Réseau d'analyse stratégique
Network for Strategic Analysis

Février 2021 Numéro 9

Note politique

Qu'est-ce que la dissuasion en zone grise ?

Hannah Hollander

Contexte

Les types de conflits que les États cherchent à dissuader ont évolué depuis la guerre froide, présentant chaque fois de nouveaux défis. La théorie de la dissuasion est devenue populaire pendant la guerre froide, avec les capacités nucléaires dissuadant les États-Unis et la Russie de s'engager dans un conflit direct. Après la guerre froide, et surtout au début des années 2000 avec les guerres en Afghanistan et en Irak, les États occidentaux ont eu du mal à trouver comment dissuader les attaques terroristes, en particulier celles perpétrées par des acteurs non étatiques. Vers 2010, l'accent mis sur les opérations de contre-insurrection et de lutte contre le terrorisme à grande échelle a commencé à s'estomper, et l'attention s'est portée sur le retour de la rivalité entre les grandes puissances.

La Russie, la Chine, l'Iran et la Corée du Nord ont accéléré le rythme auquel ils remettent en question l'ordre international fondé sur des règles, par des actions provocatrices et nocives qui ne franchissent cependant pas le seuil des actions de guerre. La plupart de leurs actions sont menées clandestinement dans le but de perturber l'hégémonie occidentale tout en évitant les actes ouverts qui pourraient entraîner des critiques ou des représailles. L'agression contre les pays occidentaux s'accroît et l'ambiguïté de ces menaces remet en question les concepts traditionnels de dissuasion. Alors que la théorie et les pratiques traditionnelles de dissuasion sont parfaitement assimilées, il existe un manque de consensus parmi les universitaires, les praticiens et le droit international sur ce qui constitue une agression ou une réponse appropriée en zone grise. L'absence de compréhension concrète de la zone grise rend plus difficile l'élaboration de théories et de politiques de dissuasion dans cette zone. Cette note politique passe en revue la littérature sur la théorie de la dissuasion, les définitions de ce qu'est et de ce que n'est pas la zone grise, les principales préoccupations des conflits actuels en zone grise, les défis de la dissuasion en zone grise, et conclut par plusieurs moyens de dissuader les conflits en zone grise.

La théorie de la dissuasion

Au fondement de la dissuasion, il y a la prévention de la guerre. Elle ne constitue pas une solution à long terme à un environnement de sécurité hostile, mais repose sur une approche fondée sur la menace pour convaincre les États rivaux qu'une action agressive n'est

Réseau d'analyse stratégique
Robert Sutherland Hall, Suite 403, Queen's University
+1 613.533.2381 | info@ras-nsa.ca
ras-nsa.ca

pas dans leur intérêt. La dissuasion peut être conceptualisée de plusieurs façons. La première consiste à dissuader les États par l’interdiction ou par la punition. La dissuasion par interdiction se produit lorsqu'un État dispose de capacités considérables qu'une attaque ennemie ne serait pas en mesure de surmonter ou dont l'impact serait considérablement réduit ou retardé. La dissuasion par la punition se produit lorsqu'un État agresseur choisit de ne pas attaquer parce qu'il croit que même s'il atteint son objectif, il serait soumis à une punition, telle que des sanctions ou une contre-attaque, qui serait plus coûteuse que ce qu'il a gagné lors de l'attaque initiale. Dans le scénario parfait, les capacités de défense d'un État seraient suffisamment fortes pour atteindre les deux objectifs, mais ce n'est pas le cas pour de nombreux États.

Une façon alternative, mais complémentaire, de conceptualiser la dissuasion est de la concevoir comme une pyramide. La dissuasion nucléaire se situe au sommet de la pyramide, suivie de la répression par les forces armées et la puissance dure traditionnelle. Vient ensuite la dissuasion par interdiction. Enfin, il y a la dissuasion étendue, où un État est capable de dissuader les menaces parce qu'un ou plusieurs autres États le défendent. L'article 5 de l'OTAN est un excellent exemple de dissuasion étendue. Malheureusement, la dissuasion nucléaire, la dissuasion par la punition et même la dissuasion étendue ont un effet limité lorsqu'il est difficile de déterminer la nature des attaques étrangères dans la zone grise.

Qu’est-ce que la zone grise ?

