National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

ÉTATS-UNIS ET LES OPÉRATIONS D'INFORMATION DE LA CHINE

Maj S. Roussel

JCSP 41

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 41

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 41 – PCEMI 41
2014 – 2015

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

ÉTATS-UNIS ET LES OPÉRATIONS D'INFORMATION DE LA CHINE

Maj S. Roussel

Word Count: 5520

Compte de mots : 5520

«L'art suprême de la guerre, c'est soumettre l'ennemi sans combattre. »

Sun Tzu, *L'Art de la Guerre*[1]

INTRODUCTION

La Chine s'affirme de plus en plus en Asie, mais aussi sur la scène mondiale[2]. Elle comble de plus en plus de rôles en matière de sécurité[3] et elle a une diplomatie très active[4]. Elle est malgré tout de plus en plus perçue comme une menace au sein de sa région quant à sa manière de régler les différents conflits territoriaux[5] ce qui a sans doute contribué au repositionnement des forces américaines dans le Pacifique[6]. Ce qui dérange encore plus ses voisins et les Américains, c'est surtout les capacités militaires qu'elle met en place[7]. Avec la plus grande armée de la planète[8] et un budget estimé de $145,5

[1] « Citation de Sun Tzu », *Babelio* (mai 2014), consulté le 20 avril, 2015, http://www.babelio.com/auteur/Sun-Tzu/3396/citations?pageN=3.

[2] Le Hong Hiep, "China's new wave of assertiveness in the South China Sea", *The Strategist* (May 2014), consulté le 9 décembre 2014, http://www.aspistrategist.org.au/chinas-new-wave-of-assertiveness-in-the-south-china-sea/.

[3]. Thomas Chrsitensen, « The Advantages of An Assertive China", *Council on Foreign Relations* (April 2011), consulté le 11 décembre 2014, http://www.cfr.org/china/advantages-assertive-china/p24202.

[4] Stephanie Ho, "Chinese Foreign Relations to Focus on More Active Diplomacy", *Voice of America (*Mars 2011), consulté le 18 avril 2015, http://www.voanews.com/content/chinese-foreign-relations-to-focus-on-more-active-diplomacy-117511453/136106.html.

[5] Associated Press, "China building airstrip on reclaimed island in disputed South China Sea: report", *CTV News* (17 avril 2015), consulté le 18 avril 2014, http://www.ctvnews.ca/world/china-building-airstrip-on-reclaimed-island-in-disputed-south-china-sea-report-1.2333295.

[6] Kurt Campbell and Brian Andrews, "Explaining the US 'Pivot' to Asia", *Chatam House* (August 2013), consulté le 9 décembre 2014, http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Americas/0813pp_pivottoasia.pdf.

[7] Suisheng Zhao, "Chinese Foreign Policy as a Rising Power to Fin dits Rightful Place", *Perceptions*, volume 18, no 1 (printemps 2013), consulté le 17 novembre 2014, http://sam.gov.tr/chinese-foreign-policy-as-a-rising-power-to-find-its-rightful-place/.

[8] "China Quick Facts", *Special Warfare: The Professional Bulletin Of The John F. Kennedy Special Warfare Center & School* , (July – Sept 2012), consulté le 18 avril 2015, http://eds.b.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=6fb3084d-432f-42ba-987b-7503c2ca381a%40sessionmgr113&vid=0&hid=114.

milliards US pour la défense en 2015[9], il ne fait aucun doute que la Chine est un joueur important dans sa région, mais aussi au niveau mondial.

Malgré son armée et les ressources financières dont elle dispose[10], la Chine croit toujours qu'elle accuse un retard technologique par rapport aux États-Unis[11] . Ce retard, la Chine tente de le combler par divers moyens, mais celui qui retient le plus l'attention est le fait qu'elle n'hésite pas à voler les percées technologiques des autres pays – les États-Unis semblent être la cible de choix[12] sans toutefois s'y limiter. Même les Russes ont gouté à sa médecine[13]. Malgré tout, cette approche n'est pas assez rapide. La Chine est toujours dans une position d'infériorité par rapport à la puissance militaire des États-Unis[14]. Conscient de ce désavantage, les stratèges chinois croient pouvoir combler cette lacune en appliquant les notions de Sun Tzu ayant trait au contournement et les opérations d'information[15].

C'est en fait la thèse de ce papier qui veut que la Chine voie dans les opérations d'information un moyen de contrer la menace américaine sans nécessairement devoir

---

[9] "China Defence & Security Report*", Business Monitor International* (December 2014), consulté le 18 avril 2015, http://eds.b.ebscohost.com/ehost/detail/detail?vid=5&sid=d9dbc9a4-f90a-4055-824f-5602c1a44abe%40sessionmgr115&hid=114&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=bth&AN=100119658.

[10] Tim Worstall, "China's Now The World Number One Economy And It Doesn't Matter A Darn", *Forbes* (Juillet 2014), consulté le 18 avril 2015, http://www.forbes.com/sites/timworstall/2014/12/07/chinas-now-the-world-number-one-economy-and-it-doesnt-matter-a-darn/.

[11] "China's Cyber Warfare." *Chinascope* no. 54 (November 2011): 6-16. Academic Search Complete, EBSCOhost (accessed April 18, 2015).

[12] Jose Pagliery, "Ex-NSA director: China has hacked 'every major corporation' in U.S.", *CNN* (March 2015), consulté le 18 avril 2015, http://money.cnn.com/2015/03/13/technology/security/chinese-hack-us/.

[13] Loro Horta**,** "China steals a march on Russian arms", *Asia Times* (Décembre 2013), consulté le 18 avril 2015, http://www.atimes.com/atimes/China/CHIN-02-131213.html.

[14] "China will not match US military power – general", *BBC News* (Mai 2011), consulté le 18 avril 2015, http://www.bbc.com/news/world-asia-pacific-13450316.

[15] Vincent Wei-cheng and Gwendolyn Stamper, "Asymetric war? Implication for China's Information warfare Strategies." *American Asian Review* 20, no. 4: 167. *Academic Search Complete*, EBSCO*host* (accessed April 18, 2015).

rivaliser avec les moyens techniques et militaires américains. L'exploitation des opérations d'information au sein d'une stratégie de contournement dans un contexte de People's war est pour la Chine une solution asymétrique à la menace américaine. Bref, la Chine développe ses capacités militaires en matière d'opération d'information et raffine de plus en plus sa stratégie afin d'inclure la participation du peuple chinois[16].

Comme la Chine n'est pas un modèle de société ouverte sur le monde, il n'est donc pas possible de consulter ses manuels de doctrine. La démarche utilisée pour démontrer notre thèse s'est donc articulée autour de recherches produites par différents acteurs et observateurs provenant tant des écoles militaires que des analystes de la scène mondiale des affaires militaires. Cette approche sera supportée par la doctrine canadienne afin d'établir les définitions requises et d'expliquer brièvement la portée des opérations d'information.

C'est dans ce contexte que la première partie de ce papier sera consacrée aux différentes définitions et à la mise en place du cadre des opérations d'information. Par la suite, la deuxième partie propose d'explorer l'évolution de la compréhension chinoise des opérations d'information tout en précisant le rôle de l'armée, en particulier comment elle perçoit les opérations d'information et la guerre de l'information. En troisième lieu, il sera question de faire un survol des capacités Chinoises en se limitant à la guerre cybernétique, le cyber espionnage et à la propagande. C'est finalement dans la dernière partie que l'on fera l'analyse de l'évidence afin de confirmer la thèse. Pour y arriver, il

[16] Daniel Ventre, « China's Strategy for Information Warfare : A Focus on Energy", Journal of Energy Security (May 2010), consulté le 18 avril 2015, http://ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361.

faudra revenir sur les différents aspects de sa stratégie et les exemples présentés en termes de capacités. Comme toile de fond de cette rubrique, deux réalités s'opposent. Dans un premier temps, la peur des Américains de revivre un autre Pearl Harbor et la position chinoise qui se perçoit toujours comme étant inférieure.

