Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE LA DEFENSE
ET DES ANCIENS COMBATTANTS

CDEM
CENTRE de DOCUMENTATION de l'ÉCOLE MILITAIRE

Centre de documentation de l'Ecole militaire

Cyberespace & cyberdéfense

Centre de documentation de l'Ecole militaire (CDEM)
21, place Joffre
75700 PARIS SP 07
Véronique Schultz, directrice
01. 44. 42. 81. 91
www.cdem.defense.gouv.fr

Service Analyse et Production documentaires
CDEM / SAPD
François Girodineau
01. 44. 42. 45. 76.

Rédaction
François Girodineau

Réf. :
CDEM / Fiche/ n 01/ 2012

Fiche de synthèse

24 juillet 2012

Dès sa création, Internet a vu se multiplier les menaces contre ses réseaux et ses utilisateurs : virus informatiques, intrusions de *hackers*, abus de confiance, désinformation, etc. L'ampleur des cyber-attaques contre l'Estonie en 2007, ou contre la Géorgie en 2008, a contraint la communauté de défense à considérer cet espace comme un territoire de conflictualité majeure et, dès lors, à imaginer des contre-mesures permettant de protéger les infrastructures numériques sensibles, militaires ou civiles.

1. LE CYBERESPACE, NOUVEL ENJEU DE LA GEOPOLITIQUE CONTEMPORAINE

A nouveau cadre géopolitique, nouveaux rapports au pouvoir. Le Département de la défense américain définit le cyberespace comme un « *domaine caractérisé par l'usage de l'électronique et du spectre électromagnétique pour stocker, modifier et échanger des données via des systèmes en réseaux et les structures physiques qui y sont attachées* »[1]. D'autres experts décrivent le cyberespace comme « *un espace dématérialisé, déterritorialisé, modulaire, décentralisé et non hiérarchique* »[2]. Pour la France, il s'agit d'un « *espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques* »[3]. Selon Jean-Loup Samaan (DAS), ces définitions sont incomplètes, car elles ne prennent pas suffisamment en compte la question des contenus. De la même façon, les études universitaires dédiées aux technologies de l'information sont beaucoup plus nombreuses que celles consacrées aux acteurs du cyberespace, à leurs motivations et aux conséquences géopolitiques de leurs actions. Les Chinois et les Russes, qui parlent de « *terrorisme informationnel* » à propos des outils du Web 2.0[4], s'intéressent davantage, eux, à la teneur des messages et à l'exploitation des données. Mais quelle que soit l'approche privilégiée, ce nouveau cadre d'intervention, devenu, au fil du temps, « *une sphère autonome avec ses propres processus, ses propres règles et ses propres enjeux* »[5], bouscule la vision traditionnelle de la géopolitique.

Qui contrôle le cœur du cyberespace contrôle le monde. La sécurisation des routes numériques représente un enjeu géopolitique aussi important que celle des routes maritimes. Aujourd'hui, 99% des flux intercontinentaux passent par des câbles sous-marins convergeant vers des nœuds situés aux Etats-Unis, au Brésil, en Chine, au Japon, à Singapour, en Australie, en Inde, en Egypte, en France, en Espagne et au Royaume-Uni. Aucun ne se situe en Afrique, ni au Moyen-Orient, à l'exception égyptienne. La Russie n'a aucun poids sur le tracé des réseaux sous-marins, mais elle en conserve un sur les câbles terrestres reliant l'Europe à l'Asie. Pour autant, c'est bien la zone Atlantique nord (surtout les Etats-Unis) qui constitue le cœur physique du cyberespace en termes de transport, de nombre d'abonnés ou encore d'outils extra-atmosphériques de télécommunications. Le cyberespace dépend également de 13 serveurs racines DNS[6], dont 9 aux Etats-Unis (parmi lesquels 2 sous contrôle de l'armée), 2 en Europe et 1 au Japon. *Idem* pour les *data centers*, qui stockent les données qui ne sont pas, ou plus conservées par les ordinateurs des particuliers[7]. L'avance prise par la zone Atlantique nord en matière d'infrastructures inhérentes au cyberespace constitue un facteur de puissance. Elle se trouve confortée par une capacité financière pour l'instant sans équivalent dans le reste du monde.

