ECOLE DE GUERRE

PROMOTION *VERDUN*

2015 -2016

La Guerre de l'Information Russe, la Crimée, et les Implications pour l'OTAN

Commandant Russell J. Isaacs

Sous la direction de

Paul Villatoux

Docteur en histoire

RESUME

Les capacités de la Russie dans le domaine de la guerre de l'information pendant les opérations de Crimée illustrent le nouveau défi auquel doivent faire face les dirigeants et décideurs de l'OTAN. Le conflit en cours en Ukraine met en évidence la complexité croissante de la guerre et démontre la puissance de la guerre de l'information. En outre, la première étape de l'opération menée par la Russie en Crimée, c'est-à-dire la mise en place de conditions favorables à l'obtention de renseignements au cours des années précédant l'usage de la force, démontre la volonté et la capacité de la Russie à mener une guerre d'information permanente contre les États de l'ex URSS et contre l'OTAN. Le cadre juridique et institutionnel actuel de l'OTAN est incapable de répondre efficacement au type de guerre mené en Crimée. Afin de répondre à ces nouveaux défis que représente la guerre d'information menée par la Russie, l'OTAN et les États-Unis doivent développer une doctrine, des capacités de manœuvre coordonnées ainsi qu'une campagne de protection des informations pour protéger ses membres contre les futures guerres de nouvelle génération menées par la Russie

---

Russia's invasion and annexation of Crimea exemplifies the prominent role of information warfare in Russia's new generation warfare. Russia's weaponization of information set the necessary conditions and atmospherics prior to the commencement of hostilities. During the invasion, Russia utilized information warfare to isolate the Ukrainian government from its own people prevented NATO or US intervention or assistance to Ukraine. As a result, Russian new generation warfare has secured Russia's strategic goals of annexing Crimea, extending a pro-Russian zone farther west into Ukraine, and increasing the perception of Russian strength in eastern Europe, the Baltics, and Caucuses. Furthermore, the first stage of Russia's operation in Crimea, the setting of information conditions during the years prior to the use of force, demonstrates Russia's resolve and capability to wage persistent information warfare against ex-Soviet states and NATO. Lastly, the current NATO legal and institutional framework is unable to effectively respond to the type of warfare executed in Crimea. In order to respond to these types of challenges that Russian information warfare presents, NATO and the United States must develop the doctrine and capabilities to wage a sustained, coordinated, and whole-of-government information campaign that can protect its members from future Russian new generation wars, as well as persistent Russian information aggression.

Introduction

> "*In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. The broad use of political, economic, informational, humanitarian, and other nonmilitary measures….is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces. .*"[1] **General Valery Guerasimov**

Cette déclaration, faite par le général Valery Guerasimov, chef de l'état-major général de la Fédération de Russie, décrit précisément le contexte dans lequel s'est déroulée l'invasion russe en Ukraine et l'annexion de la Crimée en 2014. Le 27 février 2014, des hommes armés, sans signe distinctif, ont pris d'assaut des installations gouvernementales en Crimée. L'apparition de ces «Little Green Men» était le signal initial du déclenchement d'une opération militaire russe prévoyant l'invasion de la Crimée. La surprise créée lors de cette opération a permis à la Russie de tromper le gouvernement ukrainien nouvellement installé et la communauté internationale.[2] En outre, les opérations de désinformation et de d'intoxication effectuées par Moscou ont déstabilisé l'Ukraine ainsi que le cycle de prise de décision de L'OTAN. Incapable de réagir efficacement face aux événements sur le terrain, l'Ukraine a peu à peu perdu son emprise sur la Crimée. Le 18 mars, la Russie réalise avec succès l'annexion de la Crimée en déployant seulement 10.000 soldats.

Les capacités de la Russie dans le domaine de la guerre de l'information pendant les opérations de Crimée illustrent le nouveau défi auquel doivent faire face les dirigeants et décideurs de l'OTAN. Le conflit en cours en Ukraine met en évidence la complexité croissante de la guerre et démontre la puissance de la guerre de l'information. Bien que ce type de guerre non-linéaire ne soit pas nouvelle et a même été utilisée par l'Allemagne lors de l'invasion en 1939 de la Pologne, les progrès technologiques modernes dans le domaine de l'information ont renforcé l'impact extrêmement puissant de ce type de guerre. Dans le contexte contemporain, l'information peut précipiter la dissolution rapide d'un Etat et rendre les moyens militaires traditionnels inopérants. Depuis la création de l'OTAN en tant que rempart contre l'Union soviétique, l'environnement international dans le domaine de la sécurité s'est transformé. Compte tenu de la multipolarité et de l'asymétrie du système international actuel, la majorité des conflits futurs sera menée dans la «Gray Zone» (zone incertaine) du spectre des conflits. Dans ces derniers, l'information peut s'avérer plus puissante que la force militaire. En outre, un État peut fusionner des outils conventionnels et non étatiques au sein d'une stratégie non-linéaire permettant d'obtenir la victoire sans effusion de sang, et

---

[1]Robert Coalsen, "Top Russian General Lays Bare Putin's Plan for Ukraine," *The world Post*, February 9, 2014, accessed 18 November 2015, http://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html

[2] Mark Galeotti, " 'Hybrid War' and 'Little Green Men' : How it Works and How It Doesn't," E-International Relations, April 16, 2015, accessed 18 November 2015, http://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/.

ce avant même le début des hostilités déclarées. Comme on le voit en Géorgie en 2008 et de nouveau en Ukraine en 2014, la Russie mène un style de guerre non déclaré qui utilise l'information comme une arme pour manipuler les perceptions au sein des populations étrangères et amener les pays à genoux avec une force militaire directe minimale. Ce type de « New Generation Warfare » et de guerre de l'information à long terme présente des défis importants pour l'OTAN notamment dans le cadre de l'application de l'article V et du renforcement de ses capacités dans le domaine de la guerre de l'information.

La problématique de cette étude repose sur la question suivante : quels enseignements l'OTAN peut-elle tirer de l'utilisation par la Russie des Opérations d'Information lors de la crise en Crimée et en Ukraine ? L'objet de ce mémoire est ainsi d'analyser la guerre de l'information russe à travers l'exemple de la Crimée et d'évaluer ses implications pour l'OTAN. Plus précisément, ce document entend démontrer que: 1) le poids de l'influence soviétique dans la théorie géopolitique russe constitue la principale base sur laquelle repose la guerre de l'information russe 2) le principe psychologique soviétique du « contrôle réflexif » (reflexive control) est l'élément central de la guerre de nouvelle génération et 3) l'efficacité de la guerre de l'information menée par la Russie démontre que l'OTAN doit développer sa propre capacité et mettre en place une structure capable de mener en permanence une guerre de l'information dans la zone grise.

Pour faire face aux nouveaux défis sécuritaires, l'OTAN et ses États membres doivent développer une volonté, une doctrine et une capacité de lutte contre les campagnes d'information afin de protéger ses membres de conflits à venir en «Gray Zone» et contre les agressions permanentes dans le domaine de l'information.

1. L'évolution de la Guerre de l'Information Russe

1.1 Les Fondations Soviétiques comme base de la théorie de la Guerre de l'Information Russe

Avant d'explorer le rôle de guerre de l'information dans la stratégie russe, il est utile de définir la manière dont la Russie de l'ère moderne utilise les informations dans les guerres afin de pouvoir le différencier du concept utilisé par l'OTAN dans le domaine des opérations d'information. Les doctrines américaine et Otanienne fournissent des définitions claires, identifient les responsables en charge des opérations, et définissent les limites des opérations d'information. Ainsi, dans la doctrine militaire des États-Unis, les opérations d'information (*Information Operations)* comprennent les moyens suivants pour influencer les publics-cibles: Public Affairs, Military Information Support Operations (MISO), Combat Camera, Civil Affairs, la sécurité des opérations et la déception militaire. Les MISO, ou opérations psychologiques, visent spécifiquement à persuader, modifier et influencer les attitudes, les croyances et le comportement d'un public-cible étranger. Les opérations

psychologiques des États-Unis ne peuvent cibler que des publics désignés spécifiquement à l'étranger et ceci en utilisant des éléments s'appuyant sur la vérité, sélectionnés pour pouvoir les influencer.

Alors que la définition des opérations d'information utilisée par l'OTAN et les États-Unis constitue un élément utile pour examiner les opérations d'influence russe, le concept de la guerre de l'information russe est à la fois plus large et moins clairement défini. La guerre de l'information russe moderne tire ses racines de la guerre psychologique soviétique. La guerre psychologique soviétique impliquait l'utilisation sophistiquée de deux éléments, l'un interne, l'autre externe pour influencer l'opinion: *Maskirovka* pour les publics-cibles externes; et *spetspropaganda*, que le gouvernement soviétique a utilisé en interne et que l'armée a utilisé vers l'extérieur. Ces deux doctrines ont été enseignées dès 1942 à l'Institut Militaire des Langues Etrangères.[3] *Spetspropaganda* visait à modifier ou manipuler les perceptions, les attitudes et le comportement des publics nationaux et étrangers. *Spetspropaganda* inclut un grand nombre de concepts actuels de la doctrine de la guerre psychologique, comme la désinformation et la propagande. Pierre Nordin, spécialiste de la désinformation et de guerre psychologique, décrit l'importance de la guerre de l'information en disant : « *Making ideology part of psychological warfare was a Soviet innovation, turning this into a massive and universal warfare. Another innovation was the incessant use of psychological weapons. The point is that peacetime never exists for the government in Moscow.*[4]"

Dans la doctrine russe contemporaine, l'influence est au centre de la planification opérationnelle et stratégique. L'un des principaux théoriciens militaires russes, le major général en retraite Ivan Vorobev, définit la guerre de l'information comme un concept comprenant trois volets: (i) l'attaque psychologique par l'information, la désinformation et la déception de l'ennemi; (Ii) l'attaque par l'utilisation de psychotropes qui affectent la psyché de l'ennemi; et (iii) l'attaque informatique.[5] Une autre grande école de pensée dans la théorie militaire russe effectue une distinction au sein de la guerre d'information en deux branches principales: l'information technique et l'information psychologique.[6] En 2014, le major-général à la retraite Charis Saifetdinov a publié un article évaluant la place de la guerre de l'information dans la guerre moderne. Il a constaté que la guerre de l'information se joue sur l'information sécurisée, sur les opérations sur les réseaux informatiques, l'intelligence artificielle, la guerre électronique et les opérations psychologiques. Cette

