

Canadian
Forces
College

Collège
des
Forces
Canadiennes



LA COMMUNICATION STRATRONIQUE: UNE ARME DE CONVICTION MASSIVE

Lieutenant-Colonel Enrico Pelle

JCSP 45

Exercice Solo Flight

Disclaimer

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

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2019.

PCEMI 45

Exercice Solo Flight

Avertissement

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

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2019.

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

LA COMMUNICATION STRATRONIQUE: UNE ARME DE CONVICTION MASSIVE

Lieutenant-Colonel Enrico Pelle

“This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

INTRODUCTION

“Les règles de la guerre ont fondamentalement changé... l’efficacité des outils non-militaires pour atteindre des objectifs stratégiques ou politiques dans un conflit a dépassé celle des armes.” - Le général Gerasimov, Chef d’état-major de la Russie, 2013

Mise en contexte

Le monde est désormais plongé dans le nouvel âge de l’information qui a transformé la planète dans un espace commun où des milliards de personnes peuvent se connecter et partager de l’information sur une échelle planétaire. Les plateformes de médias sociaux constituent un instrument clé de la révolution technologique. Par contre, ces plateformes de communication ne constituent pas uniquement une façon de se connecter avec d’autres personnes, des marchés d’affaires ou pour promouvoir des campagnes électorales. Elles peuvent maintenant être utilisées pour modeler les résultats d’élections, de campagnes militaires et même de la géopolitique. Le monde en ligne est devenu un espace global de confrontation que nous devons mieux comprendre, tandis que les batailles pour la popularité et la perception fusionnent avec les conflits du monde réel. Ce Solo Flight portera sur l’utilisation de la communication en ligne comme une arme dans les relations internationales. Il exposera la présence croissante de la communication via l’internet comme une arme de conviction massive dans les conflits géopolitiques et stratégiques. Ce texte explorera également les failles de notre structure actuelle vis-à-vis l’institutionnalisation de cette arme trans-étatique.

Question de recherche et thèse générale

Avons-nous développé une architecture adéquate pour institutionnaliser l'utilisation de la communication électronique comme une arme dans les relations internationales?

LA PLUME EST UNE ÉPÉE

La guerre des "Like"

"Le facteur décisif des guerres futures sera le narratif... quel récit gagne?"

- Étude RAND

Tout d'abord, l'internet et les réseaux sociaux ont transformé les nouvelles, la politique et la guerre tandis que, inversement, les nouvelles, la politique et la guerre ont changé l'internet pour toutes les personnes connectées. P.W. Singer et Emerson Brooking, auteurs du livre *"LikeWar - The Weaponization of Social Media"* ont développé le concept de la guerre des "Like". En terme de définition, la guerre cyber est le piratage des réseaux tandis que la guerre des "Like" est le piratage des personnes sur les réseaux en transmettant des idées virales à travers un mélange de "Like" mais aussi à travers des mensonges et un système mené par les algorithmes.¹

Afin de mieux comprendre la diffusion presque sans frontière des réseaux sociaux, voici quelques données intéressantes. Tout d'abord Facebook - en date de 2013: 845 million d'utilisateurs actifs; l'utilisateur moyen a 130 amis; une visite sur le site dure en moyenne 23

¹ Singer, P. W and Emerson T., Brooking, Likewar: The Weaponization of Social Media. Boston, Massachusetts: Houghton Mifflin Harcourt, 2018.

minutes; et 46% des utilisateurs sont âgés de plus de 45 ans.² Twitter - en date de 2013: 127 million d'utilisateurs actifs; 33% des utilisateurs sont âgés de plus de 45 ans; 54% des utilisateurs sont connectés via leur téléphone cellulaire; et une visite sur le site dure en moyenne 14 minutes.³ Instagram - en date de 2018: il y a eu un total de 45 milliards de photos partagées sur cette plateforme; plus de 60% de ses usagers visitent le site sur une base quotidienne; 80 millions de photos sont partagées quotidiennement; il y a 3.5 milliards de "Like" quotidiennement; la majorité des utilisateurs sont âgés entre 18 et 29 ans; un utilisateur moyen a 648 suiveurs et suis 359 comptes; et une étude a démontré que 8% des comptes sont falsifiés.⁴ Ces chiffres parlent d'eux-mêmes quant à la capacité presque sans limite de projection et de propagation d'une information ou d'un message sur les réseaux sociaux.