PARTIE 1 – DÉFINITIONS

Afin de bien comprendre les opérations d'information, il est essentiel de revoir quelques termes, car plusieurs définitions circulent. Cette section sera donc basée sur les définitions provenant de la doctrine canadienne. L'intention sera de définir ce qu'est l'information, les opérations d'information, la guerre de l'information et finalement définir le cadre des opérations d'information. Encore une fois, l'intention ici n'est pas de revoir toutes les notions associées aux opérations d'information, mais bien de fournir une base de connaissance commune qui facilitera la lecture de ce papier.

Information

Selon la doctrine canadienne, « l'information est définie comme ce qui informe ou a le potentiel d'informer. L'information est une combinaison du contenu et de la signification communiquée ou reçue[17] ». Elle est « représentée par des symboles et les médias ou un conduit, utilisé ou utilisable dans un contexte particulier[18] ». Finalement, il est important de noter que « la même information peut avoir plusieurs significations et être interprétées différemment par différents destinataires[19] ». Interprété de façon plus large, « un système d'information est l'ensemble d'équipement, de méthodes et de

[17] Ministère de la défense nationale, B-GG-005-004/AF-010, *Opérations d'information des FC*, (Ottawa : MDN Canada, 1998), p. 1-6.
[18] *Ibid*., p. 1-6.
[19] *Ibid*., p. 1-6.

procédures et si nécessaire de personnel, organisé pour accomplir des fonctions de traitement d'information spécifique[20] ».

Opérations d'information

Selon la doctrine canadienne, « les opérations d'information signifient des actions prises en soutien des objectifs nationaux influençant les décideurs en influant sur l'information d'un autre en exploitant et protégeant ses propres informations[21] ». De plus, « les opérations d'information demandent l'intégration étroite des capacités offensives et défensives des activités ainsi qu'une conception efficace, l'intégration et l'interaction du C2 avec le soutien d'information[22] ». Le point critique en matière d'opération d'information est que « la pleine valeur des opérations d'information peut seulement être atteinte au moyen de l'intégration efficace de plusieurs disciplines[23] ».

La prochaine figure est une représentation de l'intégration des différentes disciplines incluses dans les opérations d'information. Elle est présentée ici par souci de clarté, mais surtout parce que toutes ces disciplines ne feront pas l'objet du présent document. Ceci dit, il est malgré tout important de comprendre l'étendue des opérations d'information afin de mieux comprendre le cadre dans lequel elles sont conduites.

[20] *Ibid*., p. 1-7.
[21] *Ibid*., p. 1-7.
[22] *Ibid*., p. 1-7.
[23] *Ibid*., p. 1-7.

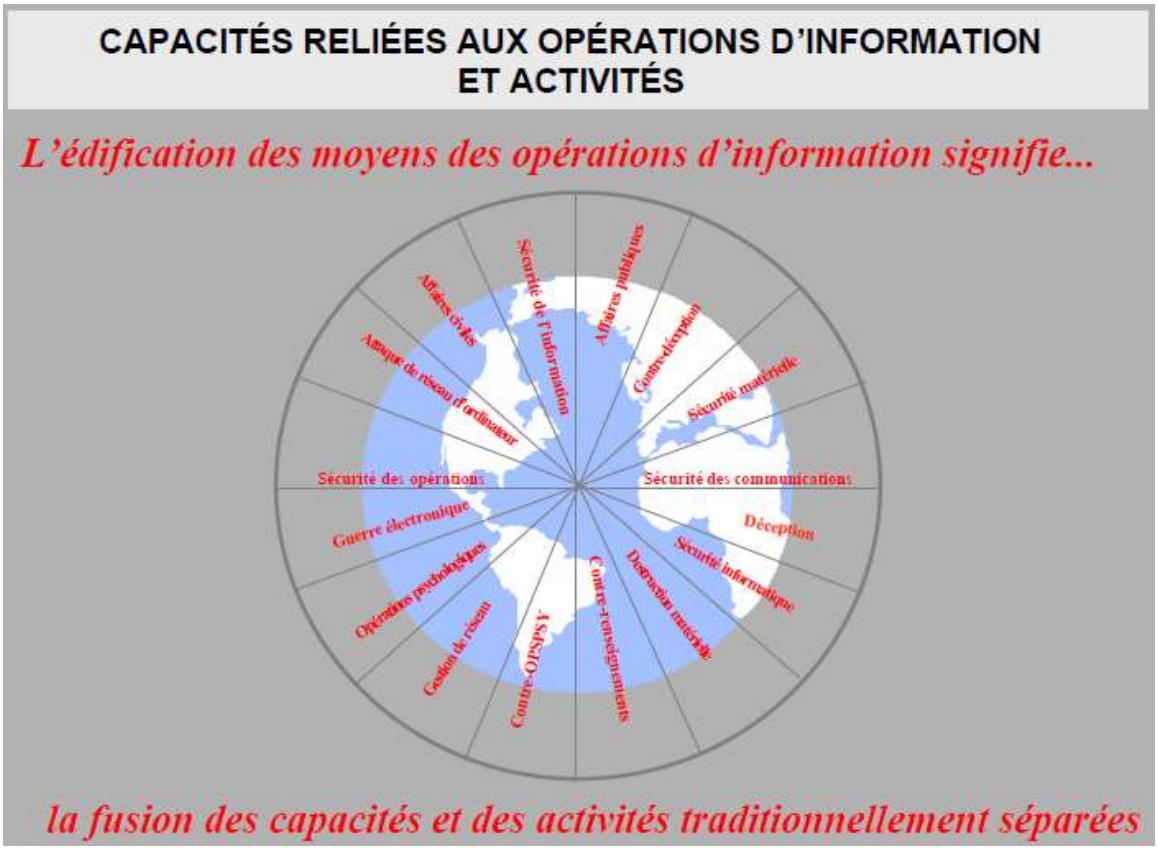

Figure 1 – Capacités reliée aux opérations d'information

Source : Ministère de la défense nationale, B-GG-005-004/AF-010, *Opérations d'information des FC*, (Ottawa : MDN Canada, 1998), p. 1-8.

Il est nécessaire de revenir sur deux concepts présentés plus haut, soit les opérations d'information offensive et défensive. Dans un premier temps, les « opérations d'information offensives incluent des actions prises pour influencer des décideurs adversaires actuels ou potentiels[24] ». Les actions offensives ont pour but d'affecter « l'utilisation ou l'accès à l'information et des systèmes d'information d'adversaires ou d'adversaires potentiels[25] ». Les moyens utilisés « peuvent comprendre l'utilisation des

[24] *Ibid*., p. 1-8.
[25] *Ibid*., p. 1-8.

OPSPSY, la déception, la GE, le renseignement, l'attaque de réseau informatique, la destruction matérielle et des opérations d'information spéciales (SIO)[26] ».

Pour les opérations défensives, elles « incluent des actions prises pour protéger ses propres informations et assurer que les décideurs amis ont un accès opportun à des informations nécessaires, pertinentes et précises[27] ». Comme son nom l'indique, le but est aussi de protéger contre « tout effort des opérations offensives[28] » provenant de l'adversaire. Ultimement, les « opérations d'information défensives s'efforcent de s'assurer que le processus de décision ami est protégé de tous les effets nuisibles, délibérés, par inadvertance ou accidentels[29] ». Il faut donc voir les opérations d'information défensives comme étant « un processus intégrant et coordonnant les politiques, les procédures, les opérations, le renseignement, le droit et la technologie[30] ».

Guerre de l'information

Définir la « guerre de l'information » ou le « information warfare » à l'aide de la doctrine canadienne est difficile, car ces termes ne sont pas mentionnés dans la doctrine. Elle utilise le terme « supériorité de l'information[31] » que l'on peut interpréter comme étant la finalité de la guerre de l'information. Par extension, il est possible de conclure que la guerre de l'information « est la capacité d'acquérir, d'exploiter et de diffuser une circulation interrompue d'information en niant la capacité à l'ennemi de faire la même

[26] *Ibid*., p. 1-8.
[27] *Ibid*., p. 1-8.
[28] *Ibid*., p. 1-8.
[29] *Ibid*., p. 1-8.
[30] *Ibid*., p. 1-8.
[31] *Ibid*., p. 1-8.

chose[32] ». Cette déduction logique est aussi supportée par le texte d'Anderson, qui voit la guerre de l'information comme étant « the capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same[33] ».

