins réversibles et plus ou moins discrets, mais toujours proportionnés. Le message des autorités est actuellement le suivant: si vous nous attaquez, vous vous exposez à une riposte graduée, potentiellement massive. Cela ressemble à une transposition de la dissuasion nucléaire dans le domaine cybernétique. Or, dans cet espace, un tel message n'est pas toujours audible. En effet, tous les coups y sont permis et la guerre asymétrique y atteint son paroxysme. La France, via ses services spécialisés, est sans nul doute capable d'exploiter des vulnérabilités, c'est-à-dire des failles inconnues du public. Nos chefs savent-ils seulement qu'ils peuvent utiliser ce mode d'action indirect préalablement à toute intervention? Sauraient-ils utiliser l'arme informatique pour accompagner leurs actions?

La question de la mise en œuvre de la LIO, lutte informatique offensive, aux niveaux tactique et opératif mérite d'être posée.

- Lever les derniers blocages

Le réalisme commande d'avancer vers les capacités offensives. Le rapport Bockel recommande d'ailleurs de «poursuivre le développement de capacités offensives au sein des armées et des services spécialisés», et s'interroge sur «la pertinence d'un discours public, voire d'une doctrine publique» sur ces capacités[21]. Pour cela, il convient d'abord de lever certains blocages, comme le blocage juridique. La mise en place d'une capacité de LIO suppose en effet l'établissement d'une doctrine et d'un cadre d'emploi compatibles avec le droit, notamment le droit international. La charte des Nations Unies, les conventions de Genève et ses protocoles additionnels, les conventions de La Haye ne mentionnent pas l'informatique. Ils ne sont pas pour autant inapplicables aux attaques informatiques, car tout texte de droit a vocation à s'appliquer à des situations futures. De même, dans le droit des conflits armés, pour une attaque informatique comme pour toute autre attaque, c'est l'effet qui sera jugé. Il conviendrait alors de veiller à l'application des principes usuels de nécessité, de proportionnalité et de discrimination[22]. Ce dernier principe serait le plus difficile à respecter, les réseaux étant pour la plupart duaux. Mais malgré quelques entraves, comme l'inviolabilité des États neutres qui soulève des problèmes avec Internet, le droit international et le droit des conflits armés peuvent s'appliquer aux attaques informatiques. Et en attendant qu'émerge un droit spécifique, certains, comme les États-Unis[23], ont pris les devants et adopté des lignes claires. Le blocage majeur serait plutôt de nature culturelle. Une armée, comme toute organisation, est un système d'hommes à quatre composantes: des matériels, des méthodes, des structures et une culture. Dans la culture militaire française, les attaques informatiques ne paraissent pas nobles. Tactiquement, tout est affaire de manœuvre, dans un cadre espace-temps que l'on peut appréhender. Même s'il peut y avoir de la ruse, le choc finira par arriver. Or, dans le cyberespace, l'ennemi avance masqué. De plus, beaucoup de militaires sont encore en phase d'appropriation, avec risque de rejet, des innovations informatiques. Comme tout domaine technique de spécialiste, l'informatique fait peur. Quant à la SSI, elle reste synonyme de contrainte et non de sûreté. Au niveau opérationnel, seule la guerre électronique est vaguement connue[24]. Il faut dire que nos engagements rustiques en Afghanistan et au Mali sont éloignés des fantasmes américains de la guerre réseau centrée et de la RMA, Revolution in military affairs. Pourtant, la défiance est dangereuse. Face à ces deux blocages, juridique et culturel, il serait dangereux de rester immobile. Rappelons que c'est en se focalisant sur la défense que nos forces armées ont subi la lourde défaite de 1940.

- De l'utilité de savoir attaquer

Pour avancer dans le domaine cyber, il faut que la fonction informatique devienne concrète et attractive. En se faisant attaquer et en apprenant soi-même à attaquer, on comprend mieux pourquoi et comment il faut se défendre.

C'est en rendant les scenarii d'attaques informatiques crédibles et en les jouant pour de

vrai que les utilisateurs apprendront à se protéger. C'est aussi en donnant aux chefs tactiques les moyens d'attaquer avec des armes informatiques aux effets concrets qu'ils auront ensuite le réflexe de se protéger et l'idée d'attaquer par ce biais. Car une attaque informatique peut avoir des effets «terrain». Un convoi de véhicule peut se faire brouiller ses GPS et se perdre, des avions peuvent se tromper de cible, un poste de commandement peut ne plus donner d'ordres ou, pire, en donner de mauvais.

L'arme informatique peut perturber les communications de l'adversaire, tromper les décideurs et nous renseigner. C'est le binôme sabotage/espionnage, version high tech, que nous offriraient des unités de cyberguerre.

- Comment faire?