---

[1] Définition reprise par SAMAAN, Jean-Loup. Le cyberespace, nouveau territoire de conflits ? Dans *Géographie des conflits*. Paris : Sedes, 2011. Cf. p. 151-170.

[2] TOUCHARD, Patrice. Cyberespace. Dans *Dictionnaire de géopolitique et de géoéconomie*. Paris : PUF, 2011. Cf. p. 165-169.

[3] ESTERAL CONSULTING. Etude sur la cyberdéfense et la cybersécurité au sein des institutions européennes. *DAS*, novembre 2011. Consulté le 14/03/2012. Disponible sur : http://www.defense.gouv.fr/content/download/149570/1496328/file/Cyberd%C3%A9fense%20et%20cybers%C3%A9curit%C3%A9%20au%20sein%20des%20institutions%20de%20l%5C%27UE.pdf

[4] PUJOL, Jean. La cyberguerre aura-t-elle lieu ? Dans *Stratégies dans le cyberespace*. Paris : L'esprit du livre, 2011. Cf. p. 69-79.

[5] SAMAAN, Jean-Loup. Les cyber-conflits, une révolution géopolitique ? *AFRI*, vol. XI, 11 novembre 2010, p. 985-1000.

[6] Domain Name Services.

[7] DOSSE, Stéphane. Géopolitique numérique : Tous les chemins mènent en Amérique. Dans *Stratégies dans le cyberespace*. Paris : L'esprit du livre, 2011. Cf. p. 49-58.

2. CONTRE-POUVOIRS ET RISQUES CIVILS DANS LE CYBERESPACE

La mobilisation et la contestation politique : révolutions 2.0. Outils récents, mais rapidement apprivoisés par les jeunes générations, les réseaux sociaux et le Web 2.0[8] occupent une place importante dans la mobilisation des foules, comme ce fut le cas lors des manifestations d'avril 2009 en Moldavie[9]. Ils permettent aux manifestants de relater leurs actions et d'informer leur entourage grâce à des commentaires, des images ou des vidéos diffusés par leurs smartphones ; les médias parlent à leur propos de « révolution Twitter »[10]. Deux mois après Chisinau, le même phénomène se déclenche en Iran, après le résultat des élections présidentielles, qui reconduisent Mahmoud Ahmadinejad dans ses fonctions. Fin 2010 et début 2011, la situation se reproduit pendant les « révolutions arabes », même si son impact semble avoir été moins important. Ainsi, à la faveur de ces nouvelles technologies, des citoyens aspirant à une nouvelle forme de liberté défient le pouvoir traditionnel.

La subversion : Wikileaks & les Anonymous. Le Web 2.0 peut aussi être instrumentalisé par des groupes cherchant à porter atteinte à l' « e-réputation » d'une institution ou d'un pays, ou qui agissent au nom d'une exigence de transparence et de vérité. L'affaire Wikileaks en témoigne. Grâce aux possibilités de fonctionnement collaboratif, transnational et nomade [11] offertes par cette technologie, une centaine de journalistes appartenant à des quotidiens prestigieux trient, analysent et publient en novembre 2010, dans leurs pages ou sur le site codirigé par Julian Assange, des milliers de documents émanant des troupes américaines positionnées en Irak et en Afghanistan. Quelques mois plus tard, Wikileaks met en ligne quelque 250 000 télégrammes diplomatiques transmis par le soldat américain Bradley Manning. A chaque fois, le retentissement des fuites est mondial et produit un effet boomerang sur la diplomatie américaine[12]. Selon le professeur Franck Petiteville, l'action de ces nouveaux protagonistes, dotés d'importantes compétences cognitives (les *skillful individuals*) et qui mettent à l'épreuve le secret et la raison d'Etat, bouleverse la diplomatie et conduit à une érosion de la souveraineté étatique[13]. Seul le temps révèlera l'incidence réelle de telles révélations, mais plusieurs contre-feux ont d'ores et déjà été allumés par le gouvernement américain, pour limiter à l'avenir ce genre de fuites. Une autre affaire a récemment défrayé la chronique : les représailles par déni d'accès organisées en 2010 et 2011 par le réseau *Anonymous*, pour contester les mesures judiciaires prononcées à l'encontre d'Assange[14], ou à l'encontre du site de téléchargement Megaupload en janvier 2012. S'ils ne constituent pas encore un phénomène social majeur, les *Anonymous* présentent un risque d'autant plus déstabilisant qu'ils ne sont liés à aucun Etat et n'ont pas de réelle motivation géopolitique. Quant au masque qui leur sert de symbole, inspiré par la bande dessinée *V pour vendetta*, il véhicule une forme de romantisme contestataire qui pourrait s'avérer fédérateur[15].

