NORTH ATLANTIC TREATY
ORGANIZATION

SCIENCE AND TECHNOLOGY
ORGANIZATION

AC/323(HFM-248)TP/868

www.sto.nato.int

STO TECHNICAL REPORT **TR-HFM-248**

Information Technology for Crisis and Disaster Response

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

Final report of NATO HFM-248.

Published November 2019

Distribution and Availability on Back Cover

NORTH ATLANTIC TREATY
ORGANIZATION

SCIENCE AND TECHNOLOGY
ORGANIZATION

AC/323(HFM-248)TP/868

www.sto.nato.int

STO TECHNICAL REPORT **TR-HFM-248**

Information Technology for Crisis and Disaster Response

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

Final report of NATO HFM-248.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

•	AVT	Applied Vehicle Technology Panel
•	HFM	Human Factors and Medicine Panel
•	IST	Information Systems Technology Panel
•	NMSG	NATO Modelling and Simulation Group
•	SAS	System Analysis and Studies Panel
•	SCI	Systems Concepts and Integration Panel
•	SET	Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published November 2019

ISBN 978-92-837-2192-5

Table of Contents

List of Figures

Acknowledgements

We would like to thank NATO Collaborative Support Office, Frank Wessels and Marie Linet, for their gracious help and support. NATO Allied Command Transformation Operational Experimentation's effort to lead and develop the four-day meeting was essential to the task. We would especially like to thank Katie Hughes and Major Andreas Bauer for bringing together this event who made that event possible. We'd also like to thank the many people at NATO Public Diplomacy Division, Mark Laity and Chris Riley, for the conversations, invitations, and opportunities they so generously gave this community. We also would like to thank Col. David Dinger at JFC-Brunssum and General Hans Damrose for the opportunity of working with them on Trident Juncture 15. Last but not least, we'd like to thank Maj. Alistair Green, Joseph Pascoguin and the many people at JFC Naples who hosted NATO ACT's Limited Objective Experiment.

We also owe a special thanks to our mentor, Dr. John Tangney, for all the assistance, advice and help that made these activities possible and enhanced their effectiveness.

HFM-248 Membership List

CHAIR

Dr. Rebecca GOOLSBY
Office of Naval Research
UNITED STATES
Email: Rebecca.Goolsby@navy.mil

MEMBERS

Maj. Danel APSE
Headquarters of Estonian Defence Forces
ESTONIA
Email: danel.apse@mil.ee

Mr. Paul CHATELIER
Naval Postgraduate School
UNITED STATES
Email: pchat@mindspring.com

Maj. Dr. Erik DE SOIR
Royal High Institute for Defence
BELGIUM
Email: erik.de.soir@telenet.be

Dr. Leonard FERRARI
Office of Naval Research – Global
UNITED STATES
Email: lferrari@nps.edu

Maj. Rick GALEANO
Joint Forces Command Brunssum
UNITED STATES
Email: rick.galeano@jfcbs.nato.int

Dr. Clinton HEINZE
Australian Defence Staff
AUSTRALIA
Email: clinton.heinze@defence.gov.au

Ms. Maria WINGATE
Australian Defence Staff
AUSTRALIA
Email: mayka.wingate@defence.gov.au

Dr. Pille PRUULMANN-VENGERFELDT
University of Tartu
ESTONIA
Email: pille.vengerfeldt@ut.ee

Dr. Marc VAN DEN HOMBERG
TNO Den Haag
NETHERLANDS
Email: marc.vandenhomberg@tno.nl

Dr. Katie WOODWARD
Dstl Portsdown West
UNITED KINGDOM
Email: klwoodward@dstl.gov.uk

PANEL/GROUP MENTOR

Dr. John TANGNEY
Office of Naval Research
UNITED STATES
Email: John.f.tangney@navy.mil

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 destiner 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.

Chapter 1 – INTRODUCTION AND BACKGROUND

> *[In October, 2010, John Holdren made]...a tremendous presentation on climate change, and the bottom line of his presentation was when he looked at the audience and said there are three strategies in dealing with climate change: suffer, adapt, or manage.*
>
> *I thought long and hard about what he'd said in regard to the environment and it struck me that social media, the 7/24 news cycle, the Internet, the power of computation today … with all this collectively, media has created a change in our political, social, economic, and behavioral environments. I would consider social media, the Internet, and everything related to that as being the sociological equivalent of climate change. It doesn't matter whether you like it, embrace it or not, the fact of the matter is it just is.*
>
> *To steal the paradigm from John Holdren, when you're talking about social media and the complete immersion in information, I think there are three strategies: suffer, adapt, or manage. I chose to adapt and manage.*
>
> – Admiral Thad Allen, (USCG-ret.) in an interview on the BP oil spill, November 2010 [1].

In 2013, when this Research Technology Group was established, Euromaidan and the events of 2014 were ahead. 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. And then, just three weeks later, something else popped up – an account to oppose the Euromaidan brand, an account called @AntiMaydan, equally professional and equally active.

This was the first 'information war' in a civil conflict and it demanded close scrutiny. Rumours and indications pointed to the distinct possibility that @AntiMaydan could be a professional, state-backed response, the first of its kind. But run by whom? Ukraine? Russia? U.S.-based computer scientists began their investigations, discovering the traces of computer-assisted manipulations of Twitter streams, while social scientists at a small circle of universities began to consider the transformation of Russian military approaches to warfighting.

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.

1.1 THE NEW INFORMATION ENVIRONMENT AND SOCIAL GROUPS: THEORETICAL PERSPECTIVES

The human factor in understanding the information environment has often been afterthought. The prior modes of mass communication were characterized by one-to-many transmissions: newspapers, radio, television, even media that was developed more for groups, such as movies and fine art, focused on the individual as consumer, as a re-actor, rather than an actor. One of the key aspects of what makes the information environment 'new' is the immense uptick in the number of information actors who are capable of creating, transmitting and receiving information on a mass scale, in real-time. People are also capable of working together more effectively in social groups, to achieve aims and create effects, without a hierarchical organizational structure.

Information platforms provided much of the world's populations with access to information capabilities that dramatically transformed social relationships, including the relationship between civil authorities and citizens. This changing relationship was the original focus of this research technology group.

Social theory continues to try to catch up with the phenomenon of online social behavior. The problem of misunderstood relationships in these environments, which occurs easily, has led to the deliberate manipulation of the knowledge gap among people online. This is where dezinformatzya, disinformation, has found fertile soil to capture, suborn and develop online social groups wrapped around a variety of ideological axes that may not conform all that much to the full range of perspectives and interests of the group members as individuals. Disinformation becomes misinformation. Many information actors deliberately attempt to steer the curious and the easily misinformed into membership in groups that they do not understand. These phenomena were impossible to miss during the three years of this research technology group.

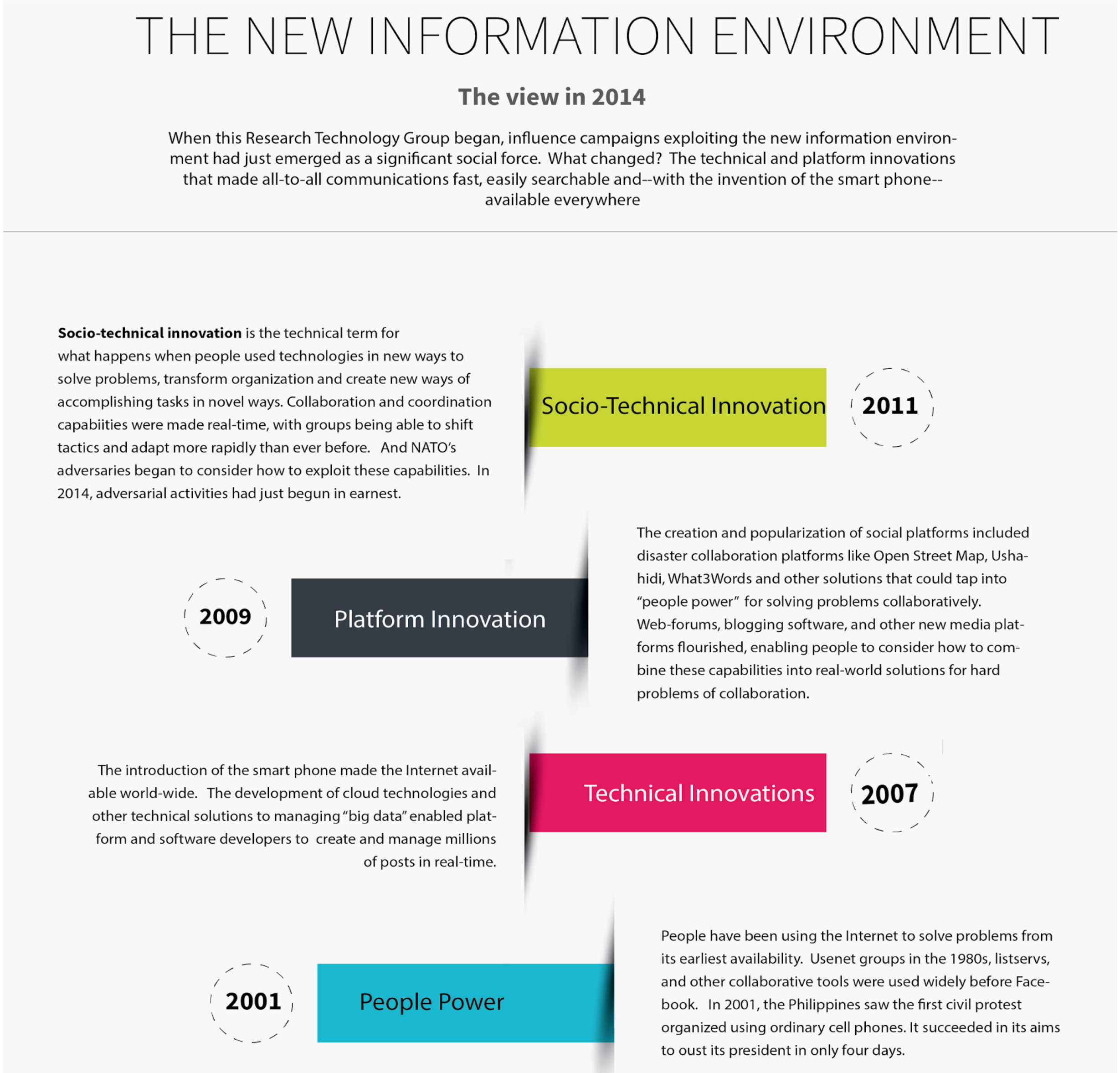
According to Derek Layder, a British sociologist, the social world consists of four intersecting domains:

- First, psychobiography: the domain of the individual, consisting of their psychological characters, as well as their biographical experiences;
- The second domain is situated activities: where interpersonal interactions happen;
- Third, the domain of social networks consists of friends, colleagues, peers and acquaintances that inevitably influence the experiences of people; and
- The fourth domain is the contextual resources, the more abstract concepts of rules, norms and regulations, located in and for investigative purposes mostly represented by various institutions [2].

In 2007, Brian Solis observed that the new information environment is "90% sociology, 10% technology" [3]. Layder's formulation touches on the transformations that have occurred in all of these domains in the new environment of social media and digital communications on social platforms such as YouTube, Blogger, WordPress, Skype and other environments. Solis' original calculus has shifted somewhat, due to the emergence of machine learning and software development. The new information environment is 'new' because of these social transformations. It is also 'new' because of the change in the basic information technologies and their rapid, global availability: cell phones, the Internet, and the other devices and technical capability. To paraphrase McLuhan, the medium still matters very much [4]. The new information environment has expanded the role of technology in the last five years, with great accelerations from 2014 onward (see Figure 1-1).

This transformation can be thought of as having three layers:

- The Technical and Platform Layers: the information architectures, mobile platforms and devices and methods of handling rich data streams. Moore's law, the observation that basic computing capacity doubles every year, is just one part of the equation [5]. The development of architectures that could take advantage of this rapid growth in capacity, such as cloud computing, enabled software platforms to manage and distribute information at unheard of scales. The Economist magazine called this the "Data Deluge" in 2010 [6].
- The Social Layer: the social use of new technologies to create, validate, and distribute information through personal, local, regional and global networks. This involves real social networks of people who know each other face to face and the rapidly evolving phenomena of cyber-social groups that are connected primarily – or entirely – by Internet capabilities.
- The Socio-Technical Layer: The combination of these layers to develop novel capabilities for a wide variety of novel outcomes, including new crowd effects. These innovations occurred in many different world contexts.



THE NEW INFORMATION ENVIRONMENT

The view in 2014

When this Research Technology Group began, influence campaigns exploiting the new information environment had just emerged as a significant social force. What changed? The technical and platform innovations that made all-to-all communications fast, easily searchable and--with the invention of the smart phone--available everywhere

Socio-technical innovation is the technical term for what happens when people used technologies in new ways to solve problems, transform organization and create new ways of accomplishing tasks in novel ways. Collaboration and coordination capabiities were made real-time, with groups being able to shift tactics and adapt more rapidly than ever before. And NATO's adversaries began to consider how to exploit these capabilities. In 2014, adversarial activities had just begun in earnest.

The creation and popularization of social platforms included disaster collaboration platforms like Open Street Map, Ushahidi, What3Words and other solutions that could tap into "people power" for solving problems collaboratively. Web-forums, blogging software, and other new media platforms flourished, enabling people to consider how to combine these capabilities into real-world solutions for hard problems of collaboration.

The introduction of the smart phone made the Internet available world-wide. The development of cloud technologies and other technical solutions to managing "big data" enabled platform and software developers to create and manage millions of posts in real-time.

People have been using the Internet to solve problems from its earliest availability. Usenet groups in the 1980s, listservs, and other collaborative tools were used widely before Facebook. In 2001, the Philippines saw the first civil protest organized using ordinary cell phones. It succeeded in its aims to oust its president in only four days.

Figure 1-1: The New Information Environment.

Technology intersects all of the four domains of the social worlds. Today, psychologists and neurologists are beginning to argue whether all of these intensive exposures to technology are bringing about fundamental changes in human brains. But while this point is still an area of open scientific inquiry, what is more clearly evident is that the biographies of individuals are clearly being affected by their connections with online societies and platforms. Important experiences are often mediated by technologies, and every day, habitual experiences of the world are embedded in texts, emails, and participation in technology-mediated spaces. More and more situated activities are located in the digital space – we meet other people and interact with them in the digital networks. But increasing number of encounters experience we also when the encounter partner is technology – self-service technologies, online banking, online governance, etc.

Our encounters with our societal structures are mediated through technologies and we form our experiences based on them. Often in traditional space, we form our understanding of police force based on the one policeman we meet. Today, the experience of police as a concept might be mediated by radar, traffic cameras, and the website used to pay for tickets. These technology-mediated experiences also have a role in forming attitudes and understandings of who the police are, what the public thinks is the police's attitude toward civilians, and all of this can color the face-to-face concept when those experiences do occur. Similarly, in absence of individual encounters with people, we form our experiences of military based on the websites or online communication we experience. Human experience of other people through online social platforms has expanded the individual's experience of a social network, reinforcing ties with distant, possibly rarely seen others. Our experience of peer-pressure, our experiences with communication, all becomes increasingly mediated by the digital platforms. The fact that the structures of our society, the domain of contextual resources are also become increasingly digital means that there is an increased expectation of uniformly digital experiences.

Platforms of communication provided by new technologies shape our experiences. We expect things online to work in certain ways. If those online experiences don't conform in ways we think are essential, professional, and appropriate, we may deem the organization or entity to be incompetent, uncaring, and unworthy of trust.

Domains of social networks are also affected by technologies, with online social networking services become synonymous with what individuals perceive to be what others (including scientists) mean when we speak of 'social networks'. Online social networking platforms create social worlds that can be as small as two people, or as large as hundreds, thousands, and more – in addition to the face-to-face, real-world social networks. Platforms like Facebook blend online and real-world social networks. Individuals one 'meets' online every day may develop more compelling influences than with face-to-face relationships. Understanding the social worlds operating in the intersections of these four domains helps also to understand that while an individual message carries often very little weight in today's society, which is saturated with information and messaging, the totality of the communication experiences consists of a larger variety of things.

1.2 SOCIO-TECHNICAL INNOVATION AND SOCIAL CHANGE

The effects of these transformations have had enormous impact in terms of accelerating change, facilitating the development of political voices of crowds and coordinating group behaviors. Early warnings and concerns about possible negative impacts and misuse were overshadowed by their obvious, potent capabilities against corruption and despotism in the first years of significant societal shifts [7], [8].

We see the most striking effects in 2001, with the 'EDSA 2' protest in the Philippines. The cell phone had only been introduced a few months before the protest, but the services available to get a landline had long been insufficient. Cell phone subscriptions filled a great need in Filipino households that had had little or no access to phones. Cell phones capability to store every phone number that a person needed was essential to making these phones easy to use. The new 'texting' function kept cell phone costs down, since data rates were much cheaper than phone call rates. Being able to send 'group texts' – texts to one's whole family, for example, to invite everyone to a party – also kept costs down – making one message contact many people, for a very small charge.

Encoding a message – putting meaning into a face-to-face utterance, a text, a tweet, a picture/meme – refers to the attempts to create and then transmit a message. Decoding a message has to do with receiving and interpreting that message. Stuart Hall, an anthropologist writing in the 1960s, explained that there are in every communication act, we encode our outgoing messages based on our experiences (or, as Layder would term them, tempered by our psycho-biographies), which include our knowledge [9].

In January 2001, Filipino activists working to unseat President Joseph Estrada used cell phones and this group messaging function to transmit a simple message: Come to EDSA, Wear Black [10]. Wearing black allowed those coming to EDSA to readily identify others in their cause, without knowing them personally. EDSA (Epifanio de los Santos Avenue) had been the site of the 1986 revolt that had ousted Ferdinand Marcos; it thus had particular political significance to those seeking to oust Estrada in January of 2001. When a sufficiently large crowd had gathered, radio and television coverage spread information about the protest. The use of cell phones to gather a crowd for civil protest is an example of socio-technical innovation – people using technologies in new ways to solve problems, coordinate action, and promote organizational change. All of these messages were encoded in clothes, in terms of place (the EDSA town square), and in terms of prior knowledge and experience.