Les "Like" et la guerre se fusionnent ensemble de la même façon que Clausewitz proposait de fusionner la guerre et la politique à l'époque à travers des moyens et des mêmes. De nos jours, il y a des armées en ligne qui utilisent les mêmes tactiques pour rencontrer leurs objectifs à l'échelle mondiale et elles se décriront comme étant en guerre ou en guerre des "Like". Des exemples récents sont Daesh contre la coalition militaire, les supporters du Président Trump contre le reste du monde et les fans de Kanye West contre ceux de Taylor Swift. Toutes ces confrontations sont très différentes mais utilisent les même tactiques ou "doctrine" pour gagner la guerre en ligne, et pour rencontrer leurs objectifs mondiaux afin d'affecter les résultats

² Social Media use in the Military Sector, posted in General Security on 31 January 2013, <https://resources.infosecinstitute.com/social-media-use-in-the-military-sector/#gref>.

³ Ibid.

⁴ 30 Insane Facts About Instagram, <https://www.thefactsite.com/instagram-facts/>.

comme ceux de la bataille de Mosul, les élections américaines de 2016 et la vente d'albums de musique.

La communication stratronique - des études de cas

Plusieurs événements récents peuvent être étudiés pour démontrer l'impact significatif de la communication via internet sur des enjeux globaux importants. Le premier étant le relâchement de la politique sur l'utilisation des médias sociaux par le Département de la défense nationale américaine en 2010. Selon cette récente politique, les Forces militaires américaines permettent à leurs membres en service et en opérations d'utiliser des téléphones intelligents et les réseaux sociaux selon des directives et paramètres fixes.⁵ Selon Roxie Merritt, Directrice des opérations des nouveaux médias au Bureau du Secrétaire de la défense des Affaires publiques au sein du Département de la défense américaine, a déclarée dans une entrevue: *"It's not about controlling the message any more. It's about giving people as much information and resources and facts as they can."*⁶ Un danger de cette politique est la possibilité que des militaires puissent trouver un adversaire sur les réseaux sociaux ce qui est tout à fait contraire à la compréhension traditionnelle des communications en temps de guerre. Avec la technologie d'aujourd'hui telle que l'intelligence artificielle et les applications de géolocalisation et de reconnaissance faciale, il est relativement facile de recueillir de l'information sur le web pour déterminer l'endroit d'un exercice ou d'une opération militaire ou de déterminer le nombre approximatif de militaires impliqués et des ressources utilisées. De l'autre côté de l'océan, le Parlement russe a voté en

⁵ US Department of Defense releases official policy on social media, <https://www.davidmeermanscott.com/blog/2010/02/us-department-of-defense-releases-official-policy-on-social-media.html>.

⁶ Ibid.

2019 d'interdire ses militaires d'utiliser des téléphones cellulaires lorsqu'ils sont en service, et ce depuis que leur utilisation de réseaux sociaux a soulevé des problématiques en terme de sécurité nationale.⁷ De plus, les militaires russes ne peuvent plus écrire sur le domaine de la défense ni de leurs Forces armées sur les réseaux sociaux et ne peuvent pas parler aux journalistes. Nous voyons ici deux philosophies et croyances opposées sur le rôle de l'internet et des réseaux sociaux sur des enjeux de sécurité nationale et de protection de la force.

Un autre événement fut l'attaque du centre commercial Westgate, à Nairobi au Kenya du 21 au 24 septembre 2013. Durant cette attaque, des jihadistes équipés d'armes automatiques tuèrent 68 personnes, en plus d'en blesser au-dessus de 200.⁸ Cette attaque terroriste fut gazouillée en direct par le groupe revendicateur de l'attaque, soit le groupe islamiste al-Shabaab. Dans ce cas, les terroristes du groupe al-Shabaab ont contrôlé le narratif public jusqu'à ce que le gouvernement fédéral du Kenya puisse répondre aux attaques lancées sur le web. Selon des statistiques recueillies, le président de la République du Kenya aurait transmis seulement 17 gazouillis, et son vice-président seulement six durant les jours de l'attaque, tandis que le groupe al-Shabaab en aurait publié 258, dont 89% des messages contenant un # (*hashtag*) améliorant ainsi l'efficacité de leur publication.⁹ Par contre, nous pouvons observer que le Ministre de l'intérieur et de la coordination du gouvernement national, le Centre national des opérations des désastres et la Police du Kenya ont tous été très actifs sur Twitter en publiant respectivement