La cyber-piraterie & la cybercriminalité. Sur le plan technique, les observateurs du cyberespace distinguent plusieurs catégories d'outils ayant un pouvoir de nuisance avéré : les *botnets* sont des réseaux d'ordinateurs, programmés à leur insu pour agir contre une cible spécifique via des *spams*[16], un « déni de service »[17] ou des virus ; le *phishing* a pour but d'abuser de la crédulité des internautes ; les *malwares*, sortes de cheval de Troie, s'installent dans les ordinateurs en toute discrétion pour en extraire des

---

[8] On appelle Web 2.0 l'ensemble des techniques simples apparues dans les années 2000, qui permettent aux utilisateurs de s'approprier Internet en modifiant, par exemple, le contenu des pages (blogs, zones de commentaires, wikis…), ou en développant leur propre réseau social grâce à des outils comme Myspace, Facebook, Twitter, Flickr, etc.

[9] Le 6 avril 2009, le parti communiste au pouvoir, déjà critiqué par la population pour sa gestion économique, est accusé d'avoir pratiqué le bourrage d'urnes lors des élections parlementaires. Les étudiants se mobilisent en masse via, notamment, les outils du Web 2.0.

[10] SAMAAN, Jean-Loup. *AFRI, op. cit.*, p. 989.

[11] Consiste à passer d'un serveur à l'autre pour des raisons de sécurité.

[12] GOMART, Thomas ; NOCETTI, Julien. De Wikileaks à l'e-G8. Dans *Ramses 2012. L'Etat submergé*. Paris : Dunod, 2011. Cf. p. 108-111.

[13] PETITEVILLE, Franck. Wikileaks ou la subversion de la diplomatie internationale. Dans *Etat du monde 2012*. Paris : La Découverte, 2011. Cf. p. 86-97.

[14] PUJOL, Jean, *op. cit.*

[15] BAYART, Benjamin. Anonymous : ces gamins bricoleurs contre lesquels les Etats ne peuvent guère lutter. *Atlantico*, 24 janvier 2012. Consulté le 15/03/2012. Disponible sur : http://www.atlantico.fr/decryptage/anonymous-gamins-bricoleurs-etat-megaupload-hackers-attaque-cyberespace-benjamin-bayart-273658.html?page=0,2

[16] Messages envoyés de manière intempestive dans une ou plusieurs boîtes mèls, dans le but de polluer les réseaux.

[17] Action de bloquer ou de couper un ordinateur à distance.

informations sensibles, telles qu'une adresse IP, un mot de passe, etc. Ces outils sont déployés de telle sorte que l'identification des auteurs des malveillances est quasiment impossible après coup. La principale difficulté pour l'analyste consiste à déterminer si l'acte de cyber-piraterie est effectué par un ou des individus isolés, s'il est motivé par des raisons politiques et s'il s'inscrit dans une stratégie précise. D'où l'importance de distinguer la **cybercriminalité** (ou **cyber-piraterie**)[18] de **l'acquisition clandestine de données**[19] et du **cyber-conflit**[20], même si les moyens utilisés sont souvent identiques. C'est donc avant tout l'étude de la cible qui permet de comprendre la motivation du cyber-pirate ou du cyber-guerrier.

3. VERS UN NOUVEL ART DE LA GUERRE ?

Contrairement à la subversion et à la cyber-piraterie, le cyber-conflit engage les moyens d'un Etat contre un autre Etat. Le cyberespace devient dès lors un cinquième cadre de combat, après la terre, la mer, l'air et l'espace[21]. Les exemples suivants montrent qu'il s'y déroule au moins quatre types d'opérations.

