

Information Technology for Crisis and Disaster Response

(STO-TR-HFM-248)

Executive Summary

The world of crisis, conflict and disaster has become deeply intertwined with information technology. When this research technology group was first formed in October of 2013, Euromaidan, the invasion of Crimea, and other significant events were unforeseen. There were precedents to suggest that information technologies, particularly the social media platforms, were important to understanding unfolding civil crisis, violence and disaster response. Understanding how to assess the information environment for rumour, critical information, emerging activities and events had become a critical capability.

Understanding information technology and how to navigate the information environment is a vital role in NATO military operations and will form a large part of the structure of the fighting forces of the future. However, military and government entities have been disadvantaged in developing effective approaches to managing information technologies. Policies and guidance had lagged technological advancement for years, but at the time this research technology group began, policies and guidance began to catch up. Adversarial information operations evolved rapidly, and the conflicts in Ukraine and the annexation of Crimea precipitated rapid changes in NATO's approach.

Researchers studying civil conflict noticed that Euromaidan was different. Within days of the protest, activists had created with their own cadre of public relations, reportedly young, professional journalists, united by a Euromaidan brand that included several different Twitter accounts, most notably @EuromaidanPR. An account to oppose the Euromaidan brand called @AntiMaydan, equally professional and equally active arose shortly afterwards. This was the first 'information war' in a civil conflict and it demanded close scrutiny.

In the months that followed, the invasion of Crimea by 'hybrid forces' showed just how timely this interdisciplinary research would be. In June of 2014, the Research Technology Group first convened in London, UK, hosting not only the major participants, but also military visitors from JFC-Brunssum and the UK, where they became the first to hear about botnets, influence operations, and the transformed information environment.

NATO JFC-Brunssum gained enormous value from its participation in this research technology group. It was a resource for advice, knowledge, and capabilities that were often urgently needed. Most importantly, the experience working with many researchers showed that an individual's personal knowledge and experience using Twitter is insufficient to understand the mass campaigns underwritten by strange and evolving technologies. Even experienced, everyday users of Twitter could not appreciate and understand the technical and social maneuvers being practiced by the adversary or predict their possible outcomes. Data science, information science, social science, computer science, and social network analysis all have their place in getting to the heart of the challenges facing NATO in current information conflicts. New tools and new science will definitely be needed in the years ahead. Engaging with research scientists in the efforts to better understand and apply new insights greatly improved NATO's response in information conflicts. Technical demonstrations to provide insights, advice, and the opportunity to learn cutting-edge techniques continues to be highly valuable as we look ahead to future collaborative research in this area.

Les technologies de l'information dans le cadre de la réponse aux crises et aux catastrophes

(STO-TR-HFM-248)

Synthèse

L'univers des crises, des conflits et des catastrophes est désormais profondément imbriqué avec celui des technologies de l'information. Lorsque ce groupe de recherche technologique a été mis sur pied en octobre 2013, Euromaidan, l'invasion de la Crimée et d'autres événements importants n'étaient pas pressentis. Pourtant, des précédents suggéraient que les technologies de l'information, en particulier les plateformes de médias sociaux, étaient importantes pour comprendre le développement des crises civiles, la violence et les interventions en cas de catastrophe. La compréhension de la façon d'évaluer l'environnement informationnel – avec ses rumeurs, ses informations critiques et ses activités émergentes – et les événements était devenu une capacité essentielle.

La compréhension des technologies de l'information et l'aptitude à naviguer dans l'environnement informationnel sont des fonctions essentielles dans les opérations militaires de l'OTAN et constitueront une partie importante de la structure des forces combattantes de l'avenir. Cependant, les entités militaires et gouvernementales ont été désavantagées dans l'élaboration d'approches efficaces de gestion des technologies de l'information. Les politiques et les directives avaient pendant des années pris du retard sur les avancées technologiques; toutefois, au moment où ce groupe de technologie de recherche a été créé, les politiques et les directives ont commencé à le combler. Les opérations d'information contradictoires ont évolué rapidement, et les conflits en Ukraine et l'annexion de la Crimée ont entraîné une modification rapide de l'approche de l'OTAN.

Les chercheurs qui étudient le conflit civil ont remarqué qu'Euromaidan était quelque chose de différent. Quelques jours avant la manifestation, des militants s'étaient regroupés avec leur propre réseau de relations publiques, apparemment des jeunes journalistes professionnels, réunis par la « marque » Euromaidan qui incluait plusieurs comptes Twitter, notamment @EuromaidanPR. Un compte destiné à répondre à la « marque » Euromaidan et appelé @AntiMaydan, tout aussi professionnel et actif, est apparu peu après. Ce fut la première « guerre de l'information » dans un conflit civil et à ce titre elle mérite d'être examinée en profondeur.

Dans les mois qui ont suivi, l'invasion de la Crimée par des « forces hybrides » a montré à quel point cette recherche interdisciplinaire était opportune. En juin 2014, le groupe de recherche technologique s'est réuni pour la première fois à Londres, au Royaume-Uni, accueillant non seulement les principaux participants, mais également des militaires de JFC-Brunssum et du Royaume-Uni ; ceux-ci ont à cette occasion été les premiers à entendre parler des réseaux d'ordinateurs (botnet), des opérations d'influence et de la transformation de l'environnement informationnel.

Le JFC-Brunssum de l'OTAN a tiré un bénéfice considérable de sa participation à ce groupe de recherche technologique. Elle lui a fourni des ressources en matière de conseils, de connaissances et de capacités qui étaient souvent nécessaires de toute urgence. Plus, important encore, l'expérience acquise auprès de nombreux chercheurs a montré que les connaissances et l'expérience personnelles d'un individu utilisant Twitter sont insuffisantes pour comprendre les campagnes de masse élaborées à l'aide de technologies inconnues et en évolution. Même expérimentés, les utilisateurs quotidiens de Twitter ne pouvaient

ni comprendre ni évaluer l'ampleur des manœuvres techniques et sociales pratiquées par l'adversaire, ni prédire leurs résultats possibles. La science des données, la science de l'information, les sciences sociales, la science informatique et l'analyse des réseaux sociaux ont toutes leur place pour relever les défis auxquels l'OTAN est confrontée dans les conflits de l'information actuels. De nouveaux outils et de nouvelles données scientifiques seront certainement nécessaires dans les années à venir. Les collaborations avec des chercheurs pour mieux comprendre et mettre en œuvre de nouvelles idées ont considérablement amélioré la réaction de l'OTAN en cas de conflit de l'information. Les démonstrations techniques offrant des perspectives, des conseils et l'opportunité d'apprendre des techniques de pointe continuent d'avoir une grande valeur alors que nous sommes tournés vers l'avenir de recherche collaborative dans ce domaine.