⁷ Russia bans smartphones for soldiers over social media fears, 20 février 2019, <https://www.bbc.com/news/world-europe-47302938>.

⁸ Attaque du centre commercial Westgate, https://fr.wikipedia.org/wiki/Attaque_du_centre_commercial_Westgate.

⁹ Twitter in the Cross Fire—The Use of Social Media in the Westgate Mall Terror Attack in Kenya, <https://journals.plos.org/plosone/article/figure?id=10.1371/journal.pone.0104136.t002>.

1523, 558 et 569 gazouillis.¹⁰ Ces chiffres imposants démontrent l'importance du combat médiatique des réseaux sociaux qui se battent afin de contrôler le narratif et de gagner la perception et la crédibilité du publique.

L'Opération PILLAR OF DEFENSE s'est caractérisée par une campagne aérienne de 8 jours par les Forces militaires israélienne contre les militants du mouvement islamiste palestinien Hamas en novembre 2012. Cette campagne militaire s'est faite baptisée comme étant la première guerre des réseaux sociaux.¹¹ La guerre opposant Israël et le Hamas à Gaza a augmenté l'intensité de surcharge d'information à un tout autre niveau dans le cadre des opérations psychologiques. Par l'entremise de blogs opérationnels, de sites web, de pages Facebook et de comptes Twitter, les deux adversaires ont inondé l'internet avec des images, des vidéos et de la propagande afin de transmettre au monde entier des messages sur les objectifs de leurs campagnes.¹² En huit jours, on rapporte que 8 million de gazouillis ont été échangés en ligne par des proxies des deux côtés du conflit dans le but de remporter la guerre de l'opinion publique.¹³ Selon le "*News English Review*", le principale compte Twitter des Forces armées israéliennes comptait plus de 327 000 suiveurs, tandis que le compte [Arabic account of the military arm Qassam Arabic@ @qassam_arabic1](#) du Hamas en comptait près de 58 000. Le Hamas a produit des gazouillis avec des images graphiques de femmes et d'enfants supposément tués par des attaques de missiles et d'obus d'artillerie israéliens. Plusieurs de ces images avaient été photo-

¹⁰ Twitter in the Cross Fire—The Use of Social Media in the Westgate Mall Terror Attack in Kenya, <https://journals.plos.org/plosone/article/figure?id=10.1371/journal.pone.0104136.t002>.

¹¹ Israel's War with Hamas 2014: Part III - The Social Media Battle, https://www.newenglishreview.org/custpage.cfm/frm/165962/sec_id/165962.

¹² Ibid.

¹³ Ibid.

chopées, falsifiées ou empruntées de la guerre civile syrienne et même de films hollywoodiens. Ces actions ont menés au blocage de comptes Twitter du Hamas. Les deux adversaires se sont affrontés sur les réseaux sociaux dans une variété de différents langages, et ce afin de remporter la victoire de l'opinion publique. Ce premier rallye mondial Facebook/Twitter a été un succès à plusieurs niveaux, produisant une communauté de partisans entraînés sur les réseaux sociaux supportés par des activités spécialisés.