Cyber-émeute[22] ou attaque punitive : Estonie 2007. Le 27 avril 2007, les sites internet du gouvernement estonien[23] sont attaqués par un flux massif de mèls destinés à bloquer les serveurs critiques. Il a été démontré, après enquête, que ceux-ci provenaient d'une cinquantaine de pays. En dépit de ses dénégations, la Russie a été suspectée d'avoir sous-traité l'attaque aux *hackers* du mouvement nationaliste estonien *Nashi*, pro-russes et mécontents du projet de démontage d'un monument à la mémoire des soldats soviétiques de la Seconde guerre mondiale, planifié par Tallin.

Cyber-attaque préventive : Géorgie 2008. En juillet 2008, Tbilissi décide de déployer des troupes en Ossétie du sud pour reprendre le contrôle de sa province séparatiste. Avant même que la Russie ne riposte en s'engageant dans le conflit, les sites internet des médias géorgiens et des infrastructures gouvernementales sensibles font l'objet d'assauts de la part de *hackers* n'hésitant pas à en bloquer les accès et en modifier les contenus. Ces agissements privent le gouvernement géorgien de la possibilité de communiquer avec sa population durant cette phase critique. Là encore, les *botnets* dispersent l'origine des actions vers une dizaine de pays, mais le Kremlin est soupçonné[24]. L'affaire géorgienne est devenue depuis un cas d'école, dans la mesure où, pour la première fois dans l'histoire de la stratégie, une offensive électronique majeure a précédé une invasion terrestre.

Cyber-espionnage : Ghosnet 2009. En mars 2009, plus d'un millier d'ordinateurs appartenant à des personnalités de haut rang (diplomates européens, représentants politiques, parmi lesquels le dalaï-lama) font l'objet d'attaques visant à espionner leurs disques durs. Après une enquête préliminaire, le gouvernement de Pékin est mis sur la sellette, les informaticiens chinois s'étant illustrés dans ce domaine dès 2005, en s'introduisant dans les serveurs du Pentagone. Si des éléments de preuve incontestables manquent encore pour incriminer la Chine, certains pays la considèrent comme un acteur potentiellement menaçant du cyberespace[25].

Cyber-sabotage : Stuxnet 2009-2010. En juin 2009, le ver informatique Stuxnet apparaît sur l'ordinateur portable d'un scientifique, soupçonné d'être lié au programme d'enrichissement d'uranium développé par la République islamique d'Iran. Particulièrement performant et furtif, le programme clandestin se propage de poste en poste jusqu'aux ordinateurs de contrôle des centrifugeuses du site de Natanz[26]. Sur place, le ver est capable de se multiplier seul, de s'installer seul et de déclencher par lui-même des séquences d'attaque déjouant les procédures habituelles de sécurité, pour fatiguer les centrifugeuses[27]. Environ un

---

[18] Cas du vol d'argent ou de la substitution d'identité.
[19] Domaine de l'intelligence et de la concurrence économiques.
[20] Dans le cadre d'une cyber-guerre, pour détruire ou affecter les capacités d'un ennemi dans le cyberespace.
[21] TOUCHARD, Patrice, *op. cit.*, p. 168.
[22] Terme repris dans TOUCHARD, Patrice, *ibid.*, p. 167.
[23] L'Estonie est l'un des Etats les plus connectés au monde. Nombre de formulaires officiels et d'archives n'existent plus que sous forme numérisée, devenant particulièrement vulnérables aux cyber-attaques.
[24] SAMAAN, Jean-Loup. *Géographie des conflits*, *op. cit.*, p. 157.
[25] SAMAAN, Jean-Loup. *Ibid.*, p. 158.
[26] ALLBRIGHT, David ; BRANNAN, Paul ; WALROND, Christina. Stuxnet Malware and Natanz : Update of ISIS December 22, 2010 Report. *ISIS*, 15 février 2011. Consulté le 05/05/2012. Disponible sur : http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf
[27] MILEVSKI, Lukas. Stuxnet and Strategy. A Special Operation in Cyberspace ? *JFQ*, n° 63, automne 2011, p. 64-69.

millier d'entre elles auraient ainsi été mises hors service. Dans cette affaire, les services de renseignement israéliens et américains, très mobilisés contre le programme iranien, figurent en haut de la liste des suspects.