Curieusement, même au sein du « Joint Publication 3-13, Information Operation » de la doctrine américaine, le terme de « information warfare » n'est pas utilisé[34] et encore moins défini. Et pourtant, en faisant un survol de la littérature disponible pour préparer ce papier, le terme « information warfare » est utilisé par plusieurs auteurs. Encore plus important, c'est les États-Unis qui ont contribués à le populariser. En fait, c'est le Pentagone qui l'a rendu si populaire si l'on se réfère au texte d'Anderson cité plus tôt. En effet, l'auteur mentionne « the Pentagon's embrace of information warfare as a slogan in the last years of the twentieth century established its importance —even if its concepts, theory and doctrine are still underdeveloped[35] ».

Cadre des opérations d'information

La meilleure façon de présenter le contexte est d'utiliser certaines figures présentées dans le manuel des Opérations terrestres de la doctrine canadienne[36]. Dans un premier temps, il faut expliquer que la conduite des opérations d'information s'articule selon trois thèmes. Premièrement, « les activités d'influence (AI), sont le principal moyen

---

[32] *Ibid*., p. 1-8.

[33] Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, (Indianapolis: John Wiley & Sons, 2010), p. 588

[34] Department of Defense, *Joint Publication 3-13 : Information Operations* (Washington, D.C. Government Printing Office, November 2014), consulté le 21 avril 2015,

[35] Ross J. Anderson, *Security Engineering*, p. 559.

[36] Ministère de la défense nationale, B-GL-300-001/FP-002, *Opérations terrestres*, (Ottawa : MDN Canada, 2008).

d'influer sur la volonté[37] ». En second lieu, il est question des « activités de contrecommandement (ACC), qui attaquent la capacité liée à l'information et au commandement[38] ». Finalement, « les activités de protection de l'information (API), qui protègent l'information amie, amoindrissant ainsi la compréhension qu'a l'adversaire de la situation[39] ». Le contexte est donc tout simplement toutes les activités conduites dans l'ensemble du spectre des opérations dont le but ultime est de « modifier l'information, la capacité, les perceptions, la volonté et, ultimement, le comportement[40] ».

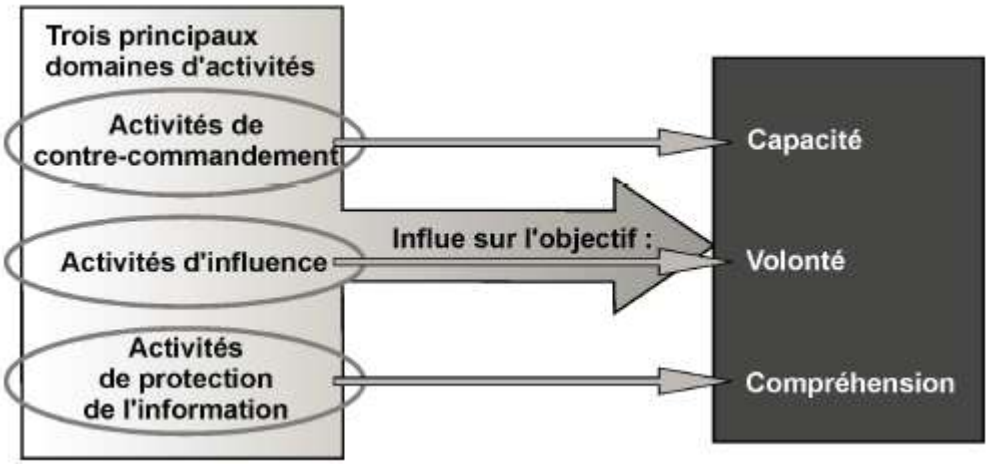

Figure 2 : Les trois principaux domaines d'activités des opérations d'information

Source : Ministère de la Défense nationale, B-GL-300-001/FP-002, *Opérations terrestres* (Ottawa : MDN Canada, 2008), p. 5-48.

Concrètement, les activités d'opération d'information sont conduites dans l'ensemble de l'espace de combat et sur l'ensemble du spectre d'intensité. Les actions doivent être conduites dans le but d' « influer sur la volonté, pour amoindrir la compréhension ou pour affecter la capacité de commandement, contrôle, communication,

[37] *Ibid*., p. 5-47.
[38] *Ibid*., p. 5-47.
[39] *Ibid*., p. 5-47.
[40] *Ibid*., p. 5-46.

informatique, renseignement, surveillance et reconnaissance (C4ISR) d'un décideur[41] ». La figure suivante illustre parfaitement ce paradigme.

Figure 3 : Éléments constitutifs des activités d'influence et des feux

Source : Ministère de la Défense nationale, B-GL-300-001/FP-002, *Opérations terrestres* (Ottawa : MDN Canada, 2008), p. 5-58.

C'est ainsi que se termine la section traitant des définitions et concepts clés des opérations d'information. Principalement à l'aide de la doctrine canadienne, l'information, les opérations offensives et défensives ainsi que le cadre ou le contexte de la conduite des opérations d'information ont été présentés. Même si le terme guerre de l'information est très rependu dans la littérature, il ne fait aucunement partie de la doctrine canadienne et américaine[42]. Une définition a toutefois été proposée en

[41] *Ibid*., p. 5-49.

[42] Même si le terme « information warfare » n'est pas dans le Joint Doctrine américaine, il est important de noter ici que la Marine américaine utilise les termes « information in warfare » et « information as warfare » dans un contexte de supériorité de l'information. Consulté la référence « The US Navy's Vision for Information Dominance », May 2010, consulté le 4 mai 2015, http://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxpZGNzeW5jfGd4OjM0NDU5MzEzZjEyZDIwZTQ. Une liste de référence de la Marine américaine plus exhaustive est aussi disponible, http://www.idcsync.org/documents. Finalement, les manuels de doctrines américains utilisent le

extrapolant la notion de supériorité de l'information. Ayant terminé la mise en place des concepts de base, la prochaine étape sera donc consacrée à l'évolution de la compréhension chinoise des opérations d'information tout en précisant le rôle de l'armée.

PARTIE 2 – HISTORIQUE ET STRATÉGIE

La prochaine partie de ce papier fera un survol de l'évolution de la compréhension chinoise des opérations d'information et de sa stratégie. Pour se faire, il faut revoir comment les Chinois ont perçu la Guerre du Golfe de 1991 et comment ils ont développé leur doctrine suite à cette analyse pour finalement adopter une approche de People's war. Mais dans un premier temps, afin de bien comprendre ce que représentent les opérations d'information et la guerre de l'information, il est nécessaire de revenir brièvement sur la dernière révolution dans les affaires militaires.

Révolution dans les affaires militaires

Rendue possible par les développements technologiques dans les années 1990[43], « IW is an integral aspect of a larger phenomenon that is generally known as the revolution in Military Affairs[44] ». En effet, la guerre de l'information représente « a major change in the nature of warfare brought about by advances in military technology

---

terme « electronic warfare » comme une composante des opérations d'information. C'est essentiellement cette composante qui est ciblée lorsqu'il est question de « information warfare ».

[43] Micheal J. Thompson, " Military Revolutions and Revolutions in Military Affairs: Accurate Descriptions of Change or Intellectual Constructs?", *Strata* (Septembre 2011), consulté le 23 avril 2015, http://artsites.uottawa.ca/strata/doc/strata3_082-108.pdf.

[44] Wei-cheng, Vincent, and Gwendolyn Stamper. "Asymetric war? Implication for China's Information warfare strategies." *American Asian Review* 20, no. 4 (Winter 2002). Academic Search Complete, EBSCOhost (accessed April 23, 2015), p. 177.

which, combined with dramatic changes in military doctrine and organizational concepts, fundamentally alter the character and conduct of military operations[45]».