Social science, media, and communications research talks about this encoding and decoding of experiences. The main argument would be as follows: In every communication act, we code the messages we send (this can happen in face-to-face communication, written or broadcasted) based on our experiences (our psycho-biographies to use the idea from the domains). We use the vocabulary, but also cultural understandings that we have experienced to encode or construct the messages. People who receive the messages usually decode them based on their own psycho-biographies – their knowledge, their understanding of the world, etc. Clifford Geertz explains that there is a richness of experience, knowledge and context in both encoding and decoding these experiences, with plenty of problems in encoding, transmission, reception, and interpretation possible [11]. But in 2001, with only a limited amount of transmission space in terms of phone bandwidth – and social networks limited to the number of phone numbers available on people's phones – activists were able to simplify the message and reach a crowd of significant size leveraging a great deal of social and cultural experience and knowledge to create a communication that easily translated from text message to event to mass media.

A great deal depended on also making most of the right moment. By 2009, many different civil protests had used cell phones and the new and emerging platforms of Twitter and Facebook, with increasing effectiveness – but also with a number of failures. Egyptian activists had tried twice before to rally people to Tahrir Square, using cell phones and Twitter, and met with failure. Technology was a tool but not a magic wand for coordination of crowds and orchestration of events.

During the period from 2001 – 2010, software platforms for exchanging information began to pop up on the information landscape. Bulletin boards and Usenet groups of the 1980s gave way to Web forums. LiveJournal, Blogger, and WordPress followed, providing new platforms for community information exchange; websites design improved and become easier to do; and bandwidth for transmission of complex and elaborate media became cheap and readily available, paving the way for YouTube. Twitter and Facebook entered an information landscape that needed a conduit for crowdsourcing the distribution and validation of this new content. The combination of the widely available 'smart' phone that could access Internet content with the growth of the cell tower capacity to manage high volume uploads of photographs and videos were the ingredients that pushed the information landscape into a new dimension.

The critical change in the information environment has been the capability for ordinary people to innovate in how they use information to organize their activities, maintain situation awareness about the world around them, and become aware of news that affects them. Disaster and crisis response teams were among the first to leverage these new capabilities and continue to be key innovators in media. By 2008, innovators in crisis response had begun to develop 'apps' and platforms, such as the Ushahidi platform and OpenStreet map. By 2010, innovators in disaster had begun to integrate these apps into robust solutions for collaborative effort, including the use of SMS on a large, many-to-many scale and dedicated Skype channels, Facebook pages, and Twitter topic groups for information collection, validation, and management capabilities that were used to great effect in Haiti in 2010. The Arab Spring in 2011 was probably the key event that showed the potential power of these changes.

1.3 ETHICAL CONSIDERATIONS FOR MILITARY USE OF GENERATED DATA

As acknowledged throughout this report, military and government entities have been at a disadvantage in developing effective approaches to manage information technologies. Whilst some policy and guidance has indeed caught up during the duration of this research technology group, some key ethical considerations remain fully addressed.

Debates on the ethics of conducting these types of online military information operations have largely been rolled up into, and are currently indistinguishable from, wider ethical debates on the use of cyber weapons [12], [13], [14], [15]. Yet judging by press reports, 21st century online information operations may share features more in line with traditional political covert action and espionage – in particular, a focus on covert intelligence gathering to support military messaging [16], [17], [18]. These factors change, exacerbate and bring to the fore old ethical dilemmas – questions that include rights to privacy, what it means to be a combatant or non-combatant in a theatre of conflict, and what constitutes legitimate conduct in attempting to deceive an adversary.

The ethics of privacy intrusion have historically barely registered as a *jus in bello* concern – largely out of scope of the law of armed conflict, and more often considered in conjunction with the ethical considerations of espionage. However, the volume of data that humans are placing on the Internet about themselves and others is increasing exponentially. To the military analyst and/or information operator, such data holds the potential to inform understandings on topics including identity and belonging, social structure, networks of power and ideas, feelings and sentiment, motivations and interests, norms of social behavior and cultural reference. Such understandings may be considered deeply invasive. Military understandings of privacy in practice are not clear.

The historic *jus in bello* concern with proportionality can be applied to this debate. Proportionality is intertwined with what actions are necessary. In practice, necessity begins with data collection: Is the collection necessary, and is it proportionate to the object to be achieved? In the interests of protecting privacy rights of data subjects, if necessity can be established, the least invasive (but practicable) methods should be considered the most proportional. This means that a wide range of methods may be considered ethically justifiable depending on the circumstances of necessity.

Having a reference point is required by which to judge the degree to which data collection is proportionate and necessary – a strong case being the relationship to publicly held privacy norms. But which public, where? Should the reference point be taken from the community from which the collector comes, or the communities in which the data owners are likely to reside? Alternatively, from the online community norms of the platform from which the data is being taken? This is further complicated as the delineation between which aspects of social life are public and private (which vary notably by culture) are often blurred online.

Here, it may be useful to consider an estimation of the intent of the individual data subject. In subscribing to platforms such as Twitter, which are essentially broadcast platforms, and uploading their personal content, does this imply the user is aware that their personal content has become public? When offering up personal information on sites such as Facebook have users just overlooked their account's privacy settings? However, even if this can be resolved, just because a blogger, for example, has reached out to the public, does this mean that governments can help themselves to the same data?

Aiming to obtain consent from data subjects may remove the need to estimate their intent. When we look at the example academic disciplines in this area (which include anthropology, psychology, media studies, computer science) all share an ethical feature. All disciplines demonstrate a commitment, one way or another, to gaining informed consent from informants or research participants. This often consists of setting out terms and conditions and asking participants to provide their consent by checking a box. However, when trying to apply these principles to real-world scenarios it becomes problematic. Firstly, there is the practicality of trying to obtain consent from potentially many millions of subjects in a given collection. Secondly, the nature of social life on some platforms many undermine the ethical value of informed consent requests. For instance, in online forums where anonymity is valued, alerting users to the presence of a researcher may not only cause anxiety but also disrupt the natural social context.

Once data has been collected and an understanding of audiences developed, operators may seek to plan communications based on what has been learned. However, are there, and should there be, limits to who can be targeted in this manner? *Jus in bello* debates have historically considered delineations of legitimate and illegitimate targets during armed conflict. This is reflected in international law, with the category of 'combatants' considered legitimate targets (subject to rights contained within the Geneva conventions and Customary International Humanitarian Law), civilians are considered 'non-combatants' and therefore are exempt from targeting.

Conducting information operations using the Internet creates or exacerbates at least three ethical dilemmas relating to the delineation of legitimate and non-legitimate targets. Firstly, in targeting civilian populations through information operations directly – at what threshold do such activities become illegitimate? Secondly, with users self-uploading data, at what point could their behavior cause the civilian to become a 'combatant'? Finally, there is the issue of using and appropriating civilian infrastructure to conduct operations, and potential collateral damage, including reputational, caused to this infrastructure. The latter two issues, especially, relate to wider ethical debates underway regarding cyber conflict more generally.

Information operations may be aimed at adversarial, neutral and friendly populations and forces. Unlike typical applications of lethal force, such operations may be specifically targeted at civilian populations (non-combatants). Intentional law prohibits the use of physical force against non-combatants but there are substantial ethical issues involved in targeted civilians even where there is no physical harm. Such issues concern psychological harm, specifically the unjustness of transgressing the rights of those who have not transgressed the rights of others. Psychological harm can be very difficult to determine given the variation in ways a given individual may respond. For example, will the transmission of false, morale damaging messages has the potential to increase suicide and/or homicide risk amongst a civilian population? How can we avoid impacting vulnerable audiences such as children? This is a major issue for online information activities, particularly as degree of operational control is necessarily ceded early. After all, once released online the messenger has little control over the subsequent use of any message. Content can 'go viral' in ways unintended and impact new, previously unforeseen audiences. For instance, the message may undergo distortion and manipulation or simply run the risk of being grossly misunderstood once removed from its initial context.

Furthermore, over recent years the number of civilian 'experts' collecting and analyzing data on humans from internet sources has increased including, but not limited to, data scientist, intelligence analysts, behavioral scientists and linguistic specialists. But at what point, if at all, does a civilian expert fall into the category of 'combatant'? This is a perennial problem in military ethics. However, it is also one that has been discussed as an issue for cyber conflict more generally. It is after all, a problem entangled with issues of geography and interdependence in a globalised and networked world where an operator can potentially access their target set from anywhere in the world, given an internet connection.

Moreover, the use of civilian infrastructure is essential to the delivery of online information operations. Not only the Internet platforms the target audience accesses the message via, but also the hardware it is accessed on, and the network infrastructure messages travel along, which are unlikely to be geographically bound and may run through neutral or allied countries as well as the domestic jurisdiction [12]. The issues that emerge involve the commercial terms and conditions placed upon users. This includes limits on how data can be used, restrictions on using fake identifies, and explicit restrictions within terms and conditions on how government organizations can harvest and use data from platforms. Insufficient consideration of these points could lead to the undermining of commercial legal structures.