Enseignements stratégiques. Malgré leur écho médiatique, il ressort de l'étude des premiers cyber-conflits que l'outil informatique n'offre pas, pour l'instant, de solution décisive sur le plan technologique. Les moyens déployés dans l'attaque par Stuxnet ont, certes, ralenti le programme nucléaire iranien, mais ils ne l'ont pas stoppé. Comme le note l'historien Patrice Touchard, les cyber-attaques « *n'ont d'intérêt que si elles ont un impact dans le monde réel ; elles sont furtives et secrètes ; la déterritorialisation du cyberespace rend très aléatoire leur confinement à un espace géographique précis* »[28]. Néanmoins, l'arme informatique intègre de manière efficace la tactique de contournement de la puissance, en ralentissant la progression d'un adversaire dans la phase préliminaire d'un conflit, phase qui se concentre désormais sur l'attaque des réseaux de communication. Comme le télégraphe de jadis, le cyberespace serait « *plus un game acceletator qu'un game changer*[29] ». Conscients de ces limites, les Etats n'en délaissent pas pour autant le volet défensif des infrastructures sensibles.

4. ORGANISATION DE LA CYBERDEFENSE

La Chine dans une position plus offensive que défensive. Le rôle du cyberespace en Chine est connu depuis la publication de *La guerre hors-limites*[30], à la suite de laquelle la réflexion en matière d'attaques cybernétiques s'est intensifiée. La cyber-défense offensive y est présentée comme « *une phase préalable de campagne militaire et une option préemptive contre les systèmes d'information de l'ennemi*[31] ». La doctrine de guerre asymétrique chinoise[32] intègre le concept de « *guerre électronique intégrée* », qui commande de prendre le contrôle des flux d'information de l'ennemi en externalisant l'attaque à des opérateurs privés, tel qu'on a pu l'observer en 2008, lors de l'offensive russe en Géorgie. La Chine est par ailleurs suspectée de développer des campagnes de cyber-espionnage et d'acquisitions clandestines de données visant, notamment, des entreprises privées ou des industries d'armement étatsuniennes[33]. Ces opérations sont conduites depuis plusieurs années par le 3ème Département de l'état-major de l'Armée populaire de libération (APL). Le programme défensif est plus récent : ce n'est qu'en mai 2011 que la Chine a mis en place une administration de cryptographie nationale, chargée de la protection des données civiles. La défense des réseaux militaires reste, elle, sous le contrôle de l'APL[34].

Mise en place du CYBERCOM aux Etats-Unis. Au lendemain de la première Guerre du golfe, les Etats-Unis engagent une réflexion sur la Révolution dans les affaires militaires (RAM). Parfois mal ressentis par *l'establishment* militaire, les débats intègrent les évolutions technologiques apparues depuis la mise en place, déjà lointaine, des réseaux ARPANET et MILnet[35], en particulier « *l'accélération du processus entre collecte du renseignement et conduite des opérations* »[36]. Le mouvement se poursuit avec la rédaction de la *National Security Presidential Directive 16*, en juillet 2002, qui prévoit la mise en œuvre de moyens offensifs par le biais informatique. En 2005, l'*US Air Force* prend le dossier cyberespace en charge, mais se heurte à l'opposition du ministre de la défense de l'époque, Robert Gates, qui ne souhaite pas laisser la responsabilité de sa mise en oeuvre à une seule arme. Finalement, conscient de la nature globale des enjeux liés au cyberespace, le Département américain de la défense crée, en mai 2010, un *Cybercommand* indépendant de toute arme, l'équivalent d'un *Combattant Command* comme le STRATCOM. Cependant, l'existence de la structure ne met pas un terme au débat entre les tenants de la cyber-guerre comme forme autonome de conflit, pouvant mener à une doctrine de cyber-dissuasion (camp des « alarmistes » et de l'*US Air Force*), et ceux qui préconisent le seul renforcement des cyber-structures