Aujourd'hui, la capacité informatique offensive française concourt à la cybersécurité et est associée à la capacité de renseignement. Pour réellement enrichir la palette des options possibles à la disposition de l'État, cette capacité doit se développer dans les forces. Au préalable, il convient de bien distinguer cyberguerre, guerre de l'information et guerre électronique. La guerre de l'information consiste à altérer l'image de son adversaire, tandis que la guerre électronique consiste à attaquer, défendre et surveiller dans le spectre électromagnétique. Il n'y a bien que la cyberguerre, qui permet d'agir dans le domaine informatique ou numérique, que la France ne pratique pas complètement dans les forces.

Pour ce qui concerne nos alliés, le Pentagone a annoncé qu'il allait augmenter les effectifs cyber de 3.000, notamment pour des «opérations numériques offensives». Le ministère de la défense britannique a, lui, reconnu dès 2011 l'existence d'unités spécialisées dans la création et l'utilisation d'armes informatiques.

Les unités de cyberguerre du Pakistan, d'Iran, de la Syrie (la Syrian electronic army), de Russie ou de Chine réalisent de véritables coups médiatiques qui en disent long sur leurs capacités en cas de conflit conventionnel. L'armée populaire chinoise (APL), sans reconnaître officiellement l'existence d'unités spécialisées, a recruté des hackers après avoir payé leurs études. L'interpénétration entre le public et le privé y est très avancée[25] et les politiques de recrutement et d'emploi des unités cyber dans ces pays nous placent face au dilemme des trois M: militaire, militant ou mercenaire? Le fait de rester immobile de notre côté donne du crédit aux tenants de l'approche indirecte et de la guerre hors limites.

En France, la création d'unités de cyberguerre n'est pas envisagée ou revendiquée. Dans un contexte de déflation d'effectifs, il est peu réaliste de créer de nouvelles entités dans les forces. Au niveau tactique, il serait judicieux de commencer par mieux utiliser la guerre électronique offensive, qui est déjà dans les prérogatives de l'armée de Terre. Les unités de guerre électronique, dont les compétences sont reconnues et l'emploi maîtrisé par les chefs, pourraient être remaniées et renforcées, afin de faire du combat cyberélectronique, et en particulier du brouillage[26]. Une brigade interarmes pourrait, selon le besoin, obtenir un renfort d'unités aux compétences élargies. C'est à un niveau opératif, c'est-à-dire interarmées, que l'on pourrait retrouver des unités spécialisées, de réserve notamment. Le cyberespace étant transverse, le niveau opératif paraît le plus à même de réagir et d'agir efficacement. Il pourrait décider de mener des attaques cybernétiques élaborées préalablement à l'attaque cinétique des forces

conventionnelles. Il pourrait tout aussi bien effectuer un brouillage de masse à l'aide d'un navire côtier que se faire assister d'unités cyber dédiées agissant depuis l'OHQ, l'Operative Headquarters, son poste de commandement basé en métropole, la plupart des opérations pouvant se faire à distance. Les attaques informatiques peuvent se faire en plusieurs phases, selon les méthodes habituelles de planification et de ciblage. On peut aisément imaginer une attaque en confidentialité d'un réseau, suivie d'un décryptage des fichiers récupérés, qui permettrait de prendre le contrôle du réseau ciblé et de le rendre indisponible (attaque en disponibilité).

Des unités de cyberguerre travaillant et s'entraînant à un niveau stratégique pourraient donc descendre au niveau opératif pour réaliser de la lutte informatique offensive en opérations et, ponctuellement, appuyer le niveau tactique.

La France a fait de gros progrès dans le domaine cyber. Très performante dans le domaine technique, elle possède les moyens de renseignement adéquats, a progressé en termes de sécurité et s'est dotée d'une chaîne opérationnelle de cyberdéfense cohérente et robuste. Car la tendance est bien là, les systèmes d'information sont toujours plus performants, virtualisés et optimisés, et il devient compliqué de les maîtriser alors même que les USA et l'Asie s'imposent comme superpuissances informatiques.

Néanmoins, l'absence de prise en compte effective de la menace cyber au niveau tactique, et la timidité française concernant la lutte informatique offensive, ne permettent pas de nous hisser parmi les nations les plus en pointe du cyberespace. Nous ne prenons donc pas totalement acte de l'hybridation des conflits et nous nous privons d'une arme redoutable et essentielle à notre époque: l'arme informatique.

[1] Livre blanc de la défense et de la sécurité nationale 2013, P.105.

[2] L'attaque a été revendiquée par les nachis, un groupe nationaliste russe, en représailles au retrait du soldat de bronze de Tallinn.

[3] En plus des attaques symboliques, comme les défigurations sur les sites officiels, la Russie a mis hors d'état de fonctionnement le système informatique de l'armée géorgienne. L'aviation de la Géorgie est ainsi restée clouée au sol en début de conflit.

[4] Le terme hacking fait référence aux jeunes gens brillants qui, dans les années 50 aux États-Unis, s'emparaient d'ordinateurs alors réservés aux industriels et aux militaires.

[5] En janvier 2009, le système informatique du ministère de la Défense a été contaminé par ce virus. Par exemple, les Rafales de la Marine, n'ayant pas pu télécharger leurs paramètres de vol, sont restés cloués au sol.