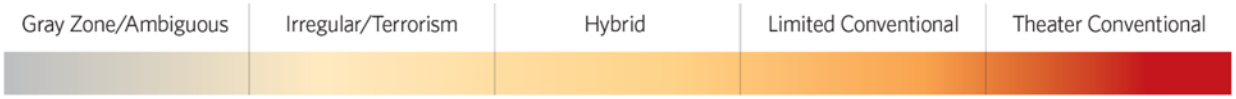
Les actions en zone grise sont souvent qualifiées de manière interchangeable de guerre « hybride » ou « non conventionnelle ». Un conflit de zone grise désigne toute confrontation qui dépasse la compétition standard et diplomatique, mais qui ne franchit pas le seuil de la guerre. Il s'agit de la zone située entre la guerre et la paix. Ce type de conflit se manifeste dans divers domaines tels que l'économie, les finances, le cyberespace, la politique et autres, là où le conflit conventionnel est axé sur l'utilisation stratégique de la violence. Il peut également être mené par des États, des acteurs non étatiques ou des intermédiaires. Les conflits de zone grise peuvent intégrer des approches conventionnelles et non conventionnelles. Les attaques de zone grise sont souvent intentionnellement dissimulées, ce qui rend difficile l'attribution de la responsabilité, et elles sont généralement juste en dessous du seuil justifiant une réponse militaire. Ainsi, la dissuasion conventionnelle ne fonctionne pas lorsqu'on ne sait pas clairement qui a mené l'attaque, quelle était l'intention de l'attaque et à quel moment une attaque dépasse la zone grise et est suffisamment dommageable pour justifier une réponse violente.

Zone grise vs guerre hybride

Malgré le chevauchement conceptuel de la « zone grise » et de la « guerre hybride », elles ne sont pas synonymes. La guerre hybride est l'utilisation combinée de tactiques conventionnelles et non conventionnelles qui dépassent le seuil de la guerre. Certaines des tactiques hybrides utilisées, telles que la désinformation, peuvent se situer dans la zone grise. Les conflits de la zone grise sont uniquement les tactiques qui ne franchissent pas la ligne d'une agression formalisée au niveau de l'État. La guerre hybride se concentre sur les événements au niveau tactique, tandis que la zone grise englobe les considérations stratégiques à long terme des compétitions internationales. La **figure 1** (page suivante) de Frank G. Hoffman fournit une représentation visuelle du spectre des conflits et montre clairement la différence entre la zone grise et la guerre hybride, où les deux relèvent du spectre des conflits dans la guerre non conventionnelle. C'est pourquoi les tactiques d'agression non conventionnelles sont souvent discutées comme un moyen de conflit de zone grise et de guerre hybride.

FIGURE 1

Spectrum of Conflict in Unconventional Warfare



Agressions contemporaines en zone grise

Le conflit de zone grise est devenu un sujet d'intérêt principalement en raison des actions de la Russie, de la Chine, de l'Iran et de la Corée du Nord au cours des dix dernières années. Ces quatre États ont utilisé la désinformation et se sont engagés dans des cyberattaques par le biais de pirates informatiques et d'intermédiaires pour pénétrer les systèmes de sécurité et causer des dommages de faible niveau. La Russie et la Chine ont toutes deux procédé à des expansions territoriales graduelles, mais par des moyens différents. En 2014, la Russie a utilisé la désinformation pour aggraver les tensions en Crimée, ce qui a conduit à son annexion. En 2015 et 2016, un pirate informatique lié au Kremlin, Sandworm, a contaminé les services publics ukrainiens avec des logiciels malveillants et a privé d'électricité des milliers d'Ukrainiens. En 2017, la Russie a également été liée à un virus qui a rendu le système informatique de Maersk, une compagnie maritime danoise, inutilisable pendant une semaine, entraînant des pertes de 300 millions de dollars. Cela s'ajoute à d'innombrables cas de désinformation et de contrôle des médias visant les alliances occidentales et les opérations de l'OTAN. La stratégie est qualifiée de « simmering borscht », où la Russie tente d'étendre son influence sans provoquer une réaction occidentale.

Depuis 2014, la Chine a construit des bases sur des îles de la mer de Chine du Sud afin d'étendre et de consolider ses revendications territoriales. Le comportement de la Chine a été qualifié de « tactique du salami » : elle érode lentement l'ordre et les normes internationales, divise les alliances et tente d'affirmer son interprétation préférée des lois internationales existantes. L'utilisation par la Chine de la sécurité maritime et des pêcheries pour étendre son contrôle sur la mer de Chine du Sud par des actes d'agression délibérés et indéniables est l'exemple parfait du conflit de zone grise. Les liens entre les entreprises chinoises et le gouvernement se sont également avérés être un point de conflit de zone grise avec Huawei, ce qui a suscité des inquiétudes parmi le Groupe des cinq. Les tensions avec la Chine ont contribué à une confrontation par la détention, le Canada détenant la cadre Meng Wanzhou et la Chine détenant les Canadiens Michael Kovrig et Michael Spavor.