Lastly, the Internet offers an exponential increase for actors to engage in deceptive behavior. Whilst the Chinese strategist Sun Tzu claimed, “All warfare is deception,” ethically there are limits to which measures are acceptable. This is reflected in the Law of International Armed Conflict (LOIAC) where deception – which is defensible, is separated from perfidy, which is not [19].

Posing as a Red Cross Medic to entice an adversary to drop their guard to kill them has been agreed under international law as a step too far. An online analogy might be a commander who is enticed by a beautiful female to meet at a location where they are assassinated. Is this perfidy? What about spreading rumours about an adversary that leads to execution by their own state/group? What about exposing facts about a military target that puts their life in danger? Or bullying, shaming, or otherwise discrediting and individual to the point where they take their own life [20]?

It is evident that there is no clear answer to such ethical dilemmas and any form of conclusion on the matter is unlikely to be fixed; what constitutes necessity and proportionality in future crisis and conflict situations will depend on many factors. Noting the apparent disadvantage of militaries and governments in developing effective approaches to manage information technologies such concerns should not unduly hamper research and innovation. There will be a pervading need to identify and understand target audiences – individuals, groups or populations – allowing messaging campaigns to be tailored in line with the inferences made about the audiences. The effectiveness of the messages must be understood and fed-back into an updated understanding of the audience. Further messaging may continue this iterative cycle of understanding and exploitation.

At the very least, it is recommended that researchers within such an environment should be cognisant of the following key points:

- Each activity should begin by considering a) is the collection necessary? And b) is it proportionate to the objective to be achieved?
- Proportionality should be determined with reference to ethics as refracted through global and local debate. That is, attention should be paid to current local and global attitudes towards online privacy.
- Proportionality should consider the method by which the data is accessed technically. The more intrusive the methods required to access and harvest data, the higher the level of privacy sought (simultaneously raising the necessity bar).
- Where practicable and un-harmful, informed consent should be gained from data subjects.
- Where informed consent is not practicable consideration should be given to estimate the intent of the data subjects when self-uploading data taking into account privacy norms of the platforms from which data is taken.
- If messaging campaigns involve the use of false online profiles with little or no connection to the operator the delineation between deception and perfidy should be considered and risks relating to the possibility of death, injury or capture, or other indirect side-effects of messaging should be fully accounted for in operational activity.

It is clear this is complex area, requiring much further debate. In the interlinked areas of proportionality and privacy, delineations between combatants and non-combatants, and limits to acceptable deceptive practices, new online means require updates in the ethical debate – and the legal response. However, creating 'soft' effect via information activity can preclude 'hard' effect, involving destruction and loss of life – potentially allowing military objectives to be achieved with less suffering. Ethical considerations may be easily justifiable in conflict on the basis of such necessary ends and providing a critical reference point by which any discussions of ethics are considered.

1.4 THE BEGINNING OF ADVERSARIAL ACTIVITIES

In 2013, when this Research and Technology Group was conceived, the problem of adversarial use of social media was already evident. In India, cell phones had been used to promote a hoax that had caused Muslims to swamp Indian railway stations in order to return to their homes in Assam. In 2012, responding to false SMS messages, young Muslims had been led to believe that Hindus were descending upon Muslims living in the region in a rage of civil violence, similar to an event that had occurred some months before. In that same year, Bangladeshis in rural areas had attacked police outposts due to outrage sparked by a Facebook post, killing twelve police officers with machetes. Bloggers in Bangladesh had been attacked and killed on the streets over Internet fuelled allegations of 'atheism'. And in 2008, in Mumbai, terrorists had used social media to coordinate armed attacks, while at the same time; people used those same Internet-based capabilities to assist civil authorities to track the terrorists in real-time [21]. The use of these new technologies for crowd manipulation and social hysteria propagation were already of significant concern to crisis responders.

Tracking rumour and attempts to influence crowds was high on the agenda of the Research Technology Group at its inception. This interest was heightened by the invasion of Crimea that began in early 2014 – and the initial use of botnets to disseminate pro-Russian messages, including distracting messages and distorted information designed to manipulate world opinion through an aggressive adversarial information campaign.

1.4.1 Botnets and Social Influence

The Russian information campaign against the West has never truly abated. Scientists noted that the extension of this campaign into the new information environment could be detected at least as early as 2009 [22]. In 2014, the first evidence of Botnets as significant purveyors of rumour and Russian-bias opinion surfaced during the invasion of the Crimea.

The creation of computer code to feed information into multiple Twitter accounts and disseminate a rumour or opinion is not a terribly difficult feat for experienced programmers. In 2014, the use of Botnets was not a common method of social influence outside of commercial advertisement or 'spam'. Much of Russian information operations appear to be the simple purchase of commercial advertisers experienced in this kind of activity ('spamming') to carry adversarial messaging against NATO (and others). This appears to continue as of 2017.

'Political astro-turfing' was another common use of fake Twitter accounts before 2014. This involves the purchase of 'fake' Twitter accounts by the thousands that would become followers of a target account on Twitter. The objective of this was to bump up the account's apparent influence to people who might look at the account but also to achieve another, more hidden effect that was just as important: the higher the number of followers one has, the more important that Twitter's underlying algorithms think one is – and the greater the spread of that account's messages by those algorithms.

Tricking Twitter's algorithms has great advantages. The higher an account's influence score (as measured by these algorithms), the more likely that account's tweets are to appear in other user's timelines. Further, the higher that score is, the more likely that account is to be 'recommended' for other accounts as an important account for others to follow.

Twitter's algorithms are proprietary and thus unavailable; researchers can only guess how they work. Commercial operators who use botnets (also called 'Botnet operators' or 'bot-herders') do have techniques, developed through trial-and-error experiments, but these are trade secrets. Russian information operations appear to have simply purchased the services of Botnet operators around the world who maintain botnets that target audiences grouped around specific topics and languages.

Botnets are arrays of bots attached to Twitter accounts, coordinated by scripts (computer code) that automate and synchronize the sending out of messages into Twitter. This code enables the botnet operator to feed identical messages into each fake account, causing scores, or hundreds or thousands, of these messages to flow into the world of Twitter.

There were a number of patterns of message amplification using botnets and those patterns evolved in the last three years. Originally, in 2014, the scripts simply issued an identical message across multiple accounts. Technologies used to assess open source materials often found many accounts carrying identical messages, often with a URL connected to a Russian media organ, usually Sputnikt.Int or RT.com in its various language editions. After 2015, 'retweet' bots were more common, with a 'feeder' account carrying the message that was echoed by the rest of the botnet through retweeting.

Twitter attempts to craft its terms of service, and its algorithms, to discourage bots and hamper their operation. Commercial bots compete with its own attempts to capture advertising revenue. Twitter's algorithms have a certain level of auto-detection of these manipulation methods, a cursory means of detecting and suspending offending accounts that violate terms of service. Bot programmers have discovered work-arounds that outpace Twitter's capacity to contain them.

In 2014, Russian media began to use botnets on Twitter to spread the Russian strategic message. With bot accounts tweeting Russian media stories over and over again through these bots, these outlets sought to get their stories in front of potential audiences and to entice those audiences to expose themselves to the Russian perspective using messages carefully encoded as objective reporting.

Decoding can happen in three dominant ways. According to Umberto Eco, there are four ways in which we can decode the message:

- We can be model readers and understand the message as it was intended;
- It may be that readers can't decode the message at all: it may be in the wrong language, for instance;
- We may be readers who miss the context or just do wrong reading of the message – we can decode it based on our experiences, but miss parts of the code unintentionally; and
- Some readers may do aberrant coding, where, while understanding the code, deliberately engage in a twisted meaning; for instance, for ideological reasons or because we don't trust the sender.

These last types of reader engage in deliberate refusal of the messages. Thus, it is not only the matter of ignorant audience who just does not get what we want, but it can be also a rebellious audience who are deliberately counteracting our messages.

Will message-senders encounter model readers in their audience, who receive, decode and behave in the expected way? Will they encounter aberrant readers – including readers who retransmit, distort, and develop alternative interpretations counter to the message sender's intentions? And what about the audiences in the middle, who are misreading, depending on their own personal psycho-biographies, situated activities, social networks and contextual understanding and resources? Which way will they fall in the conflict – into the intended interpretation or into the aberrant deliberate distorted interpretation?

Where these audiences fall can be dependent on the past experiences of the individual, ongoing encounters in which the message is received, the group norms and peer-pressure or the overall societal context. One could argue, that these days, the societal context is increasingly challenging norms and authority and through the talk of fake news, we have experienced delegitimization of the authority and validated many counter-readings that were previously considered unimaginable. If the societal narrative is about everyone having a right to have their own version or truth, we also have made it very difficult for any public institution to engage in authoritative messaging.

Social networks have also increasingly fostered what could be called filter bubbles – the algorithmic selection of materials we experience in digital media, where our interests and preferences are considered to give us often one-sided view of things. While the research about existence of the filter bubbles is contradictory, there is a certain selection bias based on our own decoding practices. We tend to agree more with the information that fits our previous experiences, thus the filter bubble we live in is not necessarily of technological origin, but affects our decoding of messages, nevertheless. We tend also to surround us with peers and social networks who share similar decoding models. Some of them come from growing up with the same cultural experiences (like almost everyone in Western hemisphere knowing about Mickey Mouse, but Pippi Longstocking is known well in Scandinavia and Baltics), some are developed through shared life-experiences (getting the #metoo or the families understanding of what a proper Thanksgiving dinner should look like). These decoding mechanisms are connected to the social networks we belong to.