[3] Ibid
[4] Brett Perry, "Non-Linear Warfare in Ukraine : the Critical Role of Information Operations and Special Operations," *Small Wars Journal*, August 14, 2015, accessed November 18, 2015, 5.
[5] Ulrik,Francke, "War by Non-Military Means : Understanding Russian Information Warfare," FOI Swedish Defense Research Agency, December 3, 2015, accessed February 14, 2016, 23.
[6] Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts," *Journal of Slavic Military Studies* 27 (2014): 102.

définition s'avère étrangement similaire à celle de la doctrine de l'OTAN.[7] Enfin, les colonels Bazylev, Dylevski, Komov et Petrunin pensent que la guerre de l'information est basée sur trois axes principaux: les attaques contre les infrastructures sensibles, les attaques dans le but de perturber le leadership de l'ennemi, et les attaques pour démoraliser et tromper la population.[8] Bien qu'il existe de nombreux points de vue théoriques sur le sujet, le fondement de la guerre de l'information russe repose sur l'utilisation de purs mensonges et de la désinformation dans le but d'influencer les perceptions et les comportements des publics-cibles. Pour exercer une influence, la Russie utilise une vaste gamme de leviers militaires et non-militaires bien coordonnés. Comme on le voit dans les opérations en Géorgie en 2008 et en Ukraine en 2014, la Russie utilise les opérations psychologiques, les médias à grande diffusion parrainés par le gouvernement (*RT* ou *la Russie d'Aujourdhui*), la cyber-guerre, la guerre électronique, les opérations de déception, la manipulation diplomatique, ou la politique étrangère "humanitaire".

La guerre d'information russe repose sur le concept soviétique du principe de « contrôle réflexif ». Les différents leviers que la Russie utilise aujourd'hui pour ses opérations d'influence et de déception visent à modifier le comportement et la pensée par le contrôle réflexif. Le contrôle réflexif est un concept soviétique qui vise à manipuler la perception afin de perturber le cycle et le comportement de prise de décision de la cible. Il a été utilisé et affiné par les praticiens soviétiques depuis les années 1960. Initialement conceptualisé par V.A. Lefebre dans les années 1960 comme une composante clé de *maskirovka* et *spetspropaganda*, le contrôle réflexif vise à perturber et à manipuler le cycle de prise de décision de l'ennemi. Le principe est similaire au concept américain de « perception management » ou de gestion de la perception. Le contrôle réflexif se définit comme un «means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action. »[9] Plus simplement, un état ou un militaire s'assure qu'un acteur ciblé reçoit certaines informations ou subit de la désinformation ce qui permet de créer une perception spécifique et ainsi de pousser l'acteur à prendre des mesures, à adopter un comportement ou à développer une idée spécifique. Le contrôle réflexif exploite les facteurs culturels, moraux et psychologiques, et les caractéristiques de comportement qui agissent comme des filtres de l'information et comme des déterminants de la perception. Le contrôle réflexif peut être utilisé pour effectuer des opérations de guerre psychologique ou de déception; par exemple, dans le but de modifier le comportement ou les croyances d'un public-cible. Il pourrait être utilisé pour insérer des informations dans le cycle de

[7] Francke, 26
[8] Ibid, 27.
[9] Timothy Thomas, "Russia's Reflexive Control Theory and the Military," 237.

décision de la cible. La perturbation du cycle de décision de l'ennemi est liée au concept de la « OODA loop » (Observer, Orient, Decide, Act) qui est utilisé pour décrire le processus de commandement et de contrôle militaire. Le contrôle réflexif vise à infiltrer les perceptions et croyances spécifiques dans la OODA Loop afin de perturber et retarder les actions de l'ennemi. Au cours des dernières décennies, les théoriciens soviétiques ont amélioré le principe du contrôle réflexif et son utilisation aux niveaux tactique, opérationnel et stratégique de la guerre.[10] L'un des théoriciens soviétiques le plus connu sur le contrôle réflexif, le major-général (ret.) M.D. Ivonov, a étudié les utilisations faite par l'armée soviétique du contrôle réflexif à partir de 1970. En 1995, Ivonov a identifié quatre méthodes de base de transfert d'informations vers une cible dans le but de prendre le contrôle réflexif. Comme l'a identifié Timothy Thomas, ces méthodes comprennent: 1) l'utilisation de la pression, des menaces ou de la coercition militaire, 2) les mesures visant à présenter des informations fausses sur la situation, 3) l'influence de l'algorithme de prise de décision de l'ennemi, et 4) la modification de la durée ou du temps de prise de décision.[11] Ces principes, dans l'étude de la guerre de l'information russe en Géorgie et en l'Ukraine sont encore utilisés par le commandement militaire russe aujourd'hui.

L'évidence la plus récente de la pertinence du contrôle réflexif est la mise en place en 2001 d'un nouveau journal russe, *Reflexive Processes and Control*. Non seulement ce journal est une publication scientifique, mais les institutions de sécurité nationale russes sont également fortement impliquées dans sa production.[12] D'autres outils psychologiques soviétiques incluent l'influence de la société (contrôle social), la manipulation de l'information, la fabrication de l'information, le chantage et l'extorsion.[13] Ces outils ont été constamment amélioré et ajusté. Aujourd'hui, ces principes soviétiques ont un rôle central dans la guerre de l'information russe. Comme l'affirme Snegovaya, "basic analysis reveals that all of the main principles and approaches the Russian government utilizes today were taken from Soviet toolkits».[14] Par exemple, l'approche 4D (dismiss, distort, distract, dismay) que de nombreux analystes des problèmes de Défense utilisent pour décrire les principes actuels russes dans la guerre de l'information est directement déduite des techniques de désinformation et de *maskirovka*. En outre, le contrôle réflexif est le principe majeur de l'approche 4D. Les discours de *Russie d'Aujourdhui*, et autres médias contrôlés par le gouvernement russe, ainsi que ceux des « cyber trolls » russes déforment les messages pour tromper le public ciblé afin de changer ses perceptions. Par conséquent, la guerre de l'information contemporaine russe est

[10] Ibid, 239.
[11] Ibid, 244-245
[12] Timothy Thomas, "Russia's Reflexive Control Theory and the Military,"*Journal of Slavic Military Studies* 17 (2004): 237.
[13] Darczewska, 15.
[14] Snegovaya, 13.

clairement basée sur le playbook/l'éventail des possibles soviétiques de contrôle réflexif et *spetspropaganda*. Toutefois, cela ne suffit pas à expliquer l'importance accordée à l'information dans la stratégie de défense russe actuellement. L'évolution de la guerre de l'information dans la stratégie russe est importante depuis la chute de l'Union Soviétique.

1.2 La Théorie Géopolitique et la Guerre de l'Information

Après la chute de l'Union Soviétique, l'évolution de la théorie géopolitique russe a conduit à la montée de guerre de l'information au sein de la stratégie russe moderne. En fait, le calcul géopolitique de la Russie au cours des dernières années est à la base même du développement de ses capacités de guerre non-linéaires. Jusqu'en 1998 et l'effondrement du rouble, la politique russe et notamment sa politique étrangère était assez équilibrée entre le libéralisme occidental et le réalisme nationaliste. Au cours des deux premiers mandats présidentiels de Vladimir Poutine entre 2000 et 2008, « like many other nations in the world, Russia sought means to balance, or more correctly contain, U.S. unipolar hegemony. The United States was not viewed as malign, but often as misguided and overbearing. »[15] Cependant, les protestations au sujet de l'affaire Bolotnaya ont déclenché un changement important dans la politique et la géopolitique étrangère russes. Ces manifestations, qui ont suivi la troisième réélection controversée de Vladimir Poutine en 2012, ont déclenché une réorientation rapide de la politique étrangère russe. Les discours de dénigrement du Kremlin par les États-Unis et l'OTAN destinés à provoquer la chute de Poutine et attaquer la Russie ont conduit à une politique intérieure qui a supprimé l'opposition et à une politique étrangère dominée par un discours nationaliste reposant sur une vision de l'OTAN perçue comme une menace extérieure imminente.

De nombreux analystes occidentaux ont utilisé le terme d'«hybride» pour décrire ce nouveau style de guerre qui unit la stratégie militaire classique et la guerre de l'information. L'un des modèles les plus explicites a été développé par Frank Hoffman, qui définit la guerre hybride comme la fusion d'une «full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. » D'autres analystes, comme Peter Pomerantsev ou Mark Galleotti ont dénommé cette nouvelle guerre comme étant « non linéaire ».[16] Ce mémoire, pour sa part, a choisi d'utiliser le terme des deux théoriciens russes de « *New Generation Warfare* ».

---

[15] Andrew C. Kuchins and Igor A. Zevelev, "Russian Foreign Policy: Continuity in Change." *The Washington Quarterly* 35 (2012): 154.
[16] Peter Pomerantsev, "How Putin in Reinventing Warfare." *Foreign Policy*, May 5, 2014, , http://www.foreignpolicy.com/articles/2014/05/05/how_putin_is_reinventing_warfare, accessed November 24, 2015.

1.3 New Generation Warfare et le Rôle de l'Information

La guerre de l'information russe contemporaine est mieux formulée à travers l'expression de *New Generation Warfare*. Le concept de *New Generation Warfare* est le résultat de l'analyse russe depuis des décennies à la suite de changements dans le système international actuel. En 1995, le général russe Makhmout Gareïev a indiqué que l'innovation technologique était en train de changer fondamentalement la guerre, à la fois dans les effets dévastateurs des armes classiques et par l'avènement de nouvelles formes de guerre. Plus précisément, il a affirmé que le progrès technologique ferait de l'information une arme particulièrement dévastatrice dans les conflits à venir.[17] Par conséquent, dès 1995, la direction militaire russe a considéré l'information comme partie intégrante de la guerre future. Coïncidant avec les changements dans le calcul géopolitique russe, cette idée a été développée en 2013 par le général Valéri Guérassimov, chef de l'état-major général de la Fédération de Russie. Gerasimov a mentionné les leçons des « Révolutions de couleur » et du Printemps arabe et décrit le potentiel dévastateur des conflits «non-linéaires» de l'avenir. Comme il l'a écrit, «information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy. In North Africa, we witnessed the use of technologies for influencing state structures and the population with the help of information networks. It is necessary to perfect activities in the information space, including the defense of our own objects.»[18] Guérassimov a estimé que l'environnement contemporain et les réalités géopolitiques russes ont empêché la conduite de la guerre ouverte. Il est désormais nécessaire de combiner l'action diplomatique, économique, politique et les outils d'information avec la force militaire. Plutôt que d'être ouvertement déclarée, cette nouvelle forme de guerre serait exécutée d'une manière dissimulée. Les outils non militaires seraient utilisés par les acteurs gouvernementaux pour dissimuler l'application de la force militaire et les véritables objectifs, tandis que les unités paramilitaires et les unités d'insurgés civils seraient utilisées à la place des soldats russes en uniforme. Plus important encore, dans les guerres actuelles, la notion d'influence est au centre de la planification opérationnelle et stratégique russe. Dans le but d'influencer de manière efficace, la Russie utilise tous les leviers militaires et non-militaires de la guerre de l'information. Le grand principe qui guide l'exécution de la guerre de l'information est le contrôle réflexif.