Bien que l'Iran et la Corée du Nord ne soient pas reconnus comme des acteurs clés dans la compétition entre grandes puissances, ils sont connus pour l'augmentation de l'agression en zone grise par des actions politiques, économiques, cybernétiques et militaires depuis 2016.

Les défis de la dissuasion en zone grise

Le paradoxe du conflit en zone grise est qu'il est plus saillant lorsque la guerre ouverte est dissuadée avec succès. C'est également pourquoi les conflits en zone grise étaient fréquents pendant la guerre froide. Le premier défi est que la zone grise est intrinsèquement ambiguë, et que la dissuasion, en particulier la dissuasion par la punition, dépend de réponses clairement définies à des attaques identifiables. Les attaques contre la société civile et qui se situent en dessous du seuil de l'article 5 de l'OTAN ne permettent pas de savoir si la solution doit être des actions militaires d'État à

État. En outre, la dissuasion traditionnelle est basée sur des attaques directes et violentes, visant généralement des infrastructures militaires, ou entraînant des violences directes contre les civils. Pourtant, les dommages causés aux réseaux électriques et cybernétiques risquent d'être tout aussi dommageables. Une interruption prolongée de l'alimentation électrique et de la cyberinfrastructure pourrait entraîner la perte de vies humaines dans le cas des hôpitaux, du contrôle du trafic et de la sécurité alimentaire, et peut provoquer des pertes financières importantes lorsque les économies sont paralysées. Une cyber-attaque récente contre une installation d'approvisionnement en eau en Floride démontre la vulnérabilité des services essentiels du secteur public. Les cyberattaques sont particulièrement difficiles à décourager parce qu'elles sont menées aussi bien par des acteurs au niveau de l'État, des groupes non étatiques et des individus, ce qui rend difficiles la recherche et l'attribution des responsabilités en temps réel. Elles visent également les secteurs privé et civil plus fréquemment que les agressions militaires classiques, ce qui nécessite une coordination entre le groupe attaqué et leurs services de sécurité nationaux.

Les États démocratiques qui choisissent de respecter l'ordre international fondé sur des règles sont désavantagés lorsqu'il s'agit de conflits en zone grise. Des États comme la Russie, la Chine, l'Iran et la Corée du Nord ont des gouvernements très centralisés qui sont capables et disposés à recourir à la propagande, à prendre pour cible des entités civiles, à repousser les limites des normes juridiques et à utiliser des moyens non étatiques à leur avantage par rapport aux États de type libéral démocratique. Les États agresseurs utilisent à leur avantage l'engagement des États démocratiques envers les normes internationales et les processus d'approbation bureaucratiques pour exercer des représailles, réduisant ainsi l'impact de la dissuasion par la punition. Les États démocratiques se trouvent dans une situation difficile en raison de ces procédures bureaucratiques et de l'importance du contrôle civil de l'armée qui protègent les valeurs centrales de leur identité libérale.

Ce à quoi ressemble la dissuasion dans la zone grise

Ce n'est pas parce que la dissuasion est plus complexe dans la zone grise qu'elle n'a aucune valeur. Les politiciens et les universitaires doivent être conscients des limites de la dissuasion dans la zone grise et savoir comment adapter leurs approches stratégiques. Des lignes directrices clairement définies pour les actes d'agression, en particulier dans le cas du cyberespace, mais aussi des critères de recours à l'escalade de la force pour les attaques non militaires, peuvent contribuer à la dissuasion en zone grise par la punition.

Dans le cas d'une agression conventionnelle en zone grise, les forces de réaction rapide sont l'un des meilleurs moyens de dissuasion de puissance dure dans lesquels l'Occident pourrait investir davantage. Dans le cas de l'annexion de la Crimée par la Russie – où des forces paramilitaires et militaires camouflées ont été utilisées – des troupes rapidement déployables auraient augmenté les risques d'agir pour la Russie et elles auraient été capables de réagir plus rapidement à la seconde où la Russie aurait franchi la ligne de démarcation entre la zone grise et la guerre hybride. En ce qui concerne le cyberespace, des cyberattaques de représailles ou même le recours à l'armée lorsqu'une ligne est franchie pourraient être des moyens efficaces. Le lien

entre la cybersécurité et les réponses militaires conventionnelles est mal défini, ce qui présente une fenêtre d'ambiguïté et une opportunité pour les attaquants. En outre, le secret entourant les cybercapacités offensives nuit à leur valeur dissuasive, car la dissuasion conventionnelle repose en partie sur une démonstration de force permettant à l'ennemi de comprendre les conséquences potentielles de ses actions.