Theoretically, the individual encounter with botnet is not supposed to count. It has been expected that it will not affect an audience's experiences and most likely will encounter resisting coding, as it does not get the code. At the same time, continuous messaging affects the social fabric and can alter the structures of communication and interpretation. It may affect also the social context in which the communication happens, altering the messages that are next to it through altering the context of decoding.

José van Djik talks about platformisation of society [23]. She argues that the platforms of FB, Twitter, Google and Amazon have formed parts of the societal structure. They have not only been spaces where the social communication happens, they are also part of shaping the communication as they have become part of the institutional fabric, the contextual resource domain. Through their logic of operation, the cultural norms, values and practices have been altered. For instance, un-friend was not a concept that existed before Facebook platform logic made it necessary.

Building trust is a slow thing – as said, one message does not matter. It is important to have regular valuable encounters with the contextual resources, with the institutions of the society. These encounters carry the power to alternate the decoding patterns through positive experiences. It is usually considered more valuable to have direct communication; face-to-face encounters are most meaningful and most impactful, but direct messaging through social media platforms, following platform logics can also be very important. Broadcast media, as it is usually attempting to gather positive decoding from diverse audiences is also often the least impactful as there are more possibilities for aberrant reading.

1.4.2 The Russian Information Maneuver Strategy (2014–2015)

Shortly after the Crimean invasion, Jolanta Darczewska outlined the theory and practice of information conflicts, introducing concepts and providing essential groundwork for understanding their impact on the information environment and target audiences [24]. Darczewska asserted that the Russians used difficult to detect methods to "subordinate the elites and the societies in other countries by making use of various kinds of secret and overt channels (secret services, diplomacy and the media)" to conduct operations of psychological impact, using methods of ideological and political sabotage. Their aim was to create an 'information front' in which to create a competitive information mirage, a hazy vision of the real-world of relationships and events that could hide, distort, and masquerade as objective facts. The inventors of this front sought to put forward a strategic communication vision that relies on an uncontested conflict space to be effective.

Darczewska asserted that Russian campaigns are highly coordinated with state actors, employing all the federal television and radio channels and well positioned as a coordinated strategic communication effort, an effort that was "years in the making":

> *The information front was supported by diplomats, politicians, political analysts, experts, and representatives of the academic and cultural elites... At the time of the Ukrainian crisis (the Euromaidan), it was combined with ideological, political and socio-cultural sabotage, provocation and diplomatic activity... Following the military occupation and incorporation of Crimea into Russia, the disinformation mechanisms were aimed at lending credibility to Moscow's intentions and concealing the gaps in the argumentation for military moves and the annexation of the Crimea itself. These arguments were absurd, such as: it was feared that... 'the Black Sea Fleet bases could be taken over by NATO,' 'Ukrainian citizens would be de-Russified' and so on and so forth* [24].

Russian information war strategist Igor Panarin casts the West in the role of information warfare aggressors. Panarin claims that the so-called 'color' revolutions in the CIS area and the 'Arab Spring' were a product of social control technology and information aggression from the United States. According to Darczewski, Panarin defines basic terms of Russian information conflict strategy as:

- Social maneuvering: the intentional control of the public aimed at gaining certain benefits;
- Information manipulation: sing authentic information in way as to give rise to false implications;
- Disinformation: the spread of manipulated or fabricated information, or some combination of both;
- Fabrication of information: the manufacture of false information; and
- Lobbying, blackmail and extortion of desired information [24].

In 2013, reporters from the St. Petersburg Times infiltrated a covert organization that hired young people as 'Internet operators'. The employees were "paid to write pro-Kremlin postings and comments on the Internet, smearing opposition leader Alexei Navalny and U.S. politics and culture" [25].

> *Moscow mayoral election. The first comments to the posting read "Do not believe a word by Navalny (ruserk91)," "His words don't mean a thing!!! He forgets what he says the moment he says it!!!" (koka_kola23), "If Navalny comes to power, he will sell our country to hell! He's simply sent from the U.S." (Vasily Sergeyev) and "America trains people to run our country. Navalny is a typical example of such an agent" (sorts2013)*

> *Another blog entry he referred to as an example of the company's work was a posting criticizing American films while praising Russian ones. "Each [American film] is a flawed film […] for, dare I say it, a flawed nation," a blogger using the moniker onerus1 wrote on Aug. 26.*
>
> *According to Novaya Gazeta's local correspondent Alexandra Garmazhapova, whose report was published on Sept. 9, Soskovets said the blog postings should be based on the given 'vectors' but look like they were written by real people, rather than generated by Internet bots. "For instance, you can write that the G20 summit is a great honor for Russia, but it's inconvenient to get home [due to road closures]," she quoted him as saying.*
>
> *Garmazhapova wrote that Soskovets claimed that the organization was active in several cities, including Moscow* [25].

This kind of organized, orchestrated campaign is an example of what Darczewska refers to as activities of 'information special forces' (or 'spetsnazes') whose role in the past has been that of "disinformation, verbal provocation and intimidation techniques described by Panarin" [24].

> *Emotional and hateful language is used in online news and polemics. They contain numerous obscenities and abusive vocabulary, such as 'pederast' or 'liberast'. Biased and tendentious interpretations of events are also highly prominent in them. The cult of Putin as Russia's successful leader and defender is clearly visible. The picture of the world is simplified and painted in black and white (where the diabolic West is black, and Russia is white). The image of the ideological opponent is clear and deprived of empathy. The opponent is discredited not only ideologically but also aesthetically ('that Bandera creep', 'the editors' ugly mugs'). Propaganda also performs discrediting (opponents) and the accrediting (inspirer) functions. These functions have an impact on its role in image-building (PR), agitation and propaganda (p. 27)* [24].

During the period from 2013 to 2015, pro-Russian and anti-Western diatribes infested the comments in news organizations, on blogs, in YouTube and other social media platforms all over the Internet, making some conversations difficult to pursue without persistent and annoying 'thread-jacking' – the change of topic in a 'thread' of discussion in an open forum.

What possible impact could such a strange, fragmented yet orchestrated campaign have on public opinion? Why would the Kremlin care about blogs, Twitter, and web forums? What result or objective did the Kremlin have in sponsoring and promoting such information manoeuvres? What is the point of the expansion of such noisy, disjointed information attacks?

1.5 THE DEVELOPMENT OF INFORMATION MANEUVERS (2014–2015)

In 2015, Ben Nimmo's work on the "4 Ds of Russian Disinformation" broke down the Russian strategy into a fairly inclusive set of tactics used by Russian information actors to manipulate crowd perception [26]. He shows how one can categorize all of these attempts to hijack critical thinking into four primary tactics: dismiss, dismay, distort and distract. Just about any message or message set in adversarial information operations will fall under one of these four tactics. These tactics can be combined to accomplish ***information manoeuvres*,** which are a higher order set of information actions that are orchestrated to achieve a specific effect. Typically, we see the combination of two or more of the 4Ds, wrapped around a current topic of interest or a more primordial frame. Nationalism, patriarchy/family, ethnic exceptionalism (and ethnic grievances, hates) are typical examples of these primordial frames.

Most people have issues and concerns that impact their core emotions. For some people, it might be a well-known, frequently discussed political issue of some controversy (such as abortion, civil rights, or ethnic pride), while for others it might be animal rights, UFOs, the tax system, the rights of rape victims, or any number of issues that they feel strongly about to the point of having a very fixed point of view on the topic. 'Hot button issues' are everywhere, often hidden below the surface, but when people are confronted with a well-crafted 'hot button' piece of information, especially if it comes up unexpectedly, they can experience a sudden, unconscious surge in their emotional state, preventing their ability to think.

Amygdala hijack is a psychological term for the phenomena that occurs when a person becomes so inflamed and emotional that they can no longer access the critical reasoning centers of the brain. Neuroscientists have performed fMRI studies that demonstrate that when people are in that state, they are physically unable to access the cerebral cortex, the rational centers of the brain where critical reasoning occurs. Further, in that state, people reject any additional information that might show this information to be wrong. The brain stem goes into 'fight or flight' mode and the individual cannot psychologically handle new information.

In 2014 and into early 2015, the West's attempts to counter to disinformation attacks on Western societies, Western leaders and political figures, and Western institutions fared poorly. People in heightened emotional states would not accept new information in these situations where social hysteria propagation had found vulnerable targets. Other methods to psychologically manipulate those who could not be brought into full amygdala hijack were also brought into play, but the amygdala hijack was a very powerful means of producing 'knee-jerk' reactions in target audiences and those strong reactions could induce deep uncertainty and worry in their social circles, even if they themselves were not in that emotional state.

Targeting negative emotions – fear, anger, and disgust – proved to be an effective manoeuvre in directing discourses down a dark, winding path to paranoiac negativity that served Russian purposes well. Over the course of this research technology group's three-year existence, this manoeuvre was improved, developed and expanded, not always with perfect results.