C'est donc dans ce contexte de révolution que l'armée chinoise a entrepris de se moderniser et cette modernisation fait couler beaucoup d'encre encore aujourd'hui[46]. Pas plus tard que l'été dernier, le président Xi Jinping a mentionné que « China will spur military innovation and called on the army to create a new strategy for "information warfare" as the country embarks on military reform [47]». Il suffit de faire une recherche rapide sur l'internet pour constater que la révolution chinoise en matière d'opérations d'information ou de guerre de l'information suscite beaucoup d'intérêt et d'écrits[48].

Comme il a été mentionné plus haut, il ne fait aucun doute que la Chine met en place des capacités militaires impressionnantes. Mais l'observation faite par Xi Jinping fait référence à beaucoup plus qu'aux moyens militaires traditionnels. En effet, ici il est question de mettre en place les conditions requises pour être en mesure de rivaliser avec les différentes puissances étrangères qui ont déjà entrepris ce virage technologique. Pour les Chinois, c'est en analysant la Guerre du Golfe de 1991 et en incorporant les concepts de la doctrine américaine que ce changement a débuté.

---

[45] Elinor Sloan, "Canada and the Revolution in Military Affairs: Current Response and Future Opportunities," *Canadian Military Journal* 1, 3 (2000), p. 7, consulté le 23 avril 2015, http://www.journal.dnd.ca/vo1/no3/doc/7-14-eng.pdf.

[46] Andy Sharp, "Xi Urges China Military Strategy for Information Warfare", *Bloomberg Business* (Août 2014), consulté le 23 avril 2015, http://www.bloomberg.com/news/articles/2014-08-31/xi-urges-new-china-military-strategy-for-information-warfare-.

[47] Sui-Lee Wee, "China's Xi urges army to create strategy for information warfare", *Reuters* (Août 2014), consulté le 23 avril 2015, http://www.reuters.com/article/2014/08/30/us-china-xi-defence-idUSKBN0GU0H020140830.

[48] Une simple recherché qui nous a permis de trouver la référence précédente a générée plus de 253 000 documents ou page web.

Guerre du Golfe

La Guerre du Golfe a changé bien des visions en ce qui concerne la conduite de la guerre peut-être plus encore pour l'armée chinoise. « The Revolution in Military Affairs (RMA) became a common term in military and defence circles in the early 1990s when the Gulf War seemed to indicate a dramatic shift in the nature of modern warfare[49]». Pour les stratèges chinois, cela marque le début d'un changement important de posture. « Strategist began to shift away from planning for a war with the Soviet Union, and began gradually to think about ways to modernize their armed forces and incorporate new technologies and fighting doctrine[50]».

Ce qui marqua l'imaginaire des stratèges chinois est surtout la défaite rapide des Irakiens. « The rapid defeat of Iraqi forces during the 1991 Gulf War served as a shock to Chinese planners[51] ». Le choc était encore plus important, car « not only was some of the military equipment the Iraqis operated purchased from China, but the scope of the defeat seemed to catch the Chinese planners somewhat off guard[52] ». Bref, la rapidité, l'ampleur de la défaite et la piètre performance du matériel chinois au sein de l'armée irakienne ont définitivement causé un état de panique.

---

[49] Micheal J. Thompson, " Military Revolutions and Revolutions in Military Affairs: Accurate Descriptions of Change or Intellectual Constructs?", *Strata* (Septembre 2011), consulté le 23 avril 2015, http://artsites.uottawa.ca/strata/doc/strata3_082-108.pdf.

[50] James R. Holmes, "Anti Access History Lessons", *The Diplomat* (Mai 2012), consulté le 23 avril 2015, http://thediplomat.com/2012/05/an-anti-access-history-lesson/.

[51] *Ibid*.

[52] *Ibid*.

Guerre de l'information

Empruntant plusieurs concepts des Américains[53], la doctrine chinoise décrit la guerre de l'information comme un processus dont le but est de «seeks to disrupt the enemy's decision-making process by interfering with the adversary's ability to obtain, process, transmit, and use information[54]». Dans la perception chinoise de la conduite des opérations d'information, la guerre de l'information « is a non-conventional weapon designed to impede an adversary's decision-making with the aim of delaying or even deterring conflict[55]». Dans l'état actuel de sa doctrine, si l'utilisation de la force « is unavoidable, the Chinese would use IW to shape the battlespace in a manner that increases their chances of victory[56]».

L'armée chinoise prévoit conduire sa guerre de l'information « with non-attributable asymmetric techniques that focus upon information suppression, destruction and alteration[57]». Le but opérationnel est de mettre l'emphase « on deep strike (*zongshen zuozhan*) against enemy command hubs, information processing centers, and supply systems[58]». L'intention est donc de frapper rapidement les points critiques « of the enemy's information and support systems[59] ». Fidèle à la tradition chinoise, les objectifs

---

[53] Kathleen T. Rhem, "China Investing in information Warfare Thechnology, Doctrine", *American Forces Press Service* (July 2005), consulté le 5 mai 2015, http://www.defense.gov/news/newsarticle.aspx?id=16594.

[54] William G. Perry, "Information Warfare: An Emerging and Preferred Tool of the People's Republic of China", *Centre for Security Policy* (October 2007), consulté le 5 mai 2015, http://www.offnews.info/downloads/perry_china_iw.pdf.

[55] *Ibid*.

[56] *Ibid.*

[57] *Ibid.*

[58] Mark A. Stokes, "China's Quest for Information Dominance", *Strategic Studies Institute* (September 1999), consulté le 5 mai 2015, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB74.pdf.

[59] *Ibid.*

« are not the seizing of territory nor the killing of enemy military personnel, but rather the destruction of the other side's willingness or capability to resist[60] ».

People's War

L'armée chinoise a passé plusieurs années à analyser, entre autres, les publications américaines en matière d'opération d'information[61]. Finalement, « the Chinese military has adopted information warfare concepts suited to its own organization and doctrine, blending its own traditional tactics, concepts from the Soviet military, and U.S. doctrine to bring the PLA into the information age[62] ». Mais une condition importante doit être remplie et c'est celle d'avoir la parité technologique avec de possibles adversaires[63]. Ce que la Chine n'a pas encore atteint dans toutes les sphères technologiques. En résumé, la doctrine chinoise en matière d'opération d'information est basée sur « a blend of American IW doctrine with unique Chinese cultural components such as the gold standard of fighting a "People's War", deceptively killing with a borrowed sword and attacking weakness rather than strength[64] ».

C'est en examinant un rapport du Pentagone produit en 2006 que le terme People's War prend tout son sens. En effet, selon ce rapport, l'intégration de « militia [and] reserve personnel would make civilian computer expertise and equipments

---

[60] *Ibid.*

[61] Larry M. Wortzel, "The Chinese's People's Liberation Army and Information Warfare", *Strategic Studies Institutes and U.S. Army War College Press* (March 2014), consulté le 5 mai 2015, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1191.pdf.

[62] *Ibid.*

[63] William G. Perry, "Information Warfare: An Emerging and Preferred Tool of the People's Republic of China", *Centre for Security Policy* (October 2007), consulté le 5 mai 2015, http://www.offnews.info/downloads/perry_china_iw.pdf.

[64] *Ibid.*

available to support PLA training and operations[65] ». Le but ici est d'intégrer du personnel provenant des « academies, institutes, and information technology industries so as to integrate them into regular military operations[66] ». Ces groupes de personnes seront donc entrainée à supporter les opérations de l'armée chinoise en préparant et en livrant des opérations de grande envergure contre d'éventuels adversaires[67].

Ceci termine donc la deuxième partie de ce papier. Elle a proposé un sommaire de concepts clés pour comprendre l'évolution de la compréhension chinoise des opérations d'information et de sa stratégie. Il a donc été question de la révolution dans les affaires militaires et de la Guerre du Golfe de 1991. La vision chinoise de la guerre de l'information y a été présentée pour finalement présenter sa stratégie de People's war. La prochaine étape consiste donc à faire un survol de quelques-unes des capacités mis en œuvre en matière d'opération d'information et de guerre de l'information.