Les théoriciens de la guerre russe, le lieutenant-général (retraité) S.A. Bogdanev et le colonel (retraité) Chekinov, ont mis en forme sur le plan opérationnel des théories de Gareïev et Guérassimov et ont proposé un modèle étape par étape de la guerre, qu'ils ont intitulé «*New*

[17] Rácz, 36.
[18] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War."

Generation Warfare». Il s'agit en réalité d'un modèle pour la guerre russe de l'avenir qui s'avère similaire aux opérations russes en Crimée et en Ukraine. Dans le contexte de *New Generation Warfare*, Bogdanev et Chekinov organisent les futurs conflits en deux phases principales. Pendant la première phase, les théoriciens proposent que la gamme complète des outils gouvernementaux soient utilisés dans les mois précédents une opération militaire afin d'établir les conditions nécessaires préalables aux opérations armées. Cette partie de l'opération aurait pour but de tirer profit d'un environnement favorable déjà établi par les opérations latentes réalisées au cours des années précédentes. Ces opérations latentes sont similaires à celles proposées par Douguine et Panarine et comprennent, par exemple, des programmes culturels pro-russes dans le pays ciblé, ou des campagnes d'alphabétisation pro-russes. Comme Bogdanev et Chekinov l'écrivent, « the aggressor will make an effort to involve all public institutions in the country it intends to attack, primarily the mass media and religious organizations, cultural institutions, non-governmental organizations, public movements financed from abroad, and scholars engaged in research in foreign grants. »[19] Bogdanev et Chekinov affirment également que des mesures d'information en matière économique et diplomatique doivent être adoptées afin de créer un nouvel état de fait, ou exagérer un état de fait existant, et ainsi aboutir à créer une crise qui pourrait justifier une intervention sous le couvert d'une «intervention humanitaire »étrangère. En outre, les moyens multiples de l'Etat doivent être mis à profit afin de dissimuler le véritable objectif et la date de l'opération. La reconnaissance et le pré-positionnement des forces sous le couvert d'exercices de préparation permettront à l'agresseur d'obtenir un effet de surprise et de commencer le conflit sans avertissement. Cette approche reflète l'opinion de Guérassimov selon laquelle à l'avenir une guerre non-linéaire ne sera pas déclarée.[20] Outre l'élément de surprise, l'absence d'une déclaration de guerre ou de justification ne peuvent qu'exacerber l'incertitude et le désespoir ressentis par la population du pays ciblé.

Bogdanev et Chekinov proposent un modèle plus développé que celui de Douguine ou Panarine. Selon eux, la guerre de l'information est l'aspect le plus essentiel dans la première phase en particulier mais aussi dans un futur conflit en général. Comme ils l'écrivent : «a New Generation War will be dominated by information and psychological warfare that will seek to achieve superiority in troops and weapons control and depress the opponent's armed forces, personnel and population morally and psychologically. In the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory.»[21] Selon la théorie de Chekinov et Bogdanev, l'importance de l'information mise en place dans les mois

[19] S.G. Chekinov and S.A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought* 4 (2013): 17.
[20] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War."
[21] Bogdanov and Chekinov, "The Nature and Content of a New-Generation War," 16.

précédant un conflit et entretenue tout au long du conflit est le déterminant clé de la victoire. Selon leur évaluation, au cours de la phase initiale d'une *New Generation Warfare*, une intense campagne de guerre de l'information ciblera simultanément les médias étrangers ainsi que certains groupes dans le pays ciblé. Cette campagne d'information de guerre comprend à la fois des informations techniques ainsi que des mesures d'information et psychologiques et visent à réduire le soutien de la population envers son gouvernement, à augmenter le sentiment de désespoir et d'incertitude, à affaiblir le moral des militaires. Au cours de cette phase initiale, des agents secrets infiltrent le pays ciblé et exécutent des activités subversives telles que sabotage, actes terroristes afin de créer le chaos et l'instabilité.[22]

Dans l'étape suivante, juste avant l'entrée des forces terrestres, une opération agressive de guerre électronique permettra de désactiver les communications entre les responsables militaires et politiques afin de prendre le commandement et le contrôle du système du gouvernement ennemi. En outre, une offensive aérienne sera lancée pour effectuer un bombardement de précision, un tir de longue portée d'artillerie et des frappes de drones afin de neutraliser les centres de commandement et de contrôle et de détruire les infrastructures sensibles.[23] Dans la phase finale, les forces terrestres entreront dans le pays cible afin de détruire la résistance ennemie et atteindre les objectifs opérationnels. Bogdanev et Chekinov soulignent l'importance pour la Russie de développer immédiatement cette doctrine de guerre non-linéaire: «realities of our day dictate an urgent need to prepare Russia for possible new-generation wars without further delay. It is a first priority for this country because its defense and economic potential has waned significantly over the past two or three decades. »[24] Ainsi, la théorie géopolitique russe a eu une influence indéniable sur la création d'un modèle nouveau que représente une nouvelle génération de guerre. En outre, la théorie géopolitique russe et l'avènement consécutif d'une doctrine de guerre fondée sur le huis clos et la volonté de briser l'ennemi, explique l'importance de la guerre de l'information dans la pensée militaire russe.

2. La Guerre de l'Information Russe en Crimée

L'invasion par les russes de la Crimée en 2014 et l'adhésion de la Crimée à la Russie constitue un exemple du rôle de l'information dans les conflits russes actuels. Le 27 Février 2014, des hommes armés sans signe distinctif ont saisi les principales installations du gouvernement en Crimée. En trois semaines, sans le moindre coup de feu, les bases militaires ukrainiennes à travers la péninsule avaient

[22] Racz, 39.
[23] Ibid.
[24] Bogdanov and Chekinov, "The Nature and Content of a New-Generation War," 11.

cédé et le 17 Mars la Crimée a annoncé son indépendance vis-à-vis de l'Ukraine et a demandé son annexion par la Russie. L'opération était étrangement similaire au modèle de la guerre « nouvelle génération » présentée par les théoriciens russes. En outre, l'annexion rapide et sans effusion de sang de la Crimée orchestrée par la Russie est en grande partie le résultat d'une campagne de guerre de l'information de guerre bien préparée et exécutée. Sur le modèle de Bogdanov et Chekinov, l'opération de Crimée peut être divisée en deux phases, une phase préparatoire et une phase d'exécution, dont le succès a reposé sur une vaste campagne d'information de guerre.

2.1 Phase 1: L'établissement des Conditions d'une guerre de l'Information

Dans la première phase de l'opération, le premier objectif de la Russie était de mettre en place les conditions nécessaires pour le début d'une guerre de l'information en Crimée. En général, dans le but d'influencer une cible, une force doit être en mesure de livrer un message et la cible doit être en mesure de recevoir et de comprendre le message. Dans le cas de la Russie, la première phase de l'opération a consisté à 1) utiliser sa «politique étrangère à but humanitaire» pour permettre aux citoyens de l'Ukraine de comprendre les motivations des Russes et 2) utiliser le contrôle réflexif pour accroître le soutien en faveur de la culture et des politiques russes. La « politique étrangère à but humanitaire» de la Russie est similaire à la notion de «soft power» et vise à influencer d'autres Etats à travers la diffusion de la langue, de la culture et de l'idéologie russes. La région de Crimée a toujours été fortement influencée par la langue et la culture russes. En effet, plus de 60 pour cent de la population appartient à des ethnies d'origine russe et près de 90 pour cent de la population parle le russe.[25] En outre, à partir de 2007, la Russie a lancé une politique étrangère à but humanitaire pour accroître le soutien en faveur des russophiles en Ukraine et dans d'autres Etats ex-soviétiques.[26] Après 2007, la Russie a réexaminé sa politique étrangère et a créé un Conseil de coordination des compatriotes russes avec un budget de 400 millions de roubles. La mission de ce Conseil était de favoriser le soutien et la compréhension de la culture russe, et de diffuser des récits s'appuyant sur les points communs historiques et culturels entre les Russes et les Ukrainiens. Ils ont ainsi développé l'idée d'une civilisation orthodoxe slave et orientale unie ainsi que celle d'une Crimée propriété légitime de la Russie.[27] En 2009, 14 organisations non gouvernementales de compatriotes russes sont intégrées au sein de ce conseil.[28] Le Conseil de coordination pour les actions en Crimée a commémoré la célébration de la Journée de la Victoire comme une victoire capitale du peuple (non

[25] Juhan Kivirähk, et al., *The 'Humanitarian Dimension' of Russian Foreign Policy Toward Georgia, Moldova, Ukraine, and the Baltic States* (Riga: Centre for East European Policy Studies, 2010), 260.
[26] This Review recommended increasing the amount of foreign broadcasting of Russian state news agencies and expanding their offices abroad.
[27] Ibid, 257
[28] Ibid, 256.

soviétique) sur le fascisme. Il a également organisé le renforcement des relations avec l'Eglise orthodoxe ukrainienne et le Patriarcat de Moscou (UOC-MP) en organisant des camps d'été pour les jeunes intitulés « Our Home - Saint Rus » pour les scouts ukrainiens.[29] De plus, les centres culturels russes à travers l'Ukraine ont visé à accroître l'identité russe en Crimée en publiant des manuels russes, et en célébrant des jours tels que la Journée de la Russie, la Journée de Moscou, et le jour de la Réunification de la Crimée avec la Russie.[30]