En 2014, Daesh a surgi sous l'imagination du publique. Après l'exécution de James Foley par des militants de Daesh dans une vidéo de propagande qui est devenue virale, les américains ont rapporté avoir plus peur du terrorisme à ce moment qu'immédiatement après les attaques du 11 septembre 2001. Selon Martin Rudner, la doctrine évolutive du "jihadisme électronique" a eu un impact significatif sur la radicalisation de musulmans dans la diaspora des communautés occidentales.¹⁴ De nos jours, les sites web servent de bibliothèque en ligne et de répertoires de littérature jihadist, qui sont utilisées comme des plateformes pour des prêcheurs extrémistes et des forums pour le discours radical. La connectivité internet joue désormais un rôle opérationnel plus direct dans l'atteinte d'objectifs jihadists reliés au terrorisme, plus particulièrement pour inciter des acteurs potentiels à prendre des actions concrètes telles que recruter des opérateurs ou des combattants, fournir de l'entraînement virtuel sur des opérations tactiques et la fabrication d'explosifs, pour financer le terrorisme et pour planifier et préparer des attaques terroristes spécifiques. Voici quelques données sur l'utilisation de l'internet et des réseaux sociaux par Daesh. Ce dernier a une équipe dédiée d'approximativement 100 insurgés dédiés à filmer des vidéos d'exécutions (par décapitation ou fusillade) et de propagande

¹⁴ Martin Rudner (2017) "Electronic Jihad": The Internet as Al Qaeda's Catalyst for Global Terror, *Studies in Conflict & Terrorism*, 40:1, 10-23, DOI: 10.1080/1057610X.2016.1157403.

extrémiste.¹⁵ Au cours de 2014, il y avait un estimé de 46 000 à 90 000 comptes Twitter qui préconisaient Daesh ou qui étaient opérés par des partisans du groupe extrémiste. En 2015, Twitter rapportait avoir fermé 125 000 comptes sympathisants du groupe terroriste. En 2016, le même média social publiait avoir supprimé 325 000 comptes additionnels.¹⁶ Les activités de Daesh sur le web traditionnel sont sujet à de la surveillance et sont régis par des corporations, des agences gouvernementales et des pirates du web. Pour cette raison, Daesh a été forcé de trouver un nouveau sanctuaire sécuritaire en ligne, soit le “*Dark Web*”. Le “*Dark Web*” ne peut être retracé et fourni une plateforme complètement anonyme autant pour le transmetteur que pour le receveur du message. L’utilisation du “*Dark Web*” par Daesh et d’autres groupes terroristes a rendu les opérations anti-terroristes plus complexes.

Lors de la première bataille de Mosul en juin 2014, Daesh accompli l’inimaginable avec une force militaire et des moyens physiques très modestes. Le groupe extrémiste islamique, avec une force d’approximativement 2 500 combattants, armés d’AK47 et de camionnettes non-blindées se butent contre une force militaire irakienne d’approximativement 20 000 guerriers et supportés par l’organisation militaire la plus puissante au monde, des hélicoptères Blackhawk et des chars d’assauts Abrahams. Avec une tactique non-traditionnelle et inattendue, Daesh s’engage vers le combat avec des techniques de communications fondamentalement différentes, comparable à celles du Blitzkrieg des années 1940. Donc, au lieu de garder l’opération secrète pour instaurer un effet de surprise, Daesh veut que le monde entier sache l’objectif ambitieux du groupe, et ce en créant un *hashtag* (#) sur Daesh afin de propager le message stratégique avant la

¹⁵ Use of social media by the Islamic State of Iraq and the Levant, https://en.wikipedia.org/wiki/Use_of_social_media_by_the_Islamic_State_of_Iraq_and_the_Levant.

¹⁶ Ibid.

bataille tactique. Ce message stratégique se propage rapidement via l'internet et les réseaux sociaux, puis il disperse une intention de violence extrême, instaurant du coup un sentiment de peur chez les irakiens. Daesh publie des images de batailles perdues et de prise de prisonniers de guerre irakiens, provoquant une perception à ces derniers que la bataille était déjà perdue même avant qu'elle n'eu lieu. Le résultat est la capitulation de l'armée irakienne avec trop peu de résistance, les militaires irakiens se dispersent et Daesh gagne Mosul.