PARTIE 3 – CAPACITÉS

Le but de cette section n'est pas de passer en revue toutes les capacités chinoises en matière d'opération d'information. La guerre cybernétique, le cyber espionnage la propagande seront les capacités présentées. Pour ce qui est de la propagande, il est difficile de cibler seulement l'apport de l'armée chinoise dans le processus. C'est pour cette raison qu'il sera aussi question de la politique étrangère et de sécurité de la Chine dans cette rubrique. Bref, le plan ici est donc de faire un survol rapide de ces dimensions,

[65] "Annual Report to Congress - Military Power of People's Republic of China", Office of the Secretary of Defense (2006), consulté le 5 mai 2015, http://www.defense.gov/pubs/pdfs/China%20Report%202006.pdf.

[66] William G. Perry, "Information Warfare: An Emerging and Preferred Tool of the People's Republic of China", *Centre for Security Policy* (October 2007), consulté le 5 mai 2015, http://www.offnews.info/downloads/perry_china_iw.pdf.

[67] *Ibid.*

car chacune d'elle aurait pu faire l'objet d'une recherche individuelle. Ces dimensions sont surtout retenues, car elles représentent la majorité des écrits sur le sujet.

Guerre cybernétique

La Chine se retrouve souvent au banc des accusés lorsqu'il est question de guerre cybernétique ou pour son utilisation inappropriée du web[68]. Bien qu'il soit difficile de prouver hors de tous doutes l'implication de l'armée chinoise, il demeure que les « Chinese cyber-warfare units have been very active[69] ». Depuis leur balbutiement de 1997[70] à la mise en place d'un Cyber Command[71], de la simple intrusion à la destruction de l'information[72], «PLA IW units have reportedly developed detailed procedures for Internet warfare, including software for network scanning, obtaining passwords and breaking codes, and stealing data[73]». L'armée chinoise aurait aussi développé des capacités de «information-paralysing software, information-blocking software, information-deception software, and other malware; and software for effecting counter-measures destruction[74]».

Pour les Américains, ces capacités leur causent bien des maux de tête. Le directeur de la NSA souligne que « China and probably one or two other countries have

---

[68] Reuters, "China says worried by new U.S. cyber strategy", *Reuters* (April 2015), consulté le 6 mai 2015, https://ca.news.yahoo.com/china-says-worried-u-cyber-strategy-103100155.html.

[69] Desmond Ball, "China's Cyber Warfare Capabilities", *Security Challenges*, Vol 7, No. 2 (Winter 2011), consulté le 6 mai 2015, http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf.

[70] *Ibid.*

[71] Russel Hsiao, "China's Cyber Command?", *China Brief*, Volume 10, issue 15 (July 2010), consulté le 6 mai 2015, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=36658&cHash=88939b23f7#.VUnt9ct0z4g.

[72] Desmond Ball, "China's Cyber Warfare Capabilities", *Security Challenges*, Vol 7, No. 2 (Winter 2011), consulté le 6 mai 2015, http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf.

[73] *Ibid.*

[74] *Ibid.*

the ability to invade and possibly shut down computer systems of U.S. power utilities[75]». Ce dernier précise aussi que même les «aviation networks and financial companies[76]» sont à risque et représentent des cibles potentielles. Son casse-tête est de coordonner une défense commun, car le contrôle des différents systèmes est sous des juridictions différentes.

Pour le directeur du NSA, « it is only a matter of the when, not the if, that we are going to see something traumatic[77]». Il admet que plusieurs pays développent les capacités requises pour conduire de telles attaques, mais s'inquiète surtout des vulnérabilités des différents systèmes américains. Selon lui, « our vulnerability will be equivalent to a hole in our software systems that are unseen by the multinational company, the public utility, the telecom giant, the defense manufacturer, the Department of Defense[78]».

Pour l'instant, les Chinois semblent se limiter à l'indérdiction de service. C'est ce que l'on peu conclure selon le FBI qui souligne que « computer hackers linked to the Chinese government used two Chinese telecom companies and the Baidu search engine to mount mass data disruption attacks on American websites involved in circumventing Beijing's censors[79]». Très astucieux comme approche, « internet traffic entering China

---

[75] Patricia Zengerle, "NSA chief warns Chinese cyber attacks could shut U.S. infrastructure", *Reuters* (Nov 2014), consulté le 7 mai 2015, http://www.reuters.com/article/2014/11/21/us-usa-security-nsa-idUSKCN0J420Q20141121.

[76] *Ibid*.

[77] Robert Lenzner, "Chinese Cyber Attack Could Shut Down U.S. Electric Power Grid", *Forbes* (Nov 2014), consulté le 7 mai 2015, http://www.forbes.com/sites/robertlenzner/2014/11/28/chinese-cyber-attack-could-shut-down-u-s-electric-power-grid/.

[78] *Ibid.*

[79] Bill Gertz, "FBI Links Chinese Government to Cyber Attacks on U.S. Companies", *The Washington Free Beacon* (May 2015), consulté le 7 mai 2015, http://freebeacon.com/national-security/fbi-links-chinese-government-to-cyber-attacks-on-u-s-companies/.

was used in a data-denial attack against two websites involved in defeating Chinese-based web censorship[80]». Pour ce faire, « the traffic was "manipulated to create cyber attacks directed at U.S.-based websites". Même si les autorités chinoises affirment n'avoir rien à voir dans ce dossier, « the malicious activity occurred on China's backbone Internet infrastructure, and temporarily disrupted all operations on the U.S.-based websites[81]».

Cyber espionnage

Indissociable de la rubrique précédente, l'armée chinoise est aussi très active dans le domaine du cyber espionnage. Suite au rapport annuel au Congrès américain de 2012, « strong evidence has emerged that the Chinese government is directing and executing a large-scale cyber espionage campaign against the United States[82]». Selon le Dr Wortzel, «China to date has compromised a range of US networks, including those of DoD and private enterprises[83]».

À titre d'exemple de leur capacité, une technique consiste à faire l'usage de trojans. Dans un cas, « Trojan Horse programs camouflaged as Microsoft Word and PowerPoint documents have been inserted in computers in government offices in many countries around the world[84]». Un autre example fait reference au « Portable, large-capacity hard discs, often used by government agencies, have been found to carry Trojan Horses that automatically upload to Beijing Web-sites everything that the computer user

[80] *Ibid.*
[81] *Ibid.*
[82] Larry M. Wortzel, "China's Military Modernization and Cyber Activities", *Strategic Studies Quarterly* (Spring 2014), consulté le 6 mai 2015, http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/wortzel.pdf.
[83] *Ibid.*
[84] *Ibid.*

saves on the hard disc[85]». Ces techniques et bien d'autres encore poussent certains auteurs à dire que la Chine a maintenant une longueur d'avance dans le domaine de la guerre cybernétique[86].

Une unité de l'Armée chinoise a même fait les manchettes et l'objet d'un rapport extensifs. « There is evidence that since 2006 PLA Unit 61398 has penetrated the networks of at least 141 organizations, including companies, international organizations, and foreign governments[87]». Selon un rapport d'une firme de sécurité informatique indépendante, « Unit 61398, gained access to a wide variety of intellectual property and proprietary information through these intrusions[88]». Il faut noter ici qu'il n'est question que d'une unité de l'armée chinoise. En effet, « Unit 61398 is just one of more than 20 cyber attack groups with origins in China[89]».

Finalement, lors de son témoignage devant le Congrès, Dr Wortzel a tracé un bref aperçu des capacités chinoises. « There are about 16 technical reconnaissance (signals intelligence) units and bureaus in the PLA and at least seven electronic warfare and electronic countermeasures units[90]». Selon ce dernier, « each of China's seven military regions is supported by an electronic countermeasures regiment, and it looks like the PLA

---

[85] Yang Kuo-wen, Lin Ching-chuan and Rich Chang, "Bureau Warns on Tainted Discs", *Taipei Times* (November 2007) consulté le 6 mai 2015, http://www.taipeitimes.com/News/taiwan/archives/2007/11/11/2003387202

[86] David Francis, "U.S. Plays Catch-Up with China on Cyber Warfare", *The Fiscal Times* (May 2014), consulté le 6 mai 2015, http://www.thefiscaltimes.com/Articles/2014/05/11/US-Plays-Catch-China-Cyber-Warfare.