Outre promotions globale de la culture russe le Conseil de coordination a mis en œuvre des mesures visant à améliorer la connaissance de la littérature russe. Au cours de la dernière décennie, la Russie a poursuivi sa coopération dans les domaines de l'éducation entre Russes et Ukrainiens. Les accords signés entre l'Ukraine et la Russie permettent aux citoyens des deux pays de créer des écoles soit russes soit ukrainiennes. Il y a 1.119 écoles publiques où la langue russe est enseignée et 1.755 écoles qui enseignent à la fois russe et ukrainien.[31] Ces efforts de la Russie ont permis à environ 50 pour cent des étudiants ukrainiens d'étudier le russe chaque année. Ce chiffre est particulièrement significatif au regard de l'ethnie russe qui ne représente que 17,5 pour cent de la population ukrainienne.[32]

Outre sa «politique étrangère à but humanitaire», la Russie a créé des infrastructures en terme de médias nécessaires pour diffuser ses messages. La présence de médias russes en Ukraine au moment de l'opération de Crimée était ainsi largement répandue. En 2008, sur les 45 programmes étrangers autorisés à diffuser sur les réseaux câblés ukrainiens, 37 étaient en russe.[33] Au moment de l'opération de Crimée, la presse écrite russe a également été largement diffusée en Ukraine. En 2007, les livres russes représentaient 38,7 pour cent de tous les livres publiés en Ukraine. En outre, 66,7 pour cent des journaux distribués en Ukraine étaient en russe.[34] La Russie a également créé une position dominante dans le domaine des réseaux sociaux. Par exemple, les deux plates-formes les plus populaires de réseaux sociaux en Ukraine sont les sites de réseaux sociaux russes *Vkontakte* et *odnoklassniki.ru*.[35] Par conséquent, dès le début des hostilités russes en Ukraine en 2014, la Russie avait un réseau de distribution de messagerie solidement implanté en Ukraine.

Un autre objectif de la Russie lors de la phase initiale de l'opération était de réduire le soutien du population ukranienne et Crimée au profit du gouvernement ukrainien. À cette fin, la Russie a

[29] Ibid.
[30] Ibid, 278.
[31] Ibid, 287.
[32] Ibid.
[33] Ibid, 293.
[34] Ibid, 297
[35] "Contemporary Media Use in Ukraine," Gallup – Broadcasting Board of Governors, accessed February 11, 2016, www.bbg.gov/wp-content/media/2014/06/Ukraine-research-brief.pdf.

tenté de 1) de discréditer le gouvernement ukrainien et 2) de créer un fossé entre les Ukrainiens d'origine russe et le gouvernement ukrainien. Ainsi, dans le but de discréditer le gouvernement ukrainien aux yeux des habitants de Crimée, la Russie a décrit le gouvernement de Kiev comme illégitime et incompétent. Les médias russes et les cyber «trolls» ont constamment parlé du renversement de Ianoukovytch mené illégalement par des éléments extrémistes. Par ailleurs, les médias russes ont créé chez les ukrainiens d'origine russe un sentiment d'anxiété et d'insécurité dans le domaine de la stabilité économique et politique. Afin de créer des dissensions entre le gouvernement ukrainien et les personnes d'origine russe, la Russie a utilisé un large éventail de capacités d'information de guerre, et a notamment utilisé le contrôle réflexif. La Russie a dépeint les manifestants Euromaïdan qui ont déclenché la chute du président ukrainien Viktor Ianoukovytch, et le nouveau gouvernement ukrainien comme fascistes et nazis. Par ailleurs, elle a utilisé la télévision, la radio et la presse écrite pour diffuser des analogies soigneusement construites qui comparaient le mouvement politique actuel en Ukraine à l'assaut nazi de la Seconde Guerre mondiale. Ainsi par exemple, les médias russes ont étiqueté le gouvernement ukrainien et ses soutiens comme «*banderovtsi*.» Ceci est une référence claire aux adeptes de Stepan Bandera, qui est un symbole de la Seconde Guerre mondiale, du nationalisme ukrainien mais considéré comme un collaborateur nazi par les Soviétiques.[36] Le contrôle réflexif russe et la guerre de l'information sont également illustrés par l'utilisation de « trolls » dans les réseaux sociaux pour diffuser des messages afin de créer des dissensions entre le gouvernement ukrainien et les Ukrainiens d'origine russe. Un « troll » russe du gouvernement a créé un faux compte Facebook en prenant l'identité d'un médecin ukrainien. Ce compte a été utilisé pour diffuser des histoires d'extrémistes ukrainiens brûlant des personnes appartenant à une ethnie russe vivant dans un bâtiment d'Odessa. Par la suite, les utilisateurs russes sur Vkontakte ont partagé ce message plus de 5000 fois dès le premier jour suivant la publication initiale.[37] Un autre compte fictif relatait le récit d'une femme d'origine ethnique russe enceinte étranglée par des extrémistes pro-ukrainiennes dans un bâtiment public Odessa et a été largement diffusé sur Twitter et Facebook.[38] Ce type de message visent à réduire le soutien pour le gouvernement ukrainien en diffusant une image négative de ce dernier et en le présentant comme un ramassis de fascistes extrêmes qui menacent la sécurité des ethnies russes, particulièrement en Crimée.

[36] "Analysis of Russia's Information Campaign Against Ukraine," NATO STRATCOM Center of Excellence, 2014, accessed February 18, 2016, http://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine.
[37] Ibid, 28.
[38] Ibid.

2.2 Phase 2: L'Isolement de Crimée

La deuxième phase de l'invasion de la Crimée par la Russie a commencé avec la mise en place des conditions d'information et le déploiement des «petits hommes verts» du Kremlin. Le premier objectif en termes d'information de la Russie au cours de cette phase était d'accroître l'incertitude dans le but de perturber la réponse du gouvernement ukrainien et de créer un sentiment de désespoir parmi la population ukrainienne. Afin d'atteindre cet objectif, le Kremlin a utilisé une vaste gamme d'outils militaires et non militaires. Ont été utilisées : la déception, les forces d'opérations spéciales, la propagande, la guerre électronique, la cyber-guerre et la diplomatie à deux niveaux. L'utilisation de *maskirovka* a permis une surprise totale pour l'intervention russe et produit consternation et incertitude parmi la population. La Russie n'a jamais déclaré ses intentions et a facilité le développement d'une atmosphère d'ambiguïté et d'incertitude au sein de l'Ukraine. L'Ukraine a été constamment confrontée à des informations paradoxales sur les événements qui se déroulaient en Crimée et qui visaient à créer de l'incertitude et de la peur. Par exemple, quelques jours après la chute de Viktor Ianoukovytch, les forces armées russes ont rassemblé 150.000 hommes appartenant à des troupes de combat à la frontière avec l'Ukraine. Cependant, le Kremlin a affirmé que ce nouveau déploiement de troupes était seulement pour des exercices de préparation et la plupart des médias mondiaux ont écarté l'idée d'une éventuelle intervention russe. Après le 17 mars, malgré la présence des uniformes russes, celle des « petits hommes verts» et la multitude de preuves photographiques et numériques montrant les troupes russes en Crimée, la Russie a continué à nier la présence de ses forces en Crimée. Ce n'est que le 17 mars, lors de sa session télévisée annuelle, que V.Poutine, a admis la présence des troupes russes aux portes de la Crimée. Ces paradoxes ont remis en question les perceptions des dirigeants ukrainiens et des citoyens, créant ainsi une atmosphère de peur, d'hésitation et de consternation.

La Russie a utilisé ses forces d'opérations spéciales pour exercer un contrôle réflexif en manipulant les perceptions et en perturbant la capacité de l'Ukraine à évaluer efficacement la situation, prendre une décision et apporter une réponse. Les Russes ont accompli cela en isolant le gouvernement ukrainien et les forces militaires et en inhibant leur prise de décision. La Russie a perturbé le processus local de décision en permettant la saisie du parlement de Crimée par les «Little Green Men» représentant en réalité le KSO russe (Special Operations Command) et la Naval Infantry Marines.[39] Comme l'affirme Mark Galleotti, « the lack of insignia on these 'little green men' and Moscow's flat denial that they were Russian troops was enough to inject a moment's uncertainty into

[39] Galeottii, Mark, "'Hybrid War' and 'Little Green Men': How it Works, and How it Doesn't," 3.

the calculations in both Kiev and NATO. »[40] Dans le même temps, l'armée russe a appuyé des manifestations apparemment spontanées qui ont abouti à la prise d'autres bâtiments de l'administration publique, des médias, et des infrastructures critiques. Ces actions ont empêché le partage et la diffusion de l'information qui s'imposait au regard de la situation par les autorités ukrainiennes. L'exécution de la guerre électronique par les russes et le sabotage organisé des communications ont permis la destruction des nœuds clés de communication.[41]

L'utilisation sophistiquée du contrôle réflexif par la Russie apparait également évidente dans le domaine de la prise de décision au niveau national. Les «petits hommes verts» et d'autres manifestants russes ont organisé le blocus qui a finalement permis la remise des 190 bases militaires ukrainiennes sans qu'un coup de feu ne soit tiré. Cette situation a été aggravée par le degré de corruption de certains dirigeants politiques et militaires ukrainiens qui ont manifesté leur fidélité au Kremlin. La surprise totale de l'intervention imprévue des «petits hommes verts» partout en Crimée et l'isolement de cette dernière, associée à l'atmosphère déjà perturbée dans le gouvernement ukrainien nouvellement installé, a empêché toute réponse cohérente de Kiev. L'utilisation du contrôle réflexif par les russes et l'application des 4D par le Kremlin (*dismiss*, *distort*, *distract*, *dismay*) ont augmenté l'incertitude chez la population ukrainienne. Les médias russes ont présenté une réalité factuelle faussée et différente de celle présentée par les médias occidentaux.