La dissuasion par interdiction semble toutefois être la voie la plus fortement préconisée pour améliorer la dissuasion dans les zones grises. Il s'agit d'abord de favoriser les investissements et la formation en matière de cybersécurité afin d'atténuer la vulnérabilité aux attaques. La deuxième partie de la dissuasion en zone grise par interdiction est la résilience, c'est-à-dire la résilience de la cyberinfrastructure, mais aussi de la société. Lors du sommet de Varsovie de 2016, l'OTAN a présenté sept exigences de base en matière de préparation civile :

1) Assurer la continuité du gouvernement et des services gouvernementaux essentiels;
2) Un approvisionnement énergétique résilient;
3) La capacité à gérer efficacement les mouvements incontrôlés de personnes;
4) Des ressources alimentaires et en eau résilientes;
5) La capacité à faire face à des pertes massives de vies humaines;
6) Des systèmes civils de communication résilients;
7) Des systèmes civils de transport résilients.

Recommandations pour le Canada

Le Canada a régulièrement employé des méthodes de guerre hybride lors de ses interventions au sein d'États fragiles, même si cela n'est pas qualifié de cette façon. Les interventions du Canada font appel à la coopération civile et militaire ainsi qu'à des éléments économiques et politiques qui impliquent la formation, l'interaction et l'influence des forces de sécurité, des politiciens et du public.

Les États démocratiques comme le Canada ont tendance à être performants face aux menaces immédiates pour la sécurité, mais à éprouver des difficultés lorsque vient le temps de faire face aux menaces de la zone grise qui se situent en dessous du seuil et qui ne suscitent pas l'inquiétude du public qui conduirait à l'action politique. Bien que le Canada ne soit pas en guerre, le public ne sait pas que le Canada est quotidiennement la cible d'attaques de zone grise contre son cyberespace, son système d'information publique, son armée et même contre son territoire physique.

Le Canada doit élargir son engagement volontaire et stratégique dans la guerre hybride et se prémunir contre les menaces de la zone grise. La première étape pour renforcer la défense canadienne contre les conflits de la zone grise est de les comprendre. La littérature montre que nous avons besoin d'une définition plus claire de la zone grise et de la manière dont les États doivent y répondre. Cela devrait être soutenu par des organisations comme l'OTAN. Le Canada et ses alliés doivent comprendre ce qu'ils dissuadent, où ils fixent la limite des actions agressives et comment ils vont réagir. Le Canada, pour des raisons domestiques, doit clairement définir et tracer une démarcation de la zone grise d'agression. Le Canada doit également travailler au sein de l'OTAN pour établir un consensus sur les types d'attaques auxquelles l'alliance répondra en vertu de l'article 5, et sur la manière dont l'alliance entend réagir lorsqu'un acte d'agression ne franchit pas le seuil de la guerre.

L'un des aspects les plus importants de la dissuasion par la punition est une réaction rapide. Le Canada doit continuer à s'assurer que ses militaires sont à la hauteur d'une réaction rapide lorsqu'un acte d'agression dépasse la zone grise. Il existe un écart plus important dans les capacités cybernétiques offensives ou

de représailles du Canada. Le Canada devrait développer ses capacités de cybersécurité et de défense pour mener des contre-attaques – une façon de riposter par les mêmes moyens, et de demeurer dans la zone grise.

Enfin, la manière la plus pacifique et la plus rassurante de protéger les Canadiens des agressions de la zone grise est par l’interdiction et la résilience. Comme les conflits en zone grise peuvent viser n'importe qui, la partie critique et difficile de l’interdiction et de la résilience est qu'ils nécessitent un engagement important de la population générale et du secteur privé. Le gouvernement canadien devra réglementer davantage et surtout promouvoir des normes plus élevées en matière de cybersécurité et d'infrastructures résilientes dans les secteurs public et privé. La gestion des crises devra se faire entre les ministres du cabinet et les PDG. Il sera également important de mener des campagnes d'éducation auprès du public sur la manière de détecter la désinformation et les cybervulnérabilités. Les conflits dans la zone grise nécessitent une approche par la société dans son ensemble pour une dissuasion efficace et pour éviter que l'agression sorte de la zone grise et qu'une guerre ouverte se déclenche.