[87] *Ibid.*

[88] *Ibid.*

[89] Zoe Li, "What we know about the Chinese army's alleged cyber spying unit", *CNN* (May 2014), consulté le 6 mai 2015, http://www.cnn.com/2014/05/20/world/asia/china-unit-61398/.

[90] Larry M. Wortzel, "China's Military Modernization and Cyber Activities", *Strategic Studies Quarterly* (Spring 2014), consulté le 6 mai 2015, http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/wortzel.pdf.

Second Artillery Force has its own supporting unit[91]». Le but de ces organisations est « focus on cyber penetrations, cyber espionage, and electronic warfare[92]».

Propagande

Lorsqu'il est question de propagande en matière d'opération d'information, il faut obligatoirement revenir sur la politique étrangère et de sécurité de la Chine. Sachant que « the principal mission of China's military is to keep the Chinese Communist Party (CCP) in power[93]», le lien avec la politique étrangère et de sécurité s'impose. D'autant plus que la Chine propose dans sa politique des slogans accrocheurs de paix, de non-ingérence et de Peaceful Rise[94] mais qu'en réalité, ces actions n'ont souvent rien à voir avec ces fameux principes. Certains auteurs ne se cachent pas pour décrier la propagande chinoise[95].

Cette façon de faire est tout aussi visible dans le domaine des opérations d'information. La Chine préconise « the peaceful use of cyberspace. It maintains a position of 'no first use' of cyber-weapons, nor will it attack civilian targets[96]». Et pourtant, les exemples présentés plus haut témoignent du contraire. Même lorsqu'il est question de cyber espionnage, « Beijing usually attempts to refute evidence by pointing

---

[91] *Ibid.*
[92] *Ibid.*
[93] *Ibid.*
[94] Laurent Hou et Matthias Kauffmann, "Séduire l'Europe : la diplomatie publique chinoise en action », *China Institute Relations Internationales* (novembre 2011), consulté le 9 décembre 2014, http://www.china-institute.org/articles/Seduire_l_Europe_la_diplomatie_publique_chinoise_en_action3.pdf.
[95] *Ibid*.
[96] Li Zhang, "A Chinese perspective on cyber war", *International Review of the Red Cross,* Volume 94 Number 886 (Summer 2012), consulté le 6 mai 2015, https://www.icrc.org/eng/assets/files/review/2012/irrc-886-zhang.pdf.

to the anonymity of cyberspace and the lack of verifiable technical forensic data[97]». Peut-être encore plus habile comme démarche, « it also shifts the media focus by portraying itself as the victim of Washington's cyber activities and calling for greater international cooperation on cyber security[98]».

C'est ainsi que se termine la rubrique traitant des capacités chinoises en matière d'opération d'information. Le but n'était pas d'être exhaustif, mais bien de présenter les dimensions les plus importantes telles que la guerre cybernétique et les techniques employées, les capacités en matière de cyber espionnage et la propagande. Comme de raison, chacune de ces dimensions aurait pu faire l'objet de sa propre recherche. Bien qu'il ait été question de politique étrangère et de sécurité en traitant de propagande, cette escapade dans le domaine de la politique étrangère était nécessaire afin de mettre en place l'argumentions présentée pour expliquer la posture chinoise en matière d'opération d'information ayant trait à la propagande.

PARTIE 4 - ANALYSE

Cette dernière section a pour but de faire l'analyse de l'information présentée dans les parties précédentes afin de confirmer notre thèse. Pour se faire, il faut revenir sur les différents aspects de la stratégie chinoise afin de la préciser davantage et aussi revenir sur les évidences en termes de capacités. Pour y arriver, on propose d'examiner les données en traçant un bref portrait des deux puissances en cause afin de faire ressortir leur position respective dans la conduite de leurs opérations d'information.

---

[97] Larry M. Wortzel, "China's Military Modernization and Cyber Activities", *Strategic Studies Quarterly* (Spring 2014), consulté le 6 mai 2015, http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/wortzel.pdf.

[98] *Ibid.*

Effectivement, deux visions s'opposent. D'un côté, il faut comprendre que les efforts américains cherchent à prévenir le prochain Pearl Harbor[99]? C'est la hantise des États-Unis lorsqu'il est question des capacités chinoises. Cette façon de voir les choses peut aussi servir à tempérer la vision américaine par rapport à la menace que représente la Chine. Certes, la Chine présente définitivement une menace et elle semble posséder les moyens pour causer de sérieux dommages aux infrastructures américaines, mais cette réalité est aussi vraie pour les Américains. L'évidence présentée démontre les capacités chinoises, mais il ne faut pas croire que les Chinois sont les seuls à conduire des opérations de cyber espionnage ou de cyber attaques.

Deuxième aspect, la Chine est-elle si en retard? Les Chinois possèdent des capacités impressionnantes lorsqu'il est question d'opération d'information. Jumelée à sa stratégie de Peopl's war, la Chine est une menace réelle pour d'éventuels adversaires. Et pourtant, elle se prétend inférieure[100]. Une carte qu'elle joue très bien afin de tenter d'apaiser les soupçons à son égard tout en poursuivant sa quête – combler son retard technologique par tous les moyens possible. Les situations citées plus haut soulignent définitivement un savoir-faire important des Chinois. Elle n'a pas encore toute la technologie nécessaire pour conduire des opérations dans l'ensemble du spectre, mais elle prend les moyens pour y parvenir – en coupant le temps requis en matière de recherche et développement.

---

[99] Dominic Basulto, "Preventing a 'cyber Pearl Harbor' will require innovative thinking from the military", *Washinton Post* (Décembre 2014), consult. le 6 mai 2015, http://www.washingtonpost.com/blogs/innovations/wp/2014/12/10/preventing-a-cyber-pearl-harbor-will-require-innovative-thinking-from-the-military/.

[100] "China's Cyber Warfare." *Chinascope* no. 54 (November 2011): 6-16. Academic Search Complete, EBSCOhost (accessed April 18, 2015).

En ce qui concerne les capacités de la Chine de conduire des opérations d'information, nous y avons consacré une partie importante de ce papier et nous sommes conscients que nous avons à peine effleuré toutes les capacités dont elle dispose. Certaines sources placent même les capacités chinoises devant les capacités américaines dans le domaine du cyber espace[101]. Les écrits débordent d'exemple faisant référence à ces capacités dans ce domaine et comme nous l'avons présenté plus haut, il n'y a aucun doute que la Chine a entrepris le virage relié à la guerre de l'information et mise beaucoup sur les différentes dimensions des opérations d'information dans sa stratégie.

Comme nous y avons fait allusion plus haut, la doctrine chinoise est historiquement déjà structurée sur une approche asymétrique. Nous l'avons expliqué sous la rubrique de People's war, les Chinois se sont éloignés de la vision de conduire une guerre contre les Russes et ont tout simplement adapté les concepts de guerre de l'information et des opérations d'information en général à leur façon traditionnelle de conduire leurs activités. Le choc subit en analysant la Guerre du Golfe aura ouvert les yeux des stratèges chinois afin de revoir leur posture et leurs moyens. Loin d'avoir atteint les buts fixés, l'armée chinoise est sans cesse poussée par la classe politique afin de poursuivre sa modernisation et la mise en place des capacités et des organisations requises pour atteindre la parité avec les Américains.

Leur doctrine asymétrique est certainement très efficace. Un bon exemple de cette réalité est la façon dont la Chine se comporte dans le conflit de la mer de Chine. « China has made irregular warfare a key element of every aspect of its military doctrine, has

[101] David Francis, "U.S. Plays Catch-Up with China on Cyber Warfare", *The Fiscal Times* (May 2014), consulté le 6 mai 2015, http://www.thefiscaltimes.com/Articles/2014/05/11/US-Plays-Catch-China-Cyber-Warfare.

focused on political warfare in the South China Sea, and shown that it can use its coast guard and even an oil drilling platform to achieve its objectives[102]». En plus de faire usage de moyens non conventionnels, elle jumèle les opérations médiatiques ou de propagande afin de promouvoir une solution pacifique[103]. Encore une fois, il ne fait aucun doute que la stratégie asymétrique chinoise en matière de conduite des opérations d'information fonctionne. L'exemple ici traite de propagande, mais c'est aussi le cas pour ces techniques reliées au cyber espace comme il a été discuté plus haut.