Le média contrôlé par le gouvernement russe est un géant doté d'un budget de 300 millions de dollars qui diffuse continuellement des messages dans le but d'accroître l'incertitude et les informations fausses. Alors que l'Ukraine fait référence à une armée mystérieuse composée de «petits hommes verts» qui veulent se saisir des biens du gouvernement, les médias russes ont renvoyé de cette armée une image de «gens sympathiques» qui étaient «à l'écoute des civils. »[42] Les Russes ont réalisé des interviews dans les médias avec l'intervention d'habitants de Crimée, qui étaient en réalité des acteurs payés, afin de dépeindre le gouvernement ukrainien comme une menace et les soldats russes en Crimée comme une bénédiction. Le titre en première page de Lifenews.ru, un tabloïd en ligne pro-Kremlin a déclaré: « Oddessans ask Putin to save them from the terror of the Euromaidan. »[43] De même, la Russie a diffusé des images de personnes en prétendant qu'il s'agissait de personnes fuyant prétendumment l'Ukraine pour la Russie alors qu'il s'agissait d'images d'un simple passage de la frontière ukraino-polonaise. Par ailleurs, l'agence d'Etat russe ITAR-TASS a

[40] Ibid, 4.
[41] Racz, 61
[42] Kenneth Geers, "Introduction: Cyber War in Perspective," In *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 90.
[43] Michael Calderon and Luke Johnson, "Russia Wages Media War Alongside Crimea Invasion," Huffington Post, March 3, 2014, accessed March 2, 2016, http://www.huffingtonpost.com/2014/03/03/russia-media-crimea-invasion_n_4890800.html.

cité le service des frontières qui aurait déclaré qu'il y avait des signes d'une « catastrophe humanitaire. »[44]

La Russie a également utilisé la guerre cybernétique pour isoler la Crimée et se prémunir d'une réponse ukrainienne efficace. Même avant la détérioration rapide des relations entre l'Ukraine et la Russie, cette dernière avait déjà pris pour cible des politiciens ukrainiens depuis 2010 et avait infecté leurs appareils électroniques avec des malware.[45] La Russie a ainsi utilisé la guerre électronique et le sabotage dans le but de perturber la communication ukrainienne et leur capacité à répondre à des événements sur le terrain. Dans les premières étapes de l'opération, la Russie a réussi à obtenir la grille des télécommunications de la Crimée et a brouillé les communications militaires ukrainiennes par une coupure des câbles et un re-routage des appels par le biais des opérateurs russes. Ukrtelecom a découvert que ses câbles à fibres optiques ont été sabotés tandis qu'au début du mois de Mars 2014 ses bureaux ont été saisis par les troupes russes.[46] Autre exemple, alors que les troupes russes s'infiltraient en Crimée, les pirates russes fermaient le site Web du gouvernement ukrainien et piratait les téléphones cellulaires des politiciens ukrainiens.[47] La véritable efficacité de la guerre de l'information ciblée contre le gouvernement ukrainien et la population ukrainienne est difficile à mesurer, mais il est indéniable que la campagne a réussi à diminuer la perception de la réalité de la situation par les dirigeants ukrainiens et à perturber le cycle de prise de décision. L'analyste militaire ukrainien Dmitry Tymchuk a fustigé le gouvernement intérimaire ukrainien pour son manque de clairvoyance et pour sa lenteur dans les prises de décision. Les membres du Parlement ukrainien se sont plaints que les troupes ukrainiennes n'ont pas reçu les consignes en temps opportun sur les règles appropriées d'engagement.[48]

Un autre des objectifs de la Russie au cours de cette phase était de diminuer le soutien externe de l'Ukraine afin d'empêcher une intervention de l'OTAN ou des États-Unis jusqu'à ce qu'il soit trop tard. La Russie a façonné le récit des événements en Ukraine afin de changer la perception occidentale des événements de Crimée. Elle a utilisé une variété d'outils, y compris des « trolls » contre les médias et les déclarations du gouvernement. La Russie a également poussé les médias russes à exercer un contrôle réflexif pour manipuler le récit des événements en Crimée. Au cours des premières étapes de l'intervention, la Russie a tenté de contrer le récit occidental qui la présentait comme l'«agresseur russe» et a cherché à présenter le conflit comme un renversement illégal de

[44] Ibid.
[45] Geers, 90.
[46] Ibid, 91.
[47] "Ukraine says communications hit, MPs phones blocked. " Reuters, March 4 2014, accessed February 22, 2016, http://www.reuters.com/article/2014/03/04/ukraine-crisis-cybersecurity-idUSL6N0M12CF20140304.
[48] Geers, 92.

Ianoukovytch par des forces extrémistes, agitant l'image d'une guerre civile ayant pour objectif la suppression des ethnies russes. Après la justification donnée par V. Poutine indiquant que les forces russes déployées en Ukraine étaient des forces d'«auto-défense», la Russie a tenté de présenter les faits comme une intervention justifiée selon le droit international. Le Kremlin a assuré que les responsables des ethnies russes en Crimée ont officiellement demandé l'aide russe, ce qui a donné à la Russie des motifs juridiques pour intervenir en vertu de la Stratégie de Sécurité de l'Etat Russe de 2009.[49] Avant l'annexion, la Russie a assuré que la Crimée avait organisé un vote pour l'indépendance et elle a dépeint la situation en Crimée comme analogue à celle du Kosovo qui avait reçu l'appui de l'OTAN pour son autodétermination. Ces actions sont en accord avec l'argumentation de Berzins selon laquelle la stratégie d'information de la Russie en Crimée avait pour objectif de créer un voile de légalité sur ses actions.[50]

Au cours de la guerre de Crimée, la Russie a révélé l'utilisation des « cyber trolls » sur le grand public, les médias et les sites de réseaux sociaux, ce qui démontre une nouvelle facette de ses capacités en matière de guerre de l'information. Le principal acteur de cette campagne d'information a été l'agence de recherche sur Internet du gouvernement russe, Agentsvo Internet Isledovaniy. Cet organisme, doté d'un budget de 19 millions de dollars, a employé plus de 600 personnes pour créer de faux comptes sur Facebook et Twitter et poster des commentaires qui ont soutenu les objectifs d'information du gouvernement russe et façonné la réalité des faits aux yeux des populations occidentales.[51] Situé dans un bâtiment non identifié à la périphérie de Moscou, ces « trolls » ont travaillé en équipe et par période de douze heures pour attaquer les sites qui dépeignaient négativement la Russie et essayaient de contrer le récit pro-russe. Essayant de changer la perception par les populations des États-Unis et de l'OTAN, la Russie a également utilisé les déclarations militaires agressives pour créer un sentiment agressif de la force. Les survols de l'espace aérien par les pays de l'OTAN et les affirmations exagérées de la force militaire russe ont été des outils utilisés par le Kremlin. En outre, la Russie a usé de déclarations inquiétantes, comme celle faite par Dmitri Kiselyov, chef de la nouvelle organisation appartenant à l'Etat *Rossiya Sogodnya*, qui a averti que la Russie était le seul Etat qui pourrait transformer les États-Unis en « radioactive dust ». [52]

---

[49] "Analysis of Russia's Information Campaign Against Ukraine," NATO STRATCOM Center of Excellence, 2014, accessed February 22, 2016, http://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine, 24.
[50] Janis Berzins, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy", National Defense Academy of Latvia Center for Security and Strategic Research, 2014, accessed November 18, 2015, , 3
[51] Max Seddon, "Documents Show How Russia's Troll Army Hit America," *Buzzfeed*, June 2, 2014, accessed February 22, 2016, http://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america#31fidzl.
[52] Maria Tadeo, "State Television Reporter Warns Russia Could 'Turn US Into Radioactive Dust,'" *The Independent*, March 17, 2014, accessed February 18, 2016, http://www.independent.co.uk/news/world/europe/state-television-presenter-warns-russia-could-turn-the-us-into-radioactive-dust-9197433.html.

3. L'avenir de la Guerre de l'Information Russe et les implications pour l'OTAN

Les événements de Crimée permettent de tirer trois leçons importantes.

Tout d'abord, la Crimée a démontré l'efficacité russe à utiliser l'information dans le déroulement d'une guerre hybride. Le théâtre de la Crimée a offert à la Russie les conditions idéales pour tester ses capacités dans le domaine de la guerre de l'information. En effet, la Crimée était déjà la base de la flotte russe en mer Noire et de la 810ème brigade d'infanterie navale.[53] De plus, les forces militaires ukrainiennes en Crimée ont fourni, en majorité, les personnels de soutien et les troupes de première ligne. Or, la population locale, constituée pour une large part d'ethnies Russes, avait souffert des décennies de négligence et de mauvaise gouvernance par l'Ukraine.[54] Dans ce contexte, les opérations d'influence russes ont réussi à créer un fossé entre la population de Crimée et Kiev. Cela a conduit à des défections individuelles ou de bases militaires ukrainiennes entières et cela a empêché l'intervention de l'OTAN ou celle des États-Unis à temps. La Russie a été en mesure d'isoler rapidement la Crimée de l'Ukraine et de maîtriser les forces militaires ukrainiennes en Crimée. Cela a permis également l'organisation d'un référendum sur l'indépendance de la Crimée pour légitimer l'annexion, et enfin d'annexer officiellement la Crimée. Bien que la Crimée ait été un succès extraordinaire et illustre la nouvelle guerre russe, les opérations qui ont suivi dans l'Est de l'Ukraine ont montré que sa mise en œuvre demandait un travail dans la durée.

De surcroît, la première étape de l'opération de la Russie en Crimée, à savoir l'établissement d'un terreau favorable aux opérations d'informations avant même l'usage de la force, démontre la volonté et la capacité de la Russie à mener une guerre d'information efficace contre les anciens Etats de l'URSS Etats mais aussi contre les pays de l'OTAN. La Russie continuera de perfectionner son utilisation des techniques de guerre de l'information dans le cadre des guerres de nouvelle génération. Ainsi, les États de l'ex-URSS, constitués de populations ethniques russes importantes, sont particulièrement vulnérables à l'influence russe et sont des cibles faciles des campagnes d'information russes. Dans les pays Baltes, le Kremlin est en train d'effectuer un effort important pour influencer les grandes populations ethniques russes afin de susciter des scissions avec les gouvernements et de préparer les conditions propices à des opérations futures. Les autorités lettones ont signalé plusieurs programmes russes ayant pour objectifs de créer des conditions d'information favorables, y compris par la délivrance de passeports russes à des ethnies Russes vivant en Lettonie. Ils soutiennent également un mouvement pour faire du russe la deuxième langue officielle de la

[53] Galeotti,3.
[54] Ibid.