[6] Terme utilisé dans le livre blanc de 2008.

[7] Livre blanc défense et sécurité nationale 2013, P.48.

[8] Stuxnet, entré en Iran par une clé USB, a infecté le logiciel SIEMENS destiné au SCADA (Supervisory Control and Data Acquisition), qui contrôle les infrastructures industrielles vitales. Si l'Inde et l'Indonésie ont aussi été touchées, c'est l'Iran qui était ciblée. Selon des spécialistes, son programme nucléaire aurait été ralenti de cinq ans grâce à la détérioration des centrifugeuses. Malgré l'absence de revendication en bonne et due forme, Stuxnet serait le fruit d'une collaboration poussée entre les États-Unis et Israël.

[9] Livre blanc défense et sécurité nationale 2013, P.45.

[10] Ibid P 135.

[11] En témoigne la colocalisation de leurs centres de surveillance respectifs, achevée en juin de cette année (COSSI, centre opérationnel de la sécurité des systèmes d'information, et CALID, centre d'analyse en lutte informatique défensive).

[12] Concept interarmées de défense, CIA-6.3 Cyberdef, du 12 juillet 2011 et doctrine interarmées, DIA-6.3 Cyberdef du 7 janvier 2012.

[13] Plus précisément, le Contre-amiral Coustillière est l'adjoint cyber du sous-chef opérations de l'EMA.

[14] À noter que l'armée de Terre dispose d'un GIR particulier, détenant une capacité de projection en opération. En langage international, on entend souvent parler des CERT, les Computer Emergency Response Teams, qui sont des centres d'alerte et de réaction aux attaques dédiés à un secteur en particulier. Les CERT se situent donc à un niveau intermédiaire entre le CALID et les GIR, et correspondent à nos CO de composantes.

[15] Le tome 1 concerne le contexte général, le tome 2, qui s'intitule «Directive de mise en œuvre de la cyberdéfense dans les forces terrestres» est actuellement en cours d'évolution suite aux premiers retours d'expérience, afin notamment de donner des directives plus précises et concrètes (fiches d'exercices par exemple).

[16] Le renseignement qui concerne la lutte informatique active est couvert par le secret Dalia.

[17] Son installation, aux Alluets-le-Roi dans les Yvelines, a nécessité de détourner une ligne électrique à haute tension pour éviter les courts-circuits dans les villages des environs. La «bécane» surpuissante fait le bonheur des jeunes ingénieurs, recrutés à la sortie des écoles pour des contrats de trois ou six ans.

[18] Discours de M. J-Y Le Drian en ouverture du colloque sur la cyberdéfense à Rennes le 3 juin 2013.

[19] Créé en 2012, le réseau cyberdéfense de la réserve citoyenne dispose d'une cinquantaine de membres actifs. Son objectif est de sensibiliser la société aux enjeux de cyberdéfense et de cyberésilience.

[20] Livre blanc défense et sécurité nationale 2013, P 94.

[21] Recommandation n°10 sur 50 du rapport du sénateur Jean-Marie Bockel, «La cyberdéfense: un enjeu mondial, une priorité nationale», 19 juillet 2012.

[22] L'article de 2002, «Wire Warfare, computer network attack and jus in bello», du professeur Michael N. Schmitt fait autorité sur le sujet. Il explique que les principes de droit humanitaire s'appliquent à partir du moment où l'attaque informatique imputée à un État «est destinée à causer des blessures, des morts, des dommages ou des destructions».

[23] La National Security Directive 16 fixe des règles d'engagements strictes et demande notamment un niveau d'approbation à très haut niveau avant toute attaque.

[24] La guerre électronique est d'ailleurs moquée pour son nom qui serait galvaudé: «il y a autant de guerre dans la guerre élec que de sport dans le sport élec».

[25] Tout le monde se connaît et s'est rencontré à l'université comme celle, réputée, de Zhejiang à Hangzhou.

[26] À ce jour, une brigade a sous ses ordres un groupe léger de guerre électronique de moins de dix personnes. Ce groupe détecte, localise et identifie les activités radioélectriques, mais il s'avère inopérant sur la téléphonie cellulaire (GSM) ou satellitaire et ne peut pas faire de brouillage.

Saint-cyrien de la promotion du «Bicentenaire de Saint Cyr» (1999-2002), le Chef de bataillon DELAVEAU est issu de l'arme des transmissions. Chef de section au 41ème RT de Senlis, il a été projeté comme conseiller SIC du REPFRANCE en Afghanistan et a participé à plusieurs exercices interalliés et interarmées de niveau opératif. Il a ensuite commandé une unité au 48ème RT d'Agen de 2008 à 2010. Affecté à Bourges dans un bureau de développement informatique, le CEDIMAT, il a réussi le concours de l'École de guerre en 2012.

Titre : le chef de bataillon Guillaume DELAVEAU

Auteur(s) : le chef de bataillon Guillaume DELAVEAU

Date de parution 23/05/2018