Malgré tout, il manque un élément important. La Chine n'a pas encore atteint la maturité technologique par rapport aux États-Unis. C'est pourtant une condition importante pour la conduite des opérations d'information ou de la guerre de l'information comme nous l'avons expliqué plus haut. Nous avons souligné ses capacités dans le domaine du cyber espace, mais ce n'est qu'une dimension du spectre. Il lui reste du développement à faire dans bien d'autres sphères. Mais dans l'immédiat, les capacités citées en matière de cyber espace semblent indiquer que cette dimension des opérations d'information est sans l'ombre d'un doute la pièce maitresse de leur stratégie en attendant d'arriver à la parité technologique avec les Américains.

A la lumière des arguments présentés, il est donc possible de confirmer notre thèse. Il semble évident que la Chine voie dans les opérations d'information un moyen de contrer la menace américaine sans nécessairement devoir rivaliser avec les moyens

---

[102] Anthony H. Cordesman, "The Real Revolution in Military Affairs", *Centre for Strategic and International Studies* (August 2014), consulté le 6 mai 2015, http://csis.org/publication/real-revolution-military-affairs.

[103] Koh Swee Lean Collin, "Beijing's Fait Accompli in the South China Sea", *The Diplomat* (Avril 2015), consulté le 6 mai 2015, http://thediplomat.com/2015/04/beijings-fait-accompli-in-the-south-china-sea/.

techniques et militaires américains. En effet, l'exploitation des opérations d'information au sein d'une stratégie de contournement dans un contexte de People's war est pour la Chine une solution asymétrique à la menace américaine.

CONCLUSION

Dans un premier temps, nous avons proposé quelques définitions provenant de la doctrine canadienne afin d'établir une base commune, voire un langage commun. Plusieurs définitions circulent dans la littérature et il était donc nécessaire de procéder ainsi afin de présenter nos arguments et le cadre des opérations d'information. Nous avons présenté des définitions pour, l'information, les opérations offensives et défensives. Nous avons aussi proposé une définition du terme guerre de l'information, car il ne fait aucunement partie de la doctrine canadienne et américaine. Pour ce faire, nous avons extrapolé la notion de supériorité de l'information qui se veut la finalité de la guerre de l'information.

En second lieu, nous avons proposé un sommaire des concepts clés pour comprendre l'évolution de la compréhension chinoise des opérations d'information et de sa stratégie. Pour y arriver, nous avons discuté de la révolution dans les affaires militaires et de la Guerre du Golfe de 1991. C'est grâce à leur analyse de cette dernière que les stratèges chinois ont entrepris la modernisation de leur stratégie et de leur posture. La vision chinoise de la guerre de l'information y a été présentée dans le contexte de sa stratégie de People's war. La vision asymétrique traditionnelle chinoise se marie très bien avec les opérations d'information.

Dans la troisième partie, nous avons fait un survol des capacités chinoises en matière d'opération d'information. Le but n'était pas d'être exhaustif, mais bien de présenter les dimensions les plus importantes telles que la guerre cybernétique et les techniques employées, les capacités en matière de cyber espionnage et la propagande. Comme de raison, chacune de ces dimensions aurait pu faire l'objet de sa propre recherche, mais c'est essentiellement ces dimensions des opérations d'information qui font la force de la stratégie chinoise et c'est pour cette raison que nous nous sommes limités à ces dernières.

Finalement, la dernière partie avait pour but de faire l'analyse de l'information présentée dans les parties précédentes afin de confirmer notre thèse. Nous avons donc tracé les liens requis en revoyant et en précisant les différents aspects de la stratégie chinoise et nous sommes aussi revenus sur ses capacités. Nous avons présenté deux visions – soit la crainte américaine par rapport au prochain Pearl Harbor et nous avons questionné la perception chinoise par rapport à son retard technologique. C'est avec cette toile de fond que nous avons argumenté et confirmé la thèse que la Chine voie dans les opérations d'information un moyen de contrer la menace américaine sans nécessairement devoir rivaliser avec les moyens techniques et militaires américains. En effet, l'exploitation des opérations d'information au sein d'une stratégie de contournement dans un contexte de People's war est pour la Chine une solution asymétrique à la menace américaine.

Au cours de notre recherche, quelques questions ont fait surface et nous les présentons ici afin d'ouvrir le présent sujet vers d'autres dimensions. Dans le cadre de sa

politique étrangère et de sécurité, la Chine, partisane des relations bilatérales, ne fait malgré tout pas partie d'une alliance militaire dans la région[104]. Il y a certainement des échanges technologiques avec quelques pays, mais est-ce qu'elle entretient des liens avec la Russie, la Coré du Nord et l'Iran, tous des alliés potentiels naturels, en matière de recherche et développement des technologies requises pour conduire des opérations d'information? Aurait-elle besoin d'une telle alliance pour contrer la menace américaine? En fait, une alliance entre ces pays pourrait avoir des implications majeures pas seulement pour les Américains, mais pour la stabilité mondiale.

[104] Crocker, Hampson et Aall, *Rewiring Regional Security* (United States : United States Institute of Peace, 2001), p. 424.

BIBLIOGRAPHIE

Anderson, Ross J. *Security Engineering: A Guide to Building Dependable Distributed Systems*, (Indianapolis: John Wiley & Sons, 2010), consulté le 10 avril 2015, http://www.cl.cam.ac.uk/~rja14/book.html.

"Annual Report to Congress - Military Power of People's Republic of China", Office of the Secretary of Defense (2006), consulté le 5 mai 2015, http://www.defense.gov/pubs/pdfs/China%20Report%202006.pdf.

Associated Press, "China building airstrip on reclaimed island in disputed South China Sea: report", *CTV News* (17 avril 2015), consulté le 18 avril 2014, http://www.ctvnews.ca/world/china-building-airstrip-on-reclaimed-island-in-disputed-south-china-sea-report-1.2333295.

Babelio. « Citation de Sun Tzu », *Babelio* (mai 2014), consulté le 20 avril, 2015, http://www.babelio.com/auteur/Sun-Tzu/3396/citations?pageN=3.

Ball, Desmond. "China's Cyber Warfare Capabilities", *Security Challenges*, Vol 7, No. 2 (Winter 2011), consulté le 6 mai 2015, http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf.

Basulto, Dominic. "Preventing a 'cyber Pearl Harbor' will require innovative thinking from the military", *Washinton Post* (Décembre 2014), consult. le 6 mai 2015, http://www.washingtonpost.com/blogs/innovations/wp/2014/12/10/preventing-a-cyber-pearl-harbor-will-require-innovative-thinking-from-the-military/.

Campbell, Kurt and Andrews, Brian. "Explaining the US 'Pivot' to Asia", *Chatam House* (August 2013), consulté le 9 décembre 2014, http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Americas/0813pp_pivottoasia.pdf.

"China Quick Facts", *Special Warfare: The Professional Bulletin Of The John F. Kennedy Special Warfare Center & School* , (July – Sept 2012), consulté le 18 avril 2015, http://eds.b.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=6fb3084d-432f-42ba-987b-7503c2ca381a%40sessionmgr113&vid=0&hid=114.

"China's Cyber Warfare." *Chinascope* no. 54 (November 2011): 6-16. Academic Search Complete, EBSCOhost (accessed April 18, 2015).

"China Defence & Security Report*", Business Monitor International* (December 2014), consulté le 18 avril 2015, http://eds.b.ebscohost.com/ehost/detail/detail?vid=5&sid=d9dbc9a4-f90a-4055-824f-5602c1a44abe%40sessionmgr115&hid=114&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=bth&AN=100119658.

"China will not match US military power – general", *BBC News* (Mai 2011), consulté le 18 avril 2015, http://www.bbc.com/news/world-asia-pacific-13450316.
Collin, Koh Swee Lean."Beijing's Fait Accompli in the South China Sea", *The Diplomat* (Avril 2015), consulté le 6 mai 2015, http://thediplomat.com/2015/04/beijings-fait-accompli-in-the-south-china-sea/.