1.5.1 Trident Juncture 15

In 2014, adversarial information operations were mostly disinformation campaigns related to Russian media actions in the Ukraine and Crimea. By 2015, NATO had ramped up multi-national exercises, beginning with Dragoon Ride 2015 in March of that year. At this point, Russian adversarial information operations centered on attempts to degrade NATO's reputation through bot campaigns associated with the usual Russian media organs, RT.Com and Sputnikt, but also through promoting content through a variety of conspiracy blogs and websites.

NATO JFC-Brunssum had provided active participants and opportunities for interchanges between the Research Technology Group and its brand new social media analysis cell beginning in early 2014. A year later, NATO JFC-Brunssum's social media cell began considering the impact of anti-NATO messaging on its own operations, beginning in March with Dragoon Ride 2015. the beginnings of Russian information campaigns directed at NATO exercises caused considerable concern as to how to understand what was happening, whether or not these campaigns were having impact, and in general, how damaging these campaigns might be. General Hans-Lothar Domröse, the commander of Trident Juncture 15 invited the Research Technology Group to attend the three-week, LIVEX (live) portion of Trident Juncture 15, to provide a hands-on technical demonstration of new and developing technologies to monitor the information environment.

This three-week exercise provided the opportunity for NATO scientists and NATO communicators to work side by side for the first time. It was an eye-opening experience for everyone. For the scientists, it was their first opportunity to experience the everyday battle rhythm of public affairs and to interact daily with communicators who had needs and requirements requiring immediate assistance – from social science and computer science. Scientists involved in this effort returned to the experience with new ideas for urgently needed research, technical development ideas, and a greater appreciation of the evolving battlespace in the information environment. A great deal of understanding and appreciation of the problem of bot-enhanced adversarial information campaigns was gained during the period from June to November, in preparation for Trident Juncture 15. Scientists began to get a full understanding of the problems that NATO communicators faced: their priorities, their 'battle rhythm' and the challenges of the often exhausting pace of military exercises. Technologies needed to be tweaked, or invented, to keep up with the pace of information flow.

For NATO communicators, discussions with scientists and demonstrations of technologies brought a new realization about the role of technology in shaping discourses, spreading rumour and the growth of group polarization. The technical demonstrations at Trident Juncture introduced the idea of information environment assessment to NATO Public Diplomacy Division, which would ultimately develop into a plan for the NATO Digital Working Group.

1.5.2 Brilliant Jump 16 and Anakonda 16

NATO Public Diplomacy Division (PDD) continued the conversation about information environment assessment with the Research Technology Group at the NATO TIDESPRINT event in Krakow, Poland in April of 2016. NATO's improved understanding of the technical and socio-technical new information environment enabled NATO Public Diplomacy Division to develop its practices and expand its narratives in constructive ways, to 'fill the space' with more and better messages. This also developed a new demand signal for more training and exposure to new technologies from NATO forces, which led to yet another opportunity associated with the NATO Strategic Communications Center of Excellence.

1.5.3 NATO Strategic Communications Center of Excellence

The NATO Strategic Communication Center of Excellence (Stratcom COE) was stood up in September of 2014. From 2014 and into 2015, NATO Stratcom COE held teleconferences with members of the Research Technology Group to rapidly identify and address the key problems facing NATO in strategic communications. Over the years, new researchers were added, and new capabilities developed at the COE. The breadth and depth of the research done by this center is impressive by any measure. Research Technology Group members were invited to attend the COE's annual workshop in April 2016. With the success of this workshop and driven by the interests of NATO PDD, NATO Stratcom COE began to consider the development of a larger workshop for its stakeholders, in military and government for 2017. The Research Technology Group was invited to co-develop this workshop with them.

Under the leadership of Col. Maris Tutins, NATO Stratcom COE developed the workshop with RTG members in a series of meetings and teleconferences that introduced new technologies and research to a NATO stakeholder audience. Twenty-six students from seven nations attended the four-day workshop in March 2017, where they studied social network analysis, blogs, and different forms of Twitter analysis from a more academic perspective but geared to an introductory student audience.

1.5.4 Information Environment Assessment (2016–2017)

The TIDESPRINT event in Krakow, Poland in April of 2016 had given researchers and NATO communicators the opportunity to discuss a way forward for intvroducing more technology in the NATO communication strategy at all levels. NATO Public Diplomacy Division saw the need for a broad strategic planning group, which could facilitate this transformation, and, with considerable consultation with NATO-SHAPE, instituted a new committee, the NATO Digital Working Group, which held its first meeting in Brussels in November of 2016.

Chapter 2 – OPERATIONAL EFFECTS IN SUPPORT OF JOINT FORCE COMMAND BRUNSSUM

Joint Force Command Brunssum's initial interaction with Research Technology Group 248 was the result of 'information needed now' as a result of the Euromaidan crisis in Ukraine. The Ukrainian crisis generated a substantial increase in the digital information environment about these events, impossible to monitor with the then-current methods and approaches, creating a 'black hole' in situational awareness along the eastern border of NATO. This information black hole was being filled with large amounts of data via social platforms such as Vkontakte, Instagram, Twitter, blog networks, and others; all mixed in with opinion, disinformation, crowd sourced maps, and photographs and video from the events themselves.

The information was overwhelming: the sheer volume and the multitude of languages (Russian, Ukrainian, and other European languages) made assessment especially challenging. In response, Joint Force Command Brunssum (JFCBS) requested support from the Research Technology Group (RTG) to provide the expertise needed to establish an effective system for information environment assessment; many weeks of lecture, discussion and question-and-answer sessions between the RTG and Brunssum resulted in a faster, more effective response to a rapidly unfolding situation.

Joint Force Command Brunssum recommended an appointment of one of their officers to this Research Technology Group (RTG) that was made up of several experts from across NATO nations from 2014–2017. The RTG provided several opportunities during this time frame to evaluate and test academic theories and software in support of digital experimentation. As mentioned, the previous chapter, adversarial information operations evolved rapidly during this period, while JFC-Brunssum's need for new capabilities, workflows, and tools had to be constantly adapted to the rapidly changing environment.

The RTG provided clear with guidance on a practical approach to support digital information monitoring, focusing on discourse and narrative. JFCBS observed messaging surrounding Euromaidan that was changing, and the message flows themselves often changed the content of the discourses very rapidly. The strategic orchestration of messaging to achieve the goals of a nation-state actor caused great concern. JFCBS became increasingly knowledgeable and aware about the influence of social media realm in mobilizing support and disorganizing legitimate information flows.

2.1 SOCIAL MEDIA MESSAGING AND NARRATIVE CHANGE

Twitter provides a number of means for interaction on its platforms: likes, retweets, and retweets with an additional message, and replies to tweets, as well as the means to 'follow' (or be followed by) other participants on the platform. These means shape the social rules, principles, and strategies that people use to increase their followers. 'Follow-back' is one of those strategies: that is, after following an account, a user will request that the account followed reciprocate and 'follow' their account. Strategies such as 'I follow you, you follow me' and 'you follow me, I follow you' seemed to have a very positive impact on improving the communicative reach of accounts by enlarging the social networks that might receive one's tweets.

In the last several years, a new artificial means of amplifying followership has emerged in the form of 'social bots' – scripted codes that mimic human users and serve as super-spreaders of information, commercial content, opinion, malware, self-promotion, promotion of news stories, or advertisement through fake Twitter accounts – that is, Twitter accounts not associated with an individual person but established as a means to fool Twitter's algorithms to spread messages. These scripts are capable of pushing messages onto the Twitter platform at very high volume, tricking Twitter's algorithms to register these messages as emanating from many users, rather than one.

These artificial methods can be used to promote particular points of view and disinformation, far beyond the reach of ordinary accounts using normal methods. Blogs, videos, and other content can be promoted this way, making disinformation seem more real or compelling than objective ground truth. These methods can change a conversation and/or the narrative significantly.

Researchers involved in the RTG engaged in an initial research project focused on the hostile take-over of the Crimean Peninsula, the messaging ultimately was changed to misdirection and focused the topics around the water crisis that was subsequently directed at the Crimean Peninsula. This study, previously published by the NATO Strategic Command Center of Excellence, identified and described the new tactics observed in the Ukrainian discourse including misdirection, smoke-screening, thread-jacking, and hashtag latching.

Early bots were not difficult to detect. Many had errors in coding, often consistent errors, which helped re-searchers to discern their signatures and confirm their identities as bots. In the beginning, bots simply carried identical messages at large scale. Later a slightly more sophisticated pattern was detected: the use of a central 'feeder' bot that could be followed by peripheral or 'child' bots, with messages from the 'mother' or 'feeder' disseminating through retweets by the 'children'. This replicated the 'follow-back' strategy and helped to trick Twitter's algorithms to evaluate those messages as sufficiently important to be placed higher in the stack of tweets vying for a top spot when people searched on the relevant topic, keyword or hashtag. 'Discourse suppression' – displacing the tweets of legitimate, human voices when others search for information with information to distort the conversation, change the subject, or introduce noise and uncertainty – seemed to be the primary objectives during this early period.

