Information Operations for Influence

(STO-MP-SAS-105)

Executive Summary

In 2012 the SAS panel identified two key trends impacting the contemporary operating environment. The first trend is the increased appearance of, and involvement by, non-state actors (NSAs) in violent conflict, whether as a proxy for a state or as the primary adversary. The second trend is the exploitation of the cyber-domain, in particular social media (Web 2.0), by NSAs to shape and manage the narrative and conduct informational warfare. Although NATO has achieved, on the whole, technical overmatch in the areas of intelligence, surveillance, and reconnaissance (ISR) and the employment of precision munitions and unmanned aerial vehicles in denied areas, they have nevertheless faced substantial challenges in achieving asymmetric advantage in the information environment (IE), and have been slow to embrace the broad range of opportunities to counter and defeat informational warfare. This includes, but is not limited to, the use of social media to manage the narrative and to shape behaviour of target audiences. The result has been the domination of the IE by our adversaries. Moreover, it can be argued that we have entered a new phase in the evolution of warfare – one in which the IE is the contentious ground and informational warfare is the preferred method.

The 2014 Information Operations for Influence (IOI) symposium provided an environment for the defence S&T community, academics, subject matter experts and operators to discuss issues and share knowledge related to the exploitation of the IE by various adversaries as well as extant and future blue force capability gaps and requirements to conduct operations in the IE.

In total, sixteen (16) speakers, representing seven (7) nations (Canada, United States, United Kingdom, Netherlands, Norway, France and Germany), addressed topics ranging from the use of street art as an influence activity through the evolution of Russian cyber-influence capabilities and the potential for using mistrust to disrupt threat networks. The facilitated discussion and brainstorming sessions of the symposium also proved particularly informative. As a result of these sessions, more than fifty-one (51) S&T challenge areas relating to information operations and informational warfare were identified and discussed. These challenge areas include, but are not limited to, intelligence support, the role of culture, modelling and simulation, deception detection, threat network disruption, message propagation, selection and training criteria, non-verbal communication and engagement, and non-kinetic targeting.

Two key takeaways were identified at the symposium. First, the IOI S&T challenge areas are incredibly diverse, cutting across social and applied science disciplines. Second, a number of capability and knowledge deficiencies exist, requiring significant S&T investment. Based on the findings of the symposium, a three-year RTG follow-on activity, focusing on the examination of emergent adversary informational warfare capabilities and the development of a guidebook and a training course for operators to counter adversary informational warfare, will be proposed.

Les Opérations d'Influence par l'Information

(STO-MP-SAS-105)

Synthèse

En 2015, la commission SAS a identifié deux tendances essentielles qui influent sur l'environnement opérationnel contemporain. La première tendance est l'apparition et l'implication accrues d'acteurs non étatiques (ANE) dans des conflits violents, soit comme mandataires d'un État, soit comme principaux adversaires. La seconde tendance est l'exploitation du réseau Internet, en particulier les médias sociaux (Web 2.0) par des ANE pour donner forme au récit, le charpenter et mener une guerre de l'information. Bien que l'OTAN soit parvenue, dans l'ensemble, à prendre techniquement le dessus dans les domaines du renseignement, de la surveillance et de la reconnaissance (ISR) et dans l'utilisation de munitions de précision et de véhicules aériens sans pilote dans les zones hostiles, elle rencontre néanmoins de grandes difficultés pour prendre l'avantage asymétrique dans l'environnement de l'information (EI) et a mis du temps à exploiter toute la palette des options permettant de l'emporter dans cette guerre de l'information. Cela inclut, sans s'y limiter, l'utilisation des médias sociaux pour rythmer l'information et orienter le comportement du public visé. Nos adversaires ont par conséquent dominé l'EI. De plus, on peut considérer que nous sommes entrés dans une nouvelle phase de la guerre, dans laquelle l'EI est le champ de bataille et la guerre de l'information est la méthode préférée.

Le colloque « Les Opérations d'Influence par l'Information » (OII) qui s'est tenu en 2014 a permis à la communauté S&T, aux universitaires, aux experts et aux opérateurs de la défense de discuter et d'échanger des connaissances sur l'exploitation de l'EI par divers adversaires, sur les manques de moyens actuels et futurs de l'OTAN et sur les exigences à satisfaire pour mener des opérations dans l'EI.

Au total, seize (16) orateurs, représentant sept (7) pays (Canada, États-Unis, Royaume-Uni, Pays-Bas, Norvège, France et Allemagne), ont abordé des sujets allant de l'utilisation de l'art urbain comme vecteur d'influence jusqu'à l'évolution des capacités russes de cyberinfluence, en passant par la possibilité d'utiliser la méfiance pour perturber les réseaux de menace. Les sessions encadrées de discussion et de brainstorming du colloque se sont également révélées particulièrement instructives. Plus de cinquante et un (51) domaines de S&T posant problème en lien avec les opérations d'information et la guerre de l'information ont ainsi été identifiés et débattus. Ces domaines incluent notamment le soutien du renseignement, le rôle de la culture, la modélisation et la simulation, la détection de la tromperie, la perturbation des réseaux de menace, la propagation des messages, les critères de sélection et de formation, l'engagement et la communication non verbaux et le ciblage non cinétique des objectifs.

Le colloque a abouti a deux conclusions essentielles. Premièrement, les domaines de S&T OII posant problème sont incroyablement variés et touchent les disciplines des sciences sociales et des sciences appliquées. Deuxièmement, il existe un certain nombre de faiblesses en matière de capacités et de connaissances, qui exigent un investissement de S&T conséquent. À partir des résultats du colloque, un RTG assurant une activité de suivi sur trois ans sera proposé. Il se concentrera sur l'examen des capacités émergentes de nos adversaires dans le secteur de la guerre de l'information et développera un guide et un cours de formation destinés aux opérateurs, afin de contrer les actions adverses dans la guerre de l'information.