Appuyés par les téléphones intelligents, les caméras et les capteurs disponibles dans n'importe quelle zone d'opération, les réseaux sociaux nous rendent chroniques du partage d'information. De plus, cette information ne disparaît plus, elle continue de s'accumuler et toute parcelle d'information peut être utilisée à n'importe quel moment par des intervenants qui n'ont pas nécessairement nos meilleurs intérêts à cœur. Un exemple de cette pratique est le Parti communiste de la république populaire de Chine, qui en raison de la dépendance quasi universelle des citoyens chinois aux applications mobiles telles que WeChat, impose désormais un système de crédit social.¹⁷ Ce système assigne un pointage à tous les citoyen(ne)s chinois basé sur une série de facteurs prédéterminés, et ce par catégorie sociale. Les citoyens pourront être classés en ordre de pointage, puis pourront se voir récompensés pour leurs prouesses ou punis pour leurs fautes. Par exemple, des citoyens pourront se voir refuser l'accès à un avion commercial ou à un train, refuser l'accès aux meilleures écoles du pays, refuser l'accès aux meilleurs emplois, refuser l'accès aux meilleurs hôtels et être publiquement nommé comme étant

¹⁷ China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you, 29 octobre 2018, <https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4>.

un mauvais citoyen.¹⁸ Ce système se définit comme étant un moyen très efficace et indirect d'ingénierie sociale qui n'aurait pas pu exister dans le passé.

DOCTRINE, STRATÉGIE ET TACTIQUES

Aujourd'hui, l'internet est le système nerveux de notre monde moderne et la communication électronique est l'arme de conviction massive. Nous utilisons l'internet pour tout, que ce soit pour rencontrer des personnes, pour le marketing d'affaires jusqu'aux nouvelles, mais c'est aussi une zone d'opérations qui est utilisée pour rencontrer les mêmes objectifs. Dans cette zone d'opérations cyber, ils existent des tactiques que toutes sortes de groupes utilisent afin de trouver des façons de gagner le web, de rendre un message viral et d'obtenir la crédibilité de la perception du publique. Toutes les technologies peuvent être utilisées pour le bien et pour le mal. Aujourd'hui, la première stratégie de la communication comme arme de conviction massive est l'inondation du web avec des fausses vérités et des histoires alternatives. Nous pouvons utiliser les sources ouvertes d'intelligence afin de propager des théories alternatives multiples en ligne afin que la vérité soit plus difficile à trouver. Ainsi, il a de la propagation de la désinformation, c'est-à-dire que les pépites d'or sont présentes mais elles sont cachées dans l'eau boueuse de l'internet. Cette stratégie, en plus de l'authenticité planifiée sont décrites dans les prochaines lignes de ce texte.

¹⁸ China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you, 29 octobre 2018, <https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4>.

Stratégie #1 - L'authenticité planifiée

La première stratégie de communication comme arme de conviction massive est l'authenticité planifiée exemplifiée par la chanteuse américaine très populaire Taylor Swift et le britannique d'origine pakistanaise Junaid Hussain, un leader de Daesh dans les domaines du piratage et de la propagande sur internet. L'authenticité planifiée survient lorsque quelqu'un s'engage personnellement avec ses fans ou ses recrues sur le web en toute connaissance de cause que le monde entier les observe, ce qui atteint deux objectifs parallèles: un effet de grande envergure et un effet personnel d'une personne à une autre. De son côté, Junaid Hussain, devient si percutant sur les réseaux qu'il se retrouve 3e sur la liste du Pentagone des plus recherchés du groupe radical islamique. Hussain, aussi connu sous le nom de guerre d'Abu Hussain al-Britani, a été un intervenant clé dans le groupe de piratage islamique avec ses gros coups tels que ses implications dans la modification et la déformation de sites web français lors de l'attaque terroriste de Paris en 2015, dans le piratage de comptes personnels de M. Tony Blair et dans ses gazouillis à partir des comptes Twitter du *US Central Command*, de *Newsweek* et du *International Business Times*.¹⁹ Junaid Hussain a utilisé l'internet, les réseaux sociaux et l'authenticité planifiée pour influencer un grand nombre de loups solitaires terroristes, et par conséquent porter atteinte à la vie et à la sécurité d'un très grand nombre de citoyens du monde.