Researchers conducted an initial research project focused on the hostile takeover of the Crimean Peninsula, using Twitter data to identify the bot campaigns associated with this and subsequent anti-NATO discourses from 2014 until the run up to Trident Juncture in 2015. By focusing on disin-formation and distortion campaigns, the study showed that the use of bots to amplify such messages resulted in campaigns of misdirection, smoke-screening, 'thread-jacking' and hashtag latching. The study of these early efforts was recently published by the NATO Strategic Communication Center of Excellence [27].

The Dragoon Ride exercise occurred early, in March of 2015; the seeders of information to the bots were not as easily identified, as they would be after more data that had to be analyzed. During Dragoon Ride, a small number of bots were discovered to be coordinated to seed Twitter with distorted stories about NATO. Individually these bots were not very influential but collectively they appeared to have impacted the dissemination of NATO public affairs efforts. Both social networks and communication networks of the bots were examined to identify the organizational structure of the propaganda dissemination pro-cess. More tools were brought to bear on the Twitter streams, both by researchers and by JFC-Brunssum's newly created social media analysis cell. Testing and evaluation of the different sets of software assisted in TJ15 analysis. Ultimately, a combination of all tools was used in order to better 'paint the picture' for the technical demonstration.

Nitin Agarwal's 'focal structure analysis' technique was used to help identify powerful coordination structures among these botnets and trolls. Working with the RTG group, the JFC-Brunssum member worked with Dr. Agarwal to study how the FSA algorithm could be used to identify the group of coordinators and information spreaders and distinguish it from those merely picking up the information – the existence of a group within a larger group. This study set the parameters of study for the up and coming Trident Juncture 2015. It allowed the RTG to get a foothold on the dynamic changing information environment and for JFC-Brunssum to better understand what to look for in the information environment.

JFC-Brunssum social media analysts were exposed to sophisticated approaches to network analysis including the focal structure analysis approach prior to and during Trident Juncture 15. This enabled NATO communicators to become more aware of the rapid evolution of botnets deployed for propaganda dissem-ination. Working with multiple research institutions, JFC-Brunssum's social media cell began to be able to use their knowledge to develop better techniques to investigate the role that bots play in NATO communi-cations, enabling them to be more prepared for information conflicts associated with Trident Juncture 15.

Initially, there was a steep learning curve; the information environment was rapidly changing, sometimes within minutes. New software tools also complicated the situation. The software learning curve was over-come with one-on-one training from multiple universities associated with the RTG and by continued use of the software as part of the Trident Juncture 15 technical demonstration. Later, other exercises benefited from technical demonstrations and reach-back activities such as Brilliant Jump 16 and Anakonda 16. NATO Public Diplomacy Division (PDD) used these experiences and the knowledge they acquired from these efforts to suc-cessfully lobby for the creation of a NATO Digital Working Group to help rapidly transition and institu-tionalize knowledge gained from this Research Technology Group and spur further developments in the area of information environment assessment.

2.1.1 Lessons Learned from Trident Juncture 15

Trident Juncture 15 (TJ15) LIVEX was prodigious for NATO Public Affairs. This historic effort provided the largest deployed use of information forces communicating factual information via NATO mediums in NATO history. TJ15 was also the first concept cell of a Deployable Digital Production Unit. Prior to the exercise research was done and provided through a variety of contracted efforts. These reports were helpful but also distracting. The creation and activation of the NATO Media Information Center (NMIC) provided a well-rounded, multi-national communications hub for all information activities including the RTG technical demonstration. The NMIC coordinated efforts around four Operational Effects (OEs) to focus the overall messaging campaign.

While NATO operators handled all messaging, the technical demonstration team supported by examining and monitor-ing the information environment to provide insights, occasional advice, and practical knowledge about what the audiences were saying about NATO, how their messaging was spreading, and how particular campaigns were faring on a daily basis. The technical demonstration incorporated the operational effects into the overall effort for academic research, looking for signs and indicators of effectiveness of particular tweets, accounts, and campaigns during the exercise. On site co-location with NATO communicators enabled the technical demonstration to provide some small but effective guidance to NMIC leadership for message amplification with increased engagement in Twitter.

One value of the technical demonstration was in lifting this burden from the social media production unit so that they could concentrate on fulfilling the OEs. From the first day, the technical demonstration team made recommendations to significantly increase the amount of messaging, particularly during certain times, and to amplify that messaging via multi-ple platforms, such as Twitter, Facebook, Instagram, YouTube and websites by cross-posting (tweeting about a YouTube video, for example). While this seemed obvious to the academics, NATO communicators were concerned about 'spamming' their audiences. The researchers were able to show that very large upticks in messaging would be highly beneficial and would not 'wear out' their audiences as Twitter's own algorithms would support this uptick and would assist in metering out their message without causing a feeling of 'too much, too quickly'.

An advantage of having the technical demonstration team conduct analysis was in getting feedback on new tactics and approaches to messaging in Twitter. The use of humour, the inclusion of pop culture references (such as the #BacktoTheFuture campaign) and other tactics in messaging could be conducted by the production cell, with the analysis handed off to the (more objective) technical demonstration, to help evaluate and assess the impact of these novel information manoeuvres. Production cell social media producers could bring these assessments forward to help command leadership understand the value of these new campaign ideas with confidence that the statistical findings were unbiased.

Because of the co-location, social media production cell members could discuss with analysts how to craft a message to support the OEs regarding the overall communication plan based off of how the audience was reacting. The RTG team members could work on comparing of different kinds of posts fared in terms of retweets, likes, and other types of behavior, giving the production team more time to concentrate on content development.

Insights into counter-messaging were particularly valuable. It is difficult for a production team to both create content and be aware of counter-messaging. Content creation is intense activity, calling for creativity and technical capabilities that are different from analytical skills. Knowing what information was flowing around NATO's messaging helped the production cell have confidence in crafting their messages and campaigns. Having access to analytics and skilled researchers to help make sense of those new tools greatly shortened the learning curve.

One final but important lesson learned was the need to provide sufficient backup equipment and trained IT personnel. Bandwidth requirements for the public affairs efforts were considerable. The technical demonstration team from the Research Technology Group were well aware of these requirements and brought with them that equipment and trained personnel, providing for the participation of an expert advisor, Mr. Brian Steckler, from the U.S. Naval Postgraduate School, along with five graduate students. Their efforts support and knowledge substantively assisted in the execution of the public affairs mission. They provided much needed advice, backup equipment and solutions to solve problems on the ground to keep public affairs going despite unforeseen failures and constraints.

2.2 CONCLUSION

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 very insufficient to understanding the mass campaigns underwritten by strange and evolving technologies alone. Even experienced, everyday users of Twitter could not appreciate and understand the technical and social manoeuvres 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. As we look ahead to Trident Juncture 18, technical demonstrations to provide insights, advice, and the opportunity to learn cutting edge techniques continue to be highly valuable.

Chapter 3 – AN OVERVIEW OF SOCIAL MEDIA RESEARCH ACTIVITIES (2014–2017)

3.1 INTRODUCTION

The focus of this research program is to build a foundation for understanding social media as an object of modelling in order to develop tools and methods for analysis.

This work has benefited from, and has contributed to, the trans-disciplinary expertise resident in RTG-HFM-248. Established collaboration with the other researchers in the Research and Technology Group has already had considerable impact on the evolution of this work program, mainly through the experience gained in participation in discussions over the life of Trident Juncture 15, and in planning for the subsequent exercises. The international collaboration that is an inherent feature of these exercises and the consequent nature of information operations over social media has resulted in an improved understanding of the contested information environment that can be incorporated in capability development. Additionally, exposure to social media analysis tools that are in use in the other nations has given rise to new ideas for the possible applications of these tools. This has led to a broadening of our research program and subsequent improvements in the development of the Australian social media tool suite, RAPID (described in a later section). As an example, the pervasive use of botnets observed by NATO researchers resulted in a more targeted investigation of Twitter discussion dynamics, with a particular focus on discussion initiators and subsequent respondents. This has become a major feature of our research program.

3.2 A NETWORK PERSPECTIVE ON SOCIAL MEDIA INTERACTIONS

The approach we take in this research is based on the theory of social networks and the large body of knowledge in the area of Social Network Analysis (SNA).

Networks of social relations and interactions can shed light on processes leading to the flow and exchange of information, attitudes and behavioral intentions. In particular, social network theory posits two important axioms on which most network measures are based: network structure affects collective outcomes, while locations within networks affect actor outcomes [28]. Although these are foundational principles that can be used to guide the development of measures for dynamic social interaction networks, it is important to remember that in these networks, actors are linked by virtue of time-stamped interactions not static relations. Traditional social network analysis measures (e.g., degree centrality, betweenness, density, closeness, etc.) that are used to understand, describe and analyze social networks are based on the assumption that all ties exist concurrently and do not fully account for the temporal nature – and sequential order – of interactions.

Previous research has assumed that pre-existing theories of offline communication (e.g., SNA) can be directly applied to online communication. Yet, the social media environment is associated with certain idiosyncrasies and restrictions that are not present in the offline interactions from which these theories were developed. Although online communications may be formally represented as social interaction networks, it has been noted that they are not simply the cyberspace counterparts of offline social networks [29] – individuals can easily connect and freely interact without ever having to meet as persons. A fundamental premise of SNA is that the ties in a social network are typically assumed to be concurrent over the analysis period. In contrast, the social media interaction space is like a semi-structured fluid that constantly changes its shape. It is a network formed from highly dynamic digital traces rather than concurrent dyadic relations and requires new data collection and modelling strategies that allow us to follow the unfolding of social issues and to model information spreading individuals and organized systems of botnets through tailored data collections.