Chrsitensen, Thomas. « The Advantages of An Assertive China", *Council on Foreign Relations* (April 2011), consulté le 11 décembre 2014, http://www.cfr.org/china/advantages-assertive-china/p24202.

Cordesman, Anthony H. "The Real Revolution in Military Affairs", *Centre for Strategic and International Studies* (August 2014), consulté le 6 mai 2015, http://csis.org/publication/real-revolution-military-affairs.

Crocker, Hampson et Aall. *Rewiring Regional Security* (United States : United States Institute of Peace, 2001).

Department of Defense, *Joint Publication 3-13 : Information Operations* (Washington, D.C. Government Printing Office, November 2014), consulté le 21 avril 2015, http://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QFjAA&url=http%3A%2F%2Fwww.dtic.mil%2Fdoctrine%2Fnew_pubs%2Fjp3_13.pdf&ei=2KxKVfTfA9PjsASrq4CoAw&usg=AFQjCNHT-hBQ0K7H9RRS4dA8ntzp6vFs4A.

Francis, David. "U.S. Plays Catch-Up with China on Cyber Warfare", *The Fiscal Times* (May 2014), consulté le 6 mai 2015, http://www.thefiscaltimes.com/Articles/2014/05/11/US-Plays-Catch-China-Cyber-Warfare.

Gertz, Bill. "FBI Links Chinese Government to Cyber Attacks on U.S. Companies", *The Washington Free Beacon* (May 2015), consulté le 7 mai 2015, http://freebeacon.com/national-security/fbi-links-chinese-government-to-cyber-attacks-on-u-s-companies/.

Ho, Stephanie. "Chinese Foreign Relations to Focus on More Active Diplomacy", *Voice of America (*Mars 2011), consulté le 18 avril 2015, http://www.voanews.com/content/chinese-foreign-relations-to-focus-on-more-active-diplomacy-117511453/136106.html.

Holmes, James R. "Anti Access History Lessons", *The Diplomat* (Mai 2012), consulté le 23 avril 2015, http://thediplomat.com/2012/05/an-anti-access-history-lesson/.

Hong Hiep, Le. "China's new wave of assertiveness in the South China Sea", *The Strategist* (May 2014), consulté le 9 décembre 2014, http://www.aspistrategist.org.au/chinas-new-wave-of-assertiveness-in-the-south-china-sea/.

Horta, Loro. “China steals a march on Russian arms”, *Asia Times* (Décembre 2013), consulté le 18 avril 2015, http://www.atimes.com/atimes/China/CHIN-02-131213.html.

Hsiao, Russel. “China’s Cyber Command?”, *China Brief*, Volume 10, issue 15 (July 2010), consulté le 6 mai 2015, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=36658&cHash=88939b23f7#.VUnt9ct0z4g.

Hou, Laurent et Kauffmann, Matthias. “Séduire l’Europe : la diplomatie publique chinoise en action », *China Institute Relations Internationales* (novembre 2011), consulté le 9 décembre 2014, http://www.china-institute.org/articles/Seduire_l_Europe_la_diplomatie_publique_chinoise_en_action3.pdf

Lenzner, Robert. “Chinese Cyber Attack Could Shut Down U.S. Electric Power Grid”, *Forbes* (Nov 2014), consulté le 7 mai 2015, http://www.forbes.com/sites/robertlenzner/2014/11/28/chinese-cyber-attack-could-shut-down-u-s-electric-power-grid/.

Li, Zoe. “What we know about the Chinese army's alleged cyber spying unit”, *CNN* (May 2014), consulté le 6 mai 2015, http://www.cnn.com/2014/05/20/world/asia/china-unit-61398/.

Ministère de la défense nationale, B-GL-300-001/FP-002, *Opérations terrestres*, (Ottawa : MDN Canada, 2008).

Ministère de la défense nationale, B-GG-005-004/AF-010, *Opérations d’information des FC*, (Ottawa : MDN Canada, 1998).

Pagliery, Jose. “Ex-NSA director: China has hacked 'every major corporation' in U.S.”, *CNN* (March 2015), consulté le 18 avril 2015, http://money.cnn.com/2015/03/13/technology/security/chinese-hack-us/.

Perry, William G. “Information Warfare: An Emerging and Preferred Tool of the People’s Republic of China”, *Centre for Security Policy* (October 2007), consulté le 5 mai 2015, http://www.offnews.info/downloads/perry_china_iw.pdf.

Reuters. “China says worried by new U.S. cyber strategy”, *Reuters* (April 2015), consulté le 6 mai 2015, https://ca.news.yahoo.com/china-says-worried-u-cyber-strategy-103100155.html.

Rhem, Kathleen T. “China Investing in information Warfare Thechnology, Doctrine”, *American Forces Press Service* (July 2005), consulté le 5 mai 2015, http://www.defense.gov/news/newsarticle.aspx?id=16594.

Sloan, Elinor "Canada and the Revolution in Military Affairs: Current Response and Future Opportunities," *Canadian Military Journal* 1, 3 (2000), p. 7, consulté le 23 avril 2015, http://www.journal.dnd.ca/vo1/no3/doc/7-14-eng.pdf.

Sharp, Andy. "Xi Urges China Military Strategy for Information Warfare", *Bloomberg Business* (Août 2014), consulté le 23 avril 2015, http://www.bloomberg.com/news/articles/2014-08-31/xi-urges-new-china-military-strategy-for-information-warfare-.

Stokes, Mark A. "China's Quest for Information Dominance", *Strategic Studies Institute* (September 1999), consulté le 5 mai 2015, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB74.pdf.

Thompson, Micheal J. " Military Revolutions and Revolutions in Military Affairs: Accurate Descriptions of Change or Intellectual Constructs?", *Strata* (Septembre 2011), consulté le 23 avril 2015, http://artsites.uottawa.ca/strata/doc/strata3_082-108.pdf.

Ventre, Daniel. « China's Strategy for Information Warfare : A Focus on Energy", Journal of Energy Security (May 2010), consulté le 18 avril 2015, http://ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361.

Wee, Sui-Lee. "China's Xi urges army to create strategy for information warfare", *Reuters* (Août 2014), consulté le 23 avril 2015, http://www.reuters.com/article/2014/08/30/us-china-xi-defence-idUSKBN0GU0H020140830.

Wei-cheng, Vincent, and Gwendolyn Stamper. "Asymetric war? Implications for China's Information Warfare Strategies." *American Asian Review* 20, no. 4 (Winter 2002). Academic Search Complete, EBSCOhost (accessed April 23, 2015).

Worstall, Tim. "China's Now The World Number One Economy And It Doesn't Matter A Darn", *Forbes* (Juillet 2014), consulté le 18 avril 2015, http://www.forbes.com/sites/timworstall/2014/12/07/chinas-now-the-world-number-one-economy-and-it-doesnt-matter-a-darn/.

Wortzel, Larry M. "China's Military Modernization and Cyber Activities", *Strategic Studies Quarterly* (Spring 2014), consulté le 6 mai 2015, http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/wortzel.pdf.

Yang Kuo-wen, Lin Ching-chuan and Rich Chang, "Bureau Warns on Tainted Discs", *Taipei Times* (November 2007) consulté le 6 mai 2015, http://www.taipeitimes.com/News/taiwan/archives/2007/11/11/2003387202

Zengerle, Patricia. “NSA chief warns Chinese cyber attacks could shut U.S. infrastructure”, *Reuters* (Nov 2014), consulté le 7 mai 2015, http://www.reuters.com/article/2014/11/21/us-usa-security-nsa-idUSKCN0J420Q20141121.

Zhang, Li. “A Chinese perspective on cyber war”, *International Review of the Red Cross,* Volume 94 Number 886 (Summer 2012), consulté le 6 mai 2015, https://www.icrc.org/eng/assets/files/review/2012/irrc-886-zhang.pdf.

Zhao, Suisheng. “Chinese Foreign Policy as a Rising Power to Fin dits Rightful Place”, *Perceptions*, volume 18, no 1 (printemps 2013), consulté le 17 novembre 2014, http://sam.gov.tr/chinese-foreign-policy-as-a-rising-power-to-find-its-rightful-place/.