Lettonie, la collection les atmospherics et l'intelligence du frontière letton[55] Ailleurs en Europe, la Russie développe ses réseaux d'influence à travers le financement de partis politiques de droite et d'extrême-droite, et de partis de différents pays d'Europe occidentale anti européens. La Russie utilise également le contrôle réflexif en propageant des « récits » dans les médias européens dans le but d'affaiblir les leaders actuels et de renforcer l'extrême-droite. Ces « récits » sont diffusées à travers les infrastructures médiatiques russes qui sont bien établies en Europe. Ces histoires sont souvent relayées dans les journaux traditionnels et il est difficile de distinguer les messages russes des techniques de contrôle réflexif. Par exemple, en France, "La Russie d'Aujourd'hui" est un supplément pro-russe qui est publié chaque mois dans Le Figaro et apparaît comme un article indépendant du journal.[56] La Russie cible particulièrement Angela Merkel pour sa perception anti-Kremlin. Selon le Monde "Merkel est un chef de file à la tête des Etats européens qui s'opposent à l'annexion de la Crimée et qui impose des sanctions à la Russie en raison du conflit meurtrier dans l'Est de l'Ukraine."[57] Au vue de sa réussite, le système d'information Russe ne peut que continuer de fonctionner dans tout le spectre des conflits, de la paix à la guerre. Le centre de gravité des efforts russes oscillant selon les circonstances entre la guerre et la paix, ce que le général américain et commandant de l'US Special Operations Command (USSOCOM) Joseph Votel a appelé «la zone grise ».

Troisièmement, le cadre juridique et institutionnel actuel de l'OTAN s'avère incapable de répondre efficacement au type de guerre rencontré en Crimée. L'article 5 du Traité de l'OTAN stipule que «Les parties conviennent qu'une attaque armée contre l'une ou plusieurs d'entre elles survenant en Europe ou en Amérique du Nord sera considérée comme une attaque dirigée contre toutes les parties. » L'annexion russe de la Crimée n'a entraîné aucun incident ni aucun coup de feu. Selon la Russie, les événements en Crimée constituaient tout simplement un mouvement spontané d'auto-détermination dans la même veine que le Kosovo. En réalité, l'action des russes en Crimée n'était pas une attaque armée mais un type de guerre de nouvelle génération qui reposait sur une campagne d'information bien préparée, dimensionnée et menée. Toutefois, si une opération comme celle-ci visait un membre de l'OTAN, par exemple un pays comme l'Estonie, comment pourrait être invoqué l'article 5 de l'OTAN et la défense d'un membre qui ne serait pas touché par une agression armée ? Quel genre de réponse pourrait adopter l'OTAN ? L'OTAN doit faire face à ces types de questions afin d'éviter que se répète la paralysie observée en Crimée.

---

[55] Berzins,. 7.
[56] Daniel Kochis, "Countering Russian Propaganda Abroad," *Heritage Foundation Issue Brief # 4286*, October 21, 2014, accessed January 18, 2016, http://www.heritage.org/research/reports/2014/10/countering-russian-propaganda-abroad.
[57] "L'offensive médiatique russe vise l'Europe," *Le Monde*, February, 12, 2016.

3.1 Reorienting Influence in the Gray Zone

Ces observations démontrent la nécessité de re-conceptualiser guerre de l'information au sein de l'OTAN. L'opération de Crimée a démontré l'incapacité de l'OTAN à répondre à un acte d'agression dans le cadre d'une guerre de nouvelle génération - un conflit qui est non déclaré, clandestin, évite l'effusion de sang, et repose sur une campagne massive d'information de guerre. Plus important encore, la Crimée a démontré l'incapacité de l'OTAN à réagir et à mener sa propre campagne d'information de la guerre dans la «zone grise» qui, selon le commandant des opérations de commandement général spécial américain Joseph Votel,

> « *Se caractérise par une intense concurrence politique, économique, informationnelle, militaire qui dépasse de beaucoup les relations diplomatiques traditionnels »* [58]

La guerre froide était un conflit long, qui s'est traduite notamment par une série de guerres par procuration. La guerre froide a vu des affrontements tant dans le domaine, politique, militaire, de l'information et économique. L'environnement de sécurité actuel indique que l'OTAN devra faire face à de multiples conflits au sein de la zone Grise, contre la Russie, ainsi que d'autres acteurs. Le Premier ministre russe Medvedev, prenant la parole à la Conférence de Munich sur la sécurité en février 2016, a estimé que la relation actuelle entre l'OTAN et la Russie ressemble à "une nouvelle guerre froide."[59] Dans cette zone de conflit, entre la guerre et la paix, l'OTAN n'a actuellement pas la capacité de mener des opérations d'information dans la durée pour contrer l'agression.

Pour contrer les campagnes russes de guerre de l'information sur le long terme et se préparer à des conflits modernes où l'influence constitue un effet de levier complexe et sophistiqué, l'OTAN doit développer sa doctrine et sa capacité de mener des opérations d'information dans la zone grise. Tout d'abord, l'OTAN doit avoir la volonté de contrer l'information russe contre l'OTAN et ses membres. L'OTAN doit reconnaître les actions russes pour ce qu'elles sont : une guerre de l'information dans la durée. De nombreux pays d'Europe orientale ont été la cible d'influence maligne russe depuis des décennies, et ce n'est que récemment que l'OTAN a vraiment apprécié la portée de l'information russe de guerre. L'OTAN doit aussi reconnaître la présence omniprésente de contrôle réflexif russe. La guerre moderne de l'information implique un réseau complexe de leviers militaires et non-militaires d'influence, et chacun de ces leviers peut être utilisé pour exercer un contrôle réflexif. Afin de décoder et de répondre à des stratégies d'information de guerre russes, l'OTAN et

---

[58] Joseph L. Votel, Charles T. Cleveland, Charles T. Connett, and Will Irwin. "Unconventional Warfare in the Gray Zone," Joint Force Quarterly 80 (2016): 102.

[59] "Russian PM Medvedev Says New Cold War is On," *BBC*, February 13, 2016, accessed February 14, 2016, http://www.bbc.com/news/world-europe-35569094.

ses membres doivent être en mesure d'abord de reconnaître une action de contrôle réflexif. Outre cette détection et cette caractérisation, l'OTAN doit également développer sa doctrine, ses formations, ses techniques et ses procédures pour lutter contre l'influence russe dans la « zone grise». Cela signifie que l'OTAN et ses Etats doivent élaborer une doctrine de l'influence qui est commune et inter-agences, et qui met en œuvre tous les outils militaires et non-militaires de ses Etats membres pour lutter contre la guerre de l'information russe menée par la Russie chaque jour contre l'OTAN et de ses membres.

3.2 « L'Influence Persistante »

La communauté de l'Influence de l'OTAN a fait des progrès significatifs dans le développement de la doctrine pour combattre l'influence dans la zone grise. Afin de contrer les menaces posées par exemple par la guerre russe hybride, mais également la guerre sans restriction de la Chine, et la guerre asymétrique iranienne, l'US Special Operations Command (USSOCOM) élabore une doctrine fondée sur la « guerre politique». D'abord conceptualisée par George Kennan en 1948, USSOCOM envisage la guerre politique comme la mobilisation de l'ensemble du gouvernement qui peut «contrer et décourager la guerre asymétrique et hybride employée par nos adversaires étatiques et non étatiques à la fois pendant la« guerre » et le temps de « paix »à travers tout le spectre des conflits.[60] Cette approche conceptualise une approche globale politique qui est caractérisé par l'unité d'effort et de but, et qui utilise tous les outils visibles et invisibles à la disposition des États. Cette guerre politique comprend non seulement des opérations d'influence et d'information[61], mais aussi l'engagement diplomatique, la guerre économique, la, « security sector assistance » (SSA), et diverses formes d' « Unconventional Warfare » (UW).[62] Dans le domaine des activités d'information et d'influence, cette guerre a pour but de consolider les relations au sein des Etats entre les partenaires, de diminuer l'efficacité des actions adverses, d'empêcher la propagation de ces actions à des pays voisins ou tiers, de limiter la légitimité et la crédibilité du gouvernement adverse agresseur.

Un concept américain nouvellement développé vise à contrer les actions adverses sur le long terme vues sous un prisme particulier, celui du :« Cognitive Joint Force Entrée » (CJFE). Le CJFE "synchronise et emploie toutes les composantes de l'environnement mondial de l'information en vue de mener des activités d'information et d'influence pour façonner l'environnement dans les étapes de

---

[60] "SOF Support to Political Warfare," United States Army Special Operations Command White Paper, 10 March 2015, accessed February 8, 2016, http://smallwarsjournal.com/blog/sof-support-to-political-warfare, 10.
[61] *FM 3-13: Inform and Influence Operations*, 25 January 2013, 1-1.
[62] "SOF Support to Political Warfare," 11.

pré-conflit."[63] Ce concept pourrait lutter efficacement contre la guerre de l'information persistante russe menée dans de nombreux Etats ex-soviétiques, ainsi que façonner l'environnement de l'information dans d'autres pays. Ce développement par les Etats-Unis de ce concept répond à un besoin marqué doctrinaire de guerre de l'information dans un environnement hybride. Cependant, au niveau de l'OTAN, l'essence de cette doctrine de « guerre politique » doit être adopté et mis en oeuvre pour contrer le contrôle réflexif russe et défendre ses membres contre la guerre hybride.

3.3 Prennant l'Offensive Contre L'Adversarie

Actuellement, la doctrine de l'influence de l'OTAN est inscrite au sein de l'AJP-3.10, un manuel de guerre classique qui ne propose pas une approche globale de lutte contre l'influence maligne ou hybride et les menaces persistantes.[64] Pour contrer les campagnes de désinformation comme celles mises en œuvre par la Russie en Crimée, les Etats de l'OTAN ont commencé à essayer de sensibiliser le public à la désinformation russe et au contrôle réflexif. Par exemple, le Département d'Etat américain publie des mensonges russes ou des manipulations de l'information dans un document intitulé « Fiction Président Poutine: 10 fausses déclarations sur l'Ukraine. »[65] Bien que cette stratégie «*name and shame*» peut sensibiliser la population à des campagnes de désinformation et d'influence persistantes russes, il n'a pas d'action sur les idées, les attitudes ou les croyances des populations de la Russie ou des pays qu'il vise. Afin de contrer l'influence maligne dans les pays visés par les agresseurs, et de cibler les populations des agresseurs eux-mêmes, la doctrine de l'OTAN doit d'abord se concentrer sur la l'influence «phase 0 », qui peut répondre à l'influence russe persistante dans les pays de l'OTAN et être prêt à contrer l'influence maligne dans un guerre hybride.