Stratégie #2 - La désinformation

La deuxième stratégie de la communication comme arme de conviction massive est la désinformation moderne qui fut exemplifiée par les russes lors de la campagne présidentielle américaine de 2016. Cette tactique russe a trouvé des fissures dans la société américaine et a

¹⁹ Junaid Hussain, https://en.wikipedia.org/wiki/Junaid_Hussain.

exacerbé des dizaines de milliers de faux comptes Twitter dans le but de personnifier des personnalités sociales exubérantes sur Facebook dont la propagande atteint près de 140 million d'américains dans les derniers jours de la campagne. La collision du monde réel avec l'espace en ligne fut si percutant que les russes furent en mesure d'organiser un événement sur le sol américain à partir de leurs bureaux à St-Petersburg, et ce à travers des marionnettes proxies afin que des centaines de personnes se retrouvent dans la rue pour protester. Leur technique fut si efficace, qu'en utilisant la même tactique, ils étaient en mesure d'organiser une contre-protestation qui voyait maintenant deux groupes d'américains protester l'un contre l'autre dans les rues américaines. Un exemple de troll russe utilisé sur les réseaux sociaux fut Jenna Abrams, qui fut un sensation américaine suivie par 70 000 abonnés avant d'être exposée. En bref, les russes avaient une série d'armes non-létales dans leur arsenal de désinformation telles que l'attaque du consensus, les théories du complot, semer le doute, la sélection, le refus de données et les attaques personnelles.

Les élections présidentielles américaines de 2016 ont été hautement critiquées en raison de l'impact qu'aurait eu la désinformation ou "*fake news*", particulièrement via les réseaux sociaux, sur le résultat du candidat élu à la présidence. Selon Hunt Allcott et Matthew Gentzkow du *Journal of Economic Perspectives*, leur conclusion sur le sujet se traduit en quatre parties: 1) les médias sociaux étaient une importante mais pas une dominante source d'information sur les élections, avec seulement 14 pourcent des américains déclarant les médias sociaux leur plus importante source d'information; 2) dans les fausses histoires connues qui apparurent aux nouvelles dans les derniers trois mois avant les élections, ceux favorisant Donald Trump ont été partagé un total de 30 million de fois sur Facebook tandis que ceux favorisant Hilary Clinton ont été partagé 8 millions de fois; 3) l'américain moyen a vu dans l'ordre d'une à plusieurs fausses

nouvelles dans les derniers mois précédent l'élection avec un peu plus de la moitié des personnes qui se souviennent d'en avoir pris connaissance et de les avoir cru à cette époque; and 4) les gens sont plus enclin de croire les histoires qui favorisent leur candidat préféré, particulièrement s'ils ont des réseaux de médias sociaux idéologiquement distincts.²⁰ De son côté, le président élu Donald Trump est un utilisateur enthousiaste, méthodique et calculé de Twitter. Selon Brian L. Ott, dans cette nouvelle ère de la politique projetée via Twitter privilégie un discours simple, impulsif et non-civilisé selon une étude de cas du Président Trump.²¹

L'institutionnalisation aux niveaux régional, national et international de l'utilisation de la communication via l'internet est un travail en progrès. Notre société est-elle équipée et légiféré pour répondre efficacement aux effets de cette arme de conviction massive? Selon P.W. Singer et Emerson T. Brooking, auteurs de *LikeWar - The Weaponization of Social Media*, la Corée du Nord est probablement la mieux équipée pour gérer la sécurité et la défense cybernétique.²² Elle n'est pas mieux équipée parce qu'elle a plus de talent ou parce qu'elle est mieux organisée mais du fait qu'elle a une combinaison d'un régime autoritaire et qu'elle a autant de connections internet qu'un bloc de quartier de la ville de Manhattan. Ce contrôle très restreint qui évite de faire face à ces défis globaux est contrebalancé par une économie faible et peu de liberté individuelle. Tandis que certaines nations ont prouvés être capable de pénétrer les systèmes de d'autres nations, il se veut plus compliquer pour certaines nations occidentales de pénétrer les systèmes des autres. La solution n'est pas de devenir un régime autoritaire ou d'interdire les

²⁰ Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives*, 31 (2): 211-36.

²¹ Brian L. Ott (2017) The age of Twitter: Donald J. Trump and the politics of debasement, *Critical Studies in Media Communication*, 34:1, 59-68, DOI: 10.1080/15295036.2016.1266686.