---

[28] TOUCHARD, Patrice, *op. cit.*, p. 168.
[29] SAMAAN, Jean-Loup. *Géographie des conflits*, *op. cit.*, p. 169.
[30] QIAO, Liang ; WANG, Xiangsui. *La guerre hors limites*. Paris : Payot, 2003. 310 p.
[31] SAMAAN, Jean-Loup. *AFRI*, *op. cit.*, p. 997.
[32] Sur ce sujet, voir CHEN, Zhiming. La stratégie militaire « asymétrique » de la Chine. Logique et conséquences. *Etudes internationales*, vol. XLI, n° 4, décembre 2010, p. 547-569.
[33] MASTERS, Jonathan. Confronting the Cyber Threat. *CFR*, 23 mai 2011. Consulté le 14/03/2012. Disponible sur : http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577
[34] Mme Zhang veille sur les réseaux. *Intelligence Online*, n° 637, 17 mars 2011, p. 3.
[35] Ces réseaux militaires ont permis l'éclosion de l'Internet que nous connaissons aujourd'hui. ARPANET est apparu en 1969, MILnet en 1983.
[36] SAMAAN, Jean-Loup. *AFRI*, *op. cit.*, p. 994.

sensibles[37] (camp des « réalistes » et du *Department of Homeland Security*, chargé de la protection des structures civiles sur le territoire national)[38].

Des organisations internationales peu sensibilisées à la question. Le Concept stratégique de l'OTAN faisait déjà mention du cyberespace en 1999, mais il faudra attendre l'épisode estonien pour que soit créé, en mai 2008, le *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), puis la *NATO Cyber Defense Management Authority* (CDMA). Sur le plan juridique, il n'est pas certain que l'Article 5 du Traité de l'Atlantique Nord puisse s'appliquer au cas des cyber-conflits[39]. L'Union européenne s'est, quant à elle, dotée de l'*European Network and Information Security Agency* (ENISA), sans avoir encore engagé de véritable réflexion politique sur la question. Les Nations unies n'ont pas davantage mis en place de structure dédiée au cyberespace, sans doute liées par la définition stricte que leur Charte donne des actes de guerre[40]. Hamadoun Touré, Secrétaire général de l'Union internationale des télécommunications (UIT), agence de l'ONU, a toutefois fait quelques déclarations défendant le principe d'un traité international relatif au cyberespace[41]. Le premier e-G8, qui s'est tenu à Paris en mai 2011, a posé la question du problème de la représentativité d'une éventuelle gouvernance du cyberespace[42].

Une gestion du dossier encore hésitante en France. En 2008, le Livre blanc sur la défense et la sécurité nationale précise que « *l'efficacité à tous niveaux des forces de défense et de sécurité dépendra de plus en plus du bon fonctionnement de leurs systèmes d'information. La planification et l'exécution d'opérations combinées avec des actions cybernétiques tendent en effet à devenir la norme. (…) Dans le domaine informatique plus que dans tout autre milieu, il faudra, pour se défendre, savoir attaquer*[43]. » L'Agence nationale de sécurité des systèmes d'information (ANSSI, rattachée au SGDSN) est créée en 2009, pour répondre aux menaces émanant du cyberespace, mais elle n'est pas la seule à gérer le dossier : le ministère de l'Intérieur s'occupe des cas relevant de la cybercriminalité, et celui de la Défense des réseaux militaires. L'ANSSI devrait, à terme, assurer un rôle de centralisation entre ces différents acteurs. Il est à noter qu'à l'exception de quelques paragraphes du Livre blanc, aucune doctrine officielle n'organise actuellement la cyber-défense à un niveau stratégique. Quoi qu'il en soit, le moment politique semble plutôt favorable à l'adoption d'une position mesurée, concentrée sur la défense des infrastructures existantes[44].

Contre-mesures : une question d'adaptation. Comme le rappelle Jonathan Masters, du *Council on Foreign Relations*, « *l'avantage est à l'offensive dans le royaume digital* »[45], étant donné la rapidité exponentielle du développement des technologies informatiques. Ce facteur vitesse exige, de la part des structures gouvernementales assignées à la défense des infrastructures sensibles, une capacité d'adaptation qui dépend elle-même, en partie, de l'adaptabilité bureaucratique des ministères régaliens. Un problème certain, quand on sait qu'en France, par exemple, la livraison de nouveaux équipements, du type char Leclerc, hélicoptère Tigre ou avion de chasse Rafale, peut intervenir de vingt à trente ans après la passation de la commande par l'Etat[46].