La Russie maîtrisé la combinaison des opérations d'information : clandestines, secrètes, et de l'action militaire conventionnelle. Comme Peter Pomerantsev a souligné dans son article, «Unplugging Putin TV, » comprendre comment Poutine a été en mesure de tisser la guerre hybride, de créer des récits, et de la désinformation dans une réalité virtuelle est la première étape dans la conception d'une réponse appropriée.[66] Alors que les États-Unis et d'autres pays de l'OTAN limitent l'information secrète ou clandestine ciblant la population ou les décideurs adverses dans les zones de

---

[63] Ibid, 24.
[64] AJP-3.10 : Allied Joint Doctrine for Information Operations. 24 June 2015.
[65] Department of State, "President Putin's Fiction: 10 False Claims About Ukraine," Fact Sheet, Office of the Spokesperson, Washington DC, March 5, 2014, accessed November 8, 2015, http://www.state.gov/r/pa/prs/ps/2014/03/222988.htm
[66] Peter Pomerantsev, "Unplugging Putin TV," Foreign Affairs, February 19, 2015, accessed March 31, 2016, https://www.foreignaffairs.com/articles/russia-fsu/2015-02-18/unplugging-putin-tv.

conflit, a contrario, la Russie utilise agressivement ces mêmes tactiques contre les populations générales et les dirigeants dans les pays à travers le monde. L'OTAN et ses Etats membres doivent développer une capacité similaire qui peut contrer l'influence maligne persistante et cibler les populations des pays agresseurs eux-mêmes.

3.4 Une Nouvelle Doctrine Pour Une Nouvelle Environnement de l'Information

La communauté des opérations d'information de l'OTAN doit également s'adapter aux technologies contemporaines de l'environnement de l'information. Alors que des dépliants, des prospectus, et la messagerie radio sont souvent le moyen le plus efficace d'influencer les publics cibles difficiles d'accès en Afghanistan ou en Irak, l'influence des combats qui font rage en Ukraine et en Europe orientale sont relayés sur l'Internet, les médias sociaux, et les plates-formes de diffusion de télévision. L'OTAN doit pouvoir s'approprier cette haute technologie comme le font la Russie ou l'Etat islamique et faire évoluer leur approche méthodologique et de la doctrine afin d'influencer sur les plates-formes de médias modernes. Les équipes d'influence doivent être formées et équipées pour exécuter des opérations d'information sur les médias sociaux et l'Internet, et dépasser la question juridique des «débordements». Les opérations sur les médias sociaux doivent inclure les opérations psychologiques secrètes pour contrer les trolls employés par les acteurs étatiques et non étatiques, comme la Fédération de Russie. C'est seulement en exécutant sur le long terme et avec une grande envergure, une campagne d'opérations d'information sur les médias Internet et sociaux que l'OTAN sera en mesure d'atteindre efficacement ses publics cibles et contrer les influences malignes.

La communauté « influence » de l'OTAN doit aussi changer son approche méthodologique et se concentrer l'influence à long terme, sur la création de plates-formes durables de médias capable d'agir dans la durée, comme pour la Russie, les médias : *la Russie Aujourdhui* ou *Sputnik*, mais également de construire des campagnes d'influence autour de plusieurs produits (dépliant, message radio, émission de télévision) visant à modifier un comportement ou une attitude dans un groupe spécifique de personnes. Aujourd'hui, de tels produits existent mais ne sont diffusés que sur des périodes courtes : semaines ou mois. Cela ne permet pas de construire un auditoire stable ou d'optiiser l'influence. Par conséquent, l'OTAN doit apporter des modifications pertinentes à la doctrine et à la formation qui permettent le développement sur le long terme de plates-formes adaptées à la cible et alternatives.

Ces derniers mois, il y a eu des discussions importantes autour de l'établissement d'une station de télévision européenne en langue russe capable de contrer les messages provenant de sources telles

que *la Russie Aujourdhui*.[67] En outre, la télévision et radio allemande *Deutsche Welle* lance un nouveau service en langue anglaise appelé *DWNews* qui vise spécifiquement à contrer la propagande russe.[68] De plus, les populations européennes sont plus ou moins réceptives aux messages véhiculés par *la Russie Aujourdhui* ou *Sputnik*,. Des objections sont particulièrement fortes dans des pays comme l'Allemagne, qui conservent toujours en mémoire la propagande nazie, ou la France, dont l'utilisation de la propagande en Algérie durant les années 1950, résonne toujours. Par conséquent, au lieu d'essayer de copier les stratégies mises en place par les médias adverses, l'OTAN devrait se concentrer sur la lutte contre l'information adverse en développant des médias pertinents dans les zones moins compétitives. Peter Pomerantsev suggérait ainsi à la possibilité d'utiliser des programmes de télévision de divertissement comme une plate-forme d'influence sur sa population. Cela serait un moyen efficace d'influencer les Russes. La télévision russe, en plus des stations d'actualité continue, diffuse des spectacles de talent, des sitcoms addictifs et de la musique. Il démontre comment saisir l'attention de publics cible en s'appuyant sur des thèmes comme la théorie de la conspiration, des thèmes anti-occidentaux, et des thèmes nationalistes. Pomerantsev fait valoir que les émissions de divertissement adaptées à la langue et la culture russe seraient extrêmement efficaces pour influencer les publics cibles russes.[69] Les programmes de télévision, tels que la télé-réalité (Survivor) pourraient dénoncer les gouvernements adverses. Pour être efficaces, ces types de plates-formes d'influence doivent avoir des horizons à long terme et des messages professionnellement et subtilement conçus. Comme Pomerantsev souligne, Poutine contrôle la télévision russe et maintient des taux d'approbation interne de plus de 80 pour cent.[70] Par conséquent, toute plate-forme de médias doit élaborer ses messages subtilement, de sorte qu'ils soient imperceptibles dans un programme plus vaste. Ce type d'opération d'influence à long terme a été réalisé par les Alliés pendant la seconde guerre mondiale et est décrite par Selfton Delmer in *Black Boomerang*.[71] Ce livre décrit les stations de radio de propagande noires dirigées de la Grande-Bretagne (PWE), spécifiquement Gustav Siegfried Eins et Soldatensender Calais. Ces stations de radio de langue allemande ont été mis en oeuvre par la Grande-Bretagne en Allemagne dans le cadre de la guerre psychologique contre les programmes nationalistes allemands apparemment

---

[67] Cdr (R) Steve Tatham, "The Solution to Russian Propaganda is not EU or NATO Propaganda ut Advanced Social Science to Understand and Mitigate its Effects in Targeted Populations," National Defence Academy of Latvia, July 2015, http://www.stratcomcoe.org/steve-tatham-solution-russian-propaganda-not-eu-or-nato-propaganda-advanced-social-science, accessed February 26, 2016, 8.

[68] Chase Gummer, "Germany Faces Tricky Quest Countering Russian Propaganda," January 28, 2015, accessed March 31, 2016, http://www.wsj.com/articles/germany-faces-tricky-quest-countering-russian-propaganda-1422443056.

[69] Peter Pomerantsev, "Unplugging Putin TV," *Foreign Affairs*, February 19, 2015, accessed March 31, 2016, https://www.foreignaffairs.com/articles/russia-fsu/2015-02-18/unplugging-putin-tv.

[70] Ibid.

[71] Selfton Demler, *Black Boomerang*, (New York, The Viking Press, 1962).

irréductibles. Afin de s'adapter à l'environnement de l'information actuelle et contrer les menaces présentées par les Etats comme la Russie, les Etats membres de l'OTAN doivent engager des efforts de fonds pour le développement de ce type de programmes à long terme.

4. Conclusion

Au cours de la dernière décennie, les Etats-Unis et l'OTAN ont développé une capacité importante dans la lutte contre les menaces irrégulières représentées par des acteurs non-étatiques, par les insurgés et les organisations terroristes. Au cours de ces dernières années, de nouveaux défis sont apparus avec des États tels que la Russie qui ont combiné les menaces irrégulières nouvelles avec les moyens de la force conventionnelle. La forme moderne de la guerre que les acteurs comme la Russie ont adoptée est plus efficace en <<Gray Zone>> qui représente la partie du spectre des conflits entre la guerre et la paix. La <<Gray Zone>> permet aux acteurs d'exécuter des guerres hybrides non déclarées qui ne répondent pas à la définition traditionnelle de la guerre conventionnelle. Elle permet également de mener une forme de guerre durable qui intègre étroitement les domaines politique, économique, d'information et l'agression militaire contre un Etat ciblé. Cette guerre hybride moderne repose en particulier sur l'emploi d'une guerre de l'information destinée à mettre les pays cibles à genoux.

La pratique par la Russie de cette guerre hybride appelée « New Generation Warfare » illustre cette nouvelle forme de guerre. La conceptualisation de la guerre de nouvelle génération est le résultat direct de l'évolution de la théorie géopolitique russe depuis la chute de l'Union soviétique. En outre, le centre de gravité de la guerre de nouvelle génération, c'est-à-dire la guerre de l'information, est directement issu de la *spetspropaganda* soviétique, de la *maskirovka*, et du contrôle réflexif.

Les événements de Crimée permettent à l'OTAN de tirer trois leçons essentielles. Tout d'abord, la Crimée a démontré l'efficacité des capacités russes dans le domaine de la guerre d'informations menée lors d'une guerre hybride. La Crimée a offert à la Russie les conditions idéales pour tester cette guerre de l'information avec des capacités de nouvelle génération. L'invasion et l'annexion de la Crimée par la Russie démontrent le rôle capital de la guerre de l'information dans la guerre de nouvelle génération.

Les capacités développées par la Russie dans le domaine de l'information lui permettent de fixer les conditions et de connaitre l'environnement nécessaire à ses actions avant le début des hostilités. Pendant l'invasion, la Russie a utilisé la guerre de l'information pour isoler le gouvernement ukrainien de son propre peuple et empêcher une intervention ou une assistance de l'OTAN ou des États-Unis en faveur de l'Ukraine. En conséquence, la guerre de nouvelle génération a permis à la Russie de remplir les objectifs stratégiques de la Russie, à savoir : obtenir une victoire

en Crimée, l'extension d'une zone pro-russe plus à l'ouest en Ukraine, accroitre la perception de la force russe en Europe de l'Est, dans les pays baltes, et au Caucase.

En outre, la première étape de l'opération menée par la Russie en Crimée, c'est-à-dire la mise en place de conditions favorables à l'obtention de renseignements au cours des années précédant l'usage de la force, démontre la volonté et la capacité de la Russie à mener une guerre d'information permanente contre les États de l'ex URSS et contre l'OTAN.