²² Singer, P. W and Emerson T., Brooking, *Likewar: The Weaponization of Social Media*. Boston, Massachusetts: Houghton Mifflin Harcourt, 2018.

médias sociaux, mais de mieux les comprendre de s'ajuster à cette nouvelle réalité évolutive. Tel que démontré dans cette dissertation, l'utilisation de l'internet, des réseaux sociaux, des téléphones intelligents, des caméras et des capteurs représente aujourd'hui une disruption technique qui a sévèrement altérée notre réalité. Initialement hautement rattachées au monde corporatif, le fait que ces technologies semblent limitées aux frontières nationales n'est qu'une pure illusion. La nature même de ces corporations est trans-étatique, provoquant des défis de taille dans la législation de ces nouvelles technologies. Une citation illustre bien cet défi: "Des problèmes globaux requiert des solutions globales." En bref, la responsabilité ne réside pas uniquement en une seule entité mais elle est la responsabilité des gouvernements nationaux, des corporations et des individus, puis le défi sera d'éviter les écarts.

CONCLUSION

"Autrefois, tout le monde avait droit à sa propre opinion, mais pas à ses propres faits. Mais ce n'est plus le cas. Les faits n'ont pas d'importance. La perception est tout ce qui compte."

- Stephen Colberg

En conclusion, cette dissertation a illustré que l'utilisation de la communication en ligne est devenue une arme non-létale dans l'espace commun des relations internationales. À travers divers exemples de l'histoire récente, elle a exposé la présence croissante de la communication via l'internet comme une arme de conviction massive dans les conflits géo-politiques et stratégiques. Tel que démontré lors de la première bataille de Mosul, un objectif clair, des mots, des images et des vidéos sur le web peuvent avoir un impact stratégique sur l'issue tactique d'un champ de bataille. En constante évolution, la doctrine, les tactiques, l'entraînement et la législation de l'utilisation de l'internet, des réseaux sociaux et de la communication en ligne

gagnent à être connu et offrent des défis de taille aux citoyens, philosophes, académiciens, praticiens et juristes du monde entier. Avec l'émergence de l'intelligence artificielle, des algorithmes et de d'autres nouvelles technologies, quels défis affronteront nos enfants et les générations futures?

BIBLIOGRAPHIE

- Singer, P. W and Emerson T., Brookings, *Likewar: The Weaponization of Social Media*. Boston, Massachusetts: Houghton Mifflin Harcourt, 2018.
- Social Media use in the Military Sector, posted in General Security on 31 January 2013, <https://resources.infosecinstitute.com/social-media-use-in-the-military-sector/#gref>.
- US Department of Defense releases official policy on social media, <https://www.davidmeermanscott.com/blog/2010/02/us-department-of-defense-releases-official-policy-on-social-media.html>.
- Russia bans smartphones for soldiers over social media fears, 20 February 2019, <https://www.bbc.com/news/world-europe-47302938>.
- Attaque du centre commercial Westgate, https://fr.wikipedia.org/wiki/Attaque_du_centre_commercial_Westgate.
- Twitter in the Cross Fire—The Use of Social Media in the Westgate Mall Terror Attack in Kenya, <https://journals.plos.org/plosone/article/figure?id=10.1371/journal.pone.0104136.t002>.
- Gordon, Jerry, Israel's War with Hamas 2014: Part III - The Social Media Battle, August 2014 https://www.newenglishreview.org/custpage.cfm/frm/165962/sec_id/165962.
- Martin Rudner (2017) "Electronic Jihad": The Internet as Al Qaeda's Catalyst for Global Terror, *Studies in Conflict & Terrorism*, 40:1, 10-23, DOI: 10.1080/1057610X.2016.1157403.
- Use of social media by the Islamic State of Iraq and the Levant, https://en.wikipedia.org/wiki/Use_of_social_media_by_the_Islamic_State_of_Iraq_and_the_Levant.
- Ma, Alexandra, China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you, 29 octobre 2018, <https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4>.
- Junaid Hussain, https://en.wikipedia.org/wiki/Junaid_Hussain.
- Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives*, 31 (2): 211-36.
- Brian L. Ott (2017) The age of Twitter: Donald J. Trump and the politics of debasement, *Critical Studies in Media Communication*, 34:1, 59-68, DOI: 10.1080/15295036.2016.1266686.