****

Nouveau territoire de conflictualité, le cyberespace est donc, potentiellement, le lieu de production de nouvelles inégalités de puissance entre les pays qui détiennent les technologies et développent déjà des stratégies d'attaque et de défense efficaces, ceux qui affectent à la cyber-défense des moyens limités, pour l'instant peu adaptés, comme l'Inde où le sujet fait débat[47], et ceux qui sont largement dépourvus d'infrastructures numériques adéquates, comme le continent africain.

---

[37] Une dizaine de secteurs sont concernés, parmi lesquels les industries de défense, les systèmes financiers, les infrastructures de transport et d'eau potable.
[38] SAMAAN, Jean-Loup. *Géographie des conflits*, *op. cit.*, p. 161.
[39] SAMAAN, Jean-Loup. *Ibid.*, p. 157.
[40] SAMAAN, Jean-Loup. *AFRI*, *op. cit.*, p. 928.
[41] PUJOL, Jean, *op. cit.*
[42] GOMART, Thomas ; NOCETTI, Julien. De Wikileaks à l'e-G8. Dans *Ramses 2012. L'Etat submergé*. Paris : Dunod, 2011. Cf. p. 108-111.
[43] *Défense et sécurité nationale : Le Livre blanc*. Paris : Odile Jacob, 2008. Cf. p. 207.
[44] SAMAAN, Jean-Loup. *Géographie des conflits*, *op. cit.*, p. 164.
[45] MASTERS, Jonathan, *op. cit.*
[46] SAMAAN, Jean-Loup. *AFRI*, *op. cit.*, p. 988.
[47] MCKNIGHT, Ulrik. India Hacked, Part III : Building Shadow Armies. *The India Site*, octobre 2011. Consulté le 30/05/2012. Disponible sur : http://www.theindiasite.com/india-hacked-part-iii-building-shadow-armies/

POUR ALLER PLUS LOIN

(rapport)
BOCKEL, Jean-Marie. La cyberdéfense : un enjeu mondial, une priorité nationale. *Sénat*, 18 juillet 2012, Rapport d'information n° 681. 158 p. Consulté le 23/07/2012. Disponible sur : http://www.senat.fr/notice-rapport/2011/r11-681-notice.html

(ouvrage)
BETZ, David J. ; STEVENS, Tim. *Cyberspace and the State : Toward a Strategy for Cyber-power*. Londres : IISS, 2011. 158 p.
Disponible au CDEM : cote COL13/424

(ouvrage)
VENTRE, Daniel. *Cyberattaque et cyberdéfense*. Paris : Hermès science publications, 2011. 312 p.
Disponible au CDEM : cote 364.168 VEN

(rapport)
Défense et sécurité des systèmes d'information. Stratégie de la France. *ANSSI*, 15 février 2011. 24 p. Consulté le 13/02/2012. Disponible sur :
http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/une-autorite-nationale-et-une-strategie-pour-defendre-et-proteger-la-france.html

(dossier)
Operational Cyber. *JFQ*, n° 61, automne 2011, p. 8-31.
Disponible au CDEM : cote P3803/61

(dossier)
Géopolitique de l'information. Economie, technologie, stratégie. *Diplomatie / Les grands dossiers*, n° 2, avril-mai 2011. 97 p.
Disponible au CDEM : cote PER140/2

(ouvrage)
KARATZOGIANNI, Athina (dir.). *Cyber Conflict and Global Politics*. Oxon : Routledge, 2009. 246 p.
Disponible au CDEM : cote 303.375 KAR

(dossier)
La criminalité numérique. *Cahiers de la sécurité*, n° 6, octobre-décembre 2008, p. 9-172.
Disponible au CDEM : cote PER18/6

QUELQUES SITES INTERNET

Agence nationale de la sécurité des systèmes d'information – ANSSI (FR)
Atlantic Council (US)
Center for Democracy and Technology - CDT (US)
Center for Strategic and International Studies – CSIS (US)
CIDRIS - Cyberwarfare (FR)
Council on Foreign Relations - CFR (US)
Chatham House (GB)
Cyber-securité.fr (FR)
Defense Tech - Cyber Security Center (US)
EastWest Institute (US)
European Commission Digital Agenda for Europe (UE)
Institut de relations internationales et stratégiques - IRIS (FR)