Enfin, le cadre juridique et institutionnel actuel de l'OTAN est incapable de répondre efficacement au type de guerre mené en Crimée. Afin de répondre à ces nouveaux défis que représente la guerre d'information menée par la Russie, l'OTAN et les États-Unis doivent développer une doctrine, des capacités de manœuvre coordonnées ainsi qu'une campagne de protection des informations pour protéger ses membres contre les futures guerres de nouvelle génération menées par la Russie : les guerres de l'information.

Bibliographie

Berzins, Janis, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy", National Defense Academy of Latvia Center for Security and Strategic Research, 2014, accessed November 18, 2015, http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx,

Burbridge, Dean, "Employing U.S. Information Operations Against Hybrid Warfare Threats", U.S. Army War College Strategy Research Project, March 2013, accessed November 4, 2015, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA589058 .

Calderon, Michael and Johnson, Luke, "Russia Wages Media War Alongside Crimea Invasion," Huffington Post, March 3, 2014, accessed March 2, 2016, http://www.huffingtonpost.com/2014/03/03/russia-media-crimea-invasion_n_4890800.html.

Chekinov, S.G. and Bogdanev, S.A., "Asymmetrical Actions to Ensure Russia's Military Security," *Military Thought* 3 (2010).

Chekinov, S.G. and Bogdanov, S.A., "The Nature and Content of a New-Generation War," *Military Thought* 4 (2013).

Coalsen, Robert, "Top Russian General Lays Bare Putin's Plan for Ukraine," The world Post, February 9, 2014, accessed 18 November 2015, http://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html

Cohen, Ariel., Robert E Hamilton, and Army War College (U.S.). Strategic Studies Institute. *The Russian Military and the Georgia War: Lessons and Implications* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011).

Connell, Mary, "Russia's "Ambiguous Warfare and Implications for the U.S. Marine Corps ", *CNA Analysis & Solutions*, May 2015, accessed October 18, 2015, https://www.cna.org/CNA_files/PDF/DOP-2015-U-010447-Final.pdf.

Darczewska, Jolanta, "The Anatomy of Russian Information Warfare", *OSW Centre for Eastern Studies Point of View*, May 2014, accessed November 14, 2015, http://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study.

Francke, Ulrik. "War by Non-Military Means: Understanding Russian Information Warfare," FOI Swedish Defense Research Agency, December 3, 2015, accessed February 14, 2016, http://www.foi.se/en/Top-menu/Pressroom/News/2015/War-by-Non-Military-means/

Galeotti, Mark, " 'Hybrid War' and 'Little Green Men' : How it Works and How It Doesn't," *E-International Relations*, April 16, 2015, accessed 18 November 2015, http://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/.

Galeotti, Mark, "Time to Think About Hybrid Defense," *War on the Rocks*, July 2015, accessed October 25, 2015, http://warontherocks.com/2015/07/time-to-think-about-hybrid-defense/

Geers, Kenneth, "Introduction: Cyber War in Perspective," In *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015).

Hoffman, Frank. *Conflict in the 21st Century : The Rise of Hybrid Wars* (Virginia, Potomac Institute for Policy Studies, 2007).

Kivirähk, Juhan; Maliukevičius, Nerijus; Kondratenko, Dmytro; Yeremeev, Olexandr; Vrabie, Radu; Devdariani, Nana; Tsatsanashvili, Miriam; Bachiashvili, Nato; Pkhaladze, Tengiz; Pelnēns, Gatis; Kudors, Andis; Paparinskis, Mārtiņš; Dimants, Ainārs;,Lerhis, Ainārs. *The 'Humanitarian Dimension' of Russian Foreign Policy Toward Georgia, Moldova, Ukraine, and the Baltic States*. (Riga: Centre for East European Policy Studies, International Centre for Defence Studies, 2010).

Klein, Margaret, "Russia's New Military Doctrine," SWP Comments 1, German Institute for International and Security Affairs, February 9, 2016, accessed November 14, 2015, https://www.swp-berlin.org/fileadmin/contents/products/comments/2015C09_kle.pdf.

Kochis, Daniel, "Countering Russian Propaganda Abroad," Heritage Foundation Issue Brief # 4286, October 21, 2014, accessed January 18, 2016, http://www.heritage.org/research/reports/2014/10/countering-russian-propaganda-abroad.

Kuchins, Andrew C. and Zevelev, Igor A., "Russian Foreign Policy: Continuity in Change." *The Washington Quarterly* 35 (2012).

Lough, John Et Al. "Russian Influence Abroad Non-State Actors and Propaganda". Russia and Eurasia Programme, Chatham House, March 2014, accessed March 7, 2016, https://www.chathamhouse.org/event/russian-influence-abroad-non-state-actors-and-propaganda.

McDermott, Roger, "The Kremlin, the General Staff and Unlocking Future Warfare Capabilities." *Eurasia Daily Monitor*, May 2014, accessed November 2, 2015, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=42322&no_cache=1.

Panarin, Igor, "The Information War Against Russia: Operation anti-Putin" (speech given at international conference hosted by Schiller Institute, Berlin, Germany, February, 25 2012, accessed December 3, 2015, http://schiller-institut.de/seiten/201202-berlin/panarin-english.html).

Perry, Brett, "Non-Linear Warfare in Ukraine : the Critical Role of Information Operations and Special Operations," *Small Wars Journal*, August 14, 2015, accessed November 18, 2015, http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera .

Pkhaladze, Tengiz. "Religion as The Instrument Of Russian Foreign Policy Towards Neighboring Countries Georgia, Latvia, Ukraine". (Tblisi, International Centre for Geopolitical Studies, 2012).

Pomerantsev, Peter. "How Putin in Reinventing Warfare." *Foreign Policy*, May 5, 2014, accessed November 24, 2015, http://www.foreignpolicy.com/articles/2014/05/05/how_putin_is_reinventing_warfare.

Pomerantsev, Peter. "Russia and the Menace of Unreality." *The Atlantic*. September 9, 2014, accessed November 2, 2016, http://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/.

Rácz, András, “Russia’s Hybrid War in Ukraine : Breaking the Enemy’s Ability to Resist,” The Finnish Institute of International Affairs, April 2015, accessed November 2, 2015, http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ukraine/.

Rice, Condoleezza, and Robert Gates. "How America Can Counter Putin’s Moves in Syria". *Washington Post.* March 9, 2016, accessed March 12, 2016, https://www.washingtonpost.com/opinions/how-to-counter-putin-in-syria/2015/10/08/128fade2-6c66-11e5-b31c-d80d62b53e28_story.html.

Seddon, Max, “Documents Show How Russia’s Troll Army Hit America,” *Buzzfeed*, June 2, 2014, accessed February 22, 2016, http://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america#31fidzl.

Snegovaya, Maria, “Putin’s Information Warfare in the Ukraine: Soviet Origins of Russia’s Hybrid Warfare,” Institute for the Study of War, September 2015, accessed December 12, 2015, http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf

Tadeo, Maria, “State Television Reporter Warns Russia Could ‘Turn US Into Radioactive Dust,’” *The Independent*, March 17, 2014, accessed February 18, 2016, http://www.independent.co.uk/news/world/europe/state-television-presenter-warns-russia-could-turn-the-us-into-radioactive-dust-9197433.html.

Tatham, Steve Cdr (rtd). “The Solution to Russian Propaganda is not EU or NATO Propaganda ut Advanced Social Science to Understand and Mitigate its Effects in Targeted Populations,” National Defence Academy of Latvia, July 2015, accessed February 26, 2016, http://www.stratcomcoe.org/steve-tatham-solution-russian-propaganda-not-eu-or-nato-propaganda-advanced-social-science.

Thomas, Timothy, “Russia’s Reflexive Control Theory and the Military,” *Journal of Slavic Military Studies* 17 (2004).

Thomas, Timothy. “Russia’s Information Warfare Strategy: Can the Nation Cope in Future Conflicts,” *Journal of Slavic Military Studies* 27 (2014).

Thomas, Timothy. "Russia’s Military Strategy And Ukraine: Indirect, Asymmetric ”And Putin-Led". *Journal of Slavic Military Studies* 28.3 (2015): 445-461.

Van Herpen, Marcel H. *Putin’s Wars: the Rise of Russia’s New Imperialism.* (London: Rowman & Littlefield, 2015).

Ven Bruusgaard, Kristin, “Crimea and Russia’s Strategic Overhaul”, *Parameters* 44 (2014).

Votel, Joseph L.; Cleveland, Charles T.; Connett, Charles T.; Irwin, Will. “Unconventional Warfare in the Gray Zone,” *Joint Force Quarterly* 80 (2016).

Williams, Michael, “Russia’s New Doctrine: How the Kremlin Has Learned to Fight Tomorrow’s War Today,” Center for European Policy Analysis, May 9, 2014, accessed October 24, 2015, http://cepa.org/content/russia%E2%80%99s-new-doctrine-how-kremlin-has-learned-fight-tomorrow%E2%80%99s-war-today.

"Russia Security Paper Designates NATO as a Threat," BBC News, December 31, 2015, accessed January 5, 2016, http://www.bbc.com/news/world-europe-35208636.

"Contemporary Media Use in Ukraine," Gallup – Broadcasting Board of Governors, June, 2014, accessed February 11, 2016, www.bbg.gov/wp-content/media/2014/06/Ukraine-research-brief.pdf, ,.

"Analysis of Russia's Information Campaign Against Ukraine," NATO STRATCOM Center of Excellence, 2014, accessed February 18, 2016, http://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine.

"L'offensive médiatique russe vise l'Europe." *Le Monde*. 12 February 2016.

"Ukraine says communications hit, MPs phones blocked. " *Reuters*, March 4 2014, accessed February 22, 2016, http://www.reuters.com/article/2014/03/04/ukraine-crisis-cybersecurity-idUSL6N0M12CF20140304.

"Russian PM Medvedev Says New Cold War is On," BBC, February 13, 2016, accessed February 14, 2016, http://www.bbc.com/news/world-europe-35569094.

"SOF Support to Political Warfare," United States Army Special Operations Command White Paper, March 10, 2015, accessed February 8, 2016, http://smallwarsjournal.com/blog/sof-support-to-political-warfare.

AJP-3.10 : Allied Joint Doctrine for Information Operations. 24 June 2015.

FM 3-13: Inform and Influence Operations, 25 January 2013, 1-1.