One approach to counter such problems is to explicitly deal with the temporal nature of these as networks of social interactions rather than networks of meaningful relationships.

3.3 REPRESENTATION AND ANALYSIS OF TWITTER ACTIVITY

Given the current availability of public Twitter data and our ability to observe retweet/mention/reply activities, can we develop sensible models that help us understand what makes certain Twitter messages and/or their propagators more influential than others?

Social influence is not merely exerted through direct communication. It is enabled by all kinds of interactions, perceptions and external events, many of which are unobservable by the analyst. As with all attempts at model development, assumptions are inevitable. The aim of this investigation of Twitter activity was to frame the analysis questions from a dynamic network perspective using assumptions based on the results of a survey on information sharing behaviors on Twitter. So, what are the aspects of message spread that are appropriate to model given the available data and analytical methods?

A conceptual model of information spreading on Twitter was proposed for initial investigation, (Figure 3-1) (see Ref. [30]). In this model, message senders choose to either broadcast or discuss information on Twitter according to their motivations, perceptions of their imagined audience, and content/context features of the tweeted message. Who receives this tweet (the message receiver) will be dependent on the diffusion strategies that the message sender uses and the subsequent choices that the message receiver makes. Message receivers may then continue to spread the information by discussing or broadcasting the tweet in turn or they may adopt the role of passive consumers. Passive consumers are users who do not produce content on Twitter but passively read the tweets of others. They may continue to share the content of the tweet in other social networks (online or offline) or the information may instigate some change to their own attitudes or beliefs.

Social activity in the Twittersphere occurs at different scales of time and virtual space. In particular, in order to exploit the range of digital data that are readily available, consideration was given to three classes of activity that can be represented as Twitter networks, and that range in duration from sequences of instantaneous events to comparatively long-term relations. These three types of networks characterize in turn:

1) The diffusion of information, opinions, ideas, etc. manifested through retweets;

2) Discussion thread dynamics (dynamic online communities, publics, etc.); and

3) The connectivity of followers and friends.

When considered in the spatial dimension, their coverage ranges from local virtual neighborhoods to the whole connected network. The focus of analysis is on the temporal network paths over which continuous flows connect pairs of nodes, either directly or via other nodes. In this way network actors and their inter-relationships are described in terms of their position on one or more paths (e.g., source, destination, at the intersection of paths, etc.), and the network structure is described in terms of flow patterns.

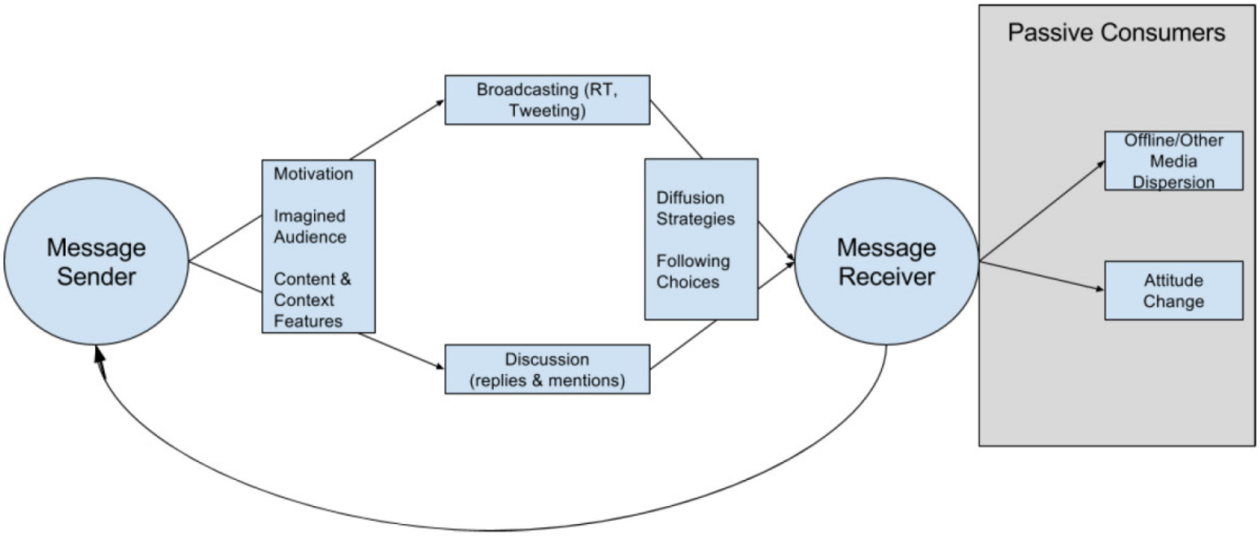


Figure 3-1: Conceptual Model of Information Spreading on Twitter [30].

3.3.1 Strategies for Data Collection, Refinement, and Structuring

Twitter represents an idealized platform for individuals to rapidly and widely share information with others. The ease with which data can be sourced through Twitter's API has resulted in a disproportionate number of big data studies aimed at assessing what information is most widely propagated through the 'Twittersphere' network and why. The focus on digital data has led researchers to overlook the importance of 'small data': traditional methods of data collection, such as survey and experimental studies. Although big data can measure the impact of Twitter messaging in terms of observable retweet/mention/reply behavior, the richness at the level of the individual could be lost if big data approaches are exclusively used, and therefore lead to inappropriate generalizations and conclusions. A way to address this shortcoming is to synthesise these two approaches by using a survey and social network methodology and collect both forms of data to explore Twitter behavior [31].

A comprehensive survey was designed on the basis of a model of Twitter information-sharing informed by prior literature. In all, 173 active and registered Twitter users answered questions relating to their:

1) Motivations for information-sharing;
2) Their imagined audience;
3) Strategies used for facilitating information propagation;
4) Choice of tweet content; and
5) Motivations for following others.

The survey also assessed the role of message reception on the users' attitudes and consequent information spreading. Participants also consented to provide their Twitter handle as part of the survey, making it possible to collect data from the Twitter API in order to construct ego-centered networks of users and their followers, discussion networks and networks of information flows. For each class of network, we developed analysis questions that focus on the spread and reach of Twitter users as information spreaders and the network positional attributes of users.

3.3.2 Data Collection Design

Any sort of Twitter network analysis must begin with a scheme for network construction, the choice of which depends very much on the analysis questions. Data collection entails the tracking of tweets, according to a pre-designed policy tailored to the chosen network type. This data set was intended to form the basis for constructing broadcasting and discussion networks. In addition, the Twitter API provides data on users' followers and friends.

Unfortunately, the first attempt at network data collection resulted in networks that did not align well enough with the survey data to enable the planned network analyses. The data limitations resulted in largely disconnected flows, severely skewing the network measure calculations. For the same reason, it was not possible to capture significant discussion threads and examine the roles of the survey participants in these networks.

Another impediment was the unforeseen limitation in the retweet meta-data provided by the Twitter API. All retweets are tagged with the original tweet id and the Twitter handle of its originator; however, the API does not provide information on the other users in the flow path. As a result, it is impossible to recreate the retweet trajectory. All that one can determine is the set of users who re-tweeted the original post and the time of each retweet, but not the direct intermediary of that tweet's trajectory through the network.

A second survey was designed on the basis of these findings. The data collection plan was designed specifically to capture the study participants' discussion networks and data on their network followers and friends.

3.3.3 Data Collection and Network Construction

Our requirements for tailored data collection led to the development of the Real-Time Analytics Platform for Interactive Data-Mining (RAPID) through a long-standing collaboration between DST and University of Melbourne. RAPID is a real-time SM data collection and processing system that is being continuously refined as research requirements develop. It is currently restricted to Twitter data, aiming to extend this to other SM platforms in time.

RAPID's data collection strategies are aimed at enabling tracking of certain topics and/or usernames and at constructing networks, with continual refinements of the tracking and filtering features based on new knowledge about online behaviors [32], [33]. The interface allows the user to directly interact with and modify the collection policy in real-time. Some of the most useful features include:

- Topic discovery (query expansion for discovering new keywords);
- Discussion tracking through recursive tracing of replies;
- Community/network extraction; and
- Real-time data interaction (community graphs, image wall, word cloud, tweet time-line, user profiles).

Additionally, it also allows the retrospective selection of data subsets and subsequent analysis in slower time.

3.3.4 Combining Network and Survey Analysis

The analysis of our study participants' Twitter behavior combined the qualitative analysis of the survey with an investigation of networks constructed from digital data recording the tweeting activities of the participants; drawing out certain network characteristics and comparing them with qualitative results from their survey responses.

An in-depth analysis of 82 discussion networks was conducted. Networks were constructed by collecting the screen names and tweet ids that were associated with each originating tweet that involved a participant. Components were extracted from the collection of tweet ids and links, containing at least ten tweets and involving at least one study participant. The focus of this investigation was on discussion style of participants that were involved in at least three discussions.

Preliminary results reveal that these networks evolve into three different types of structure, which can be broadly described as string, branch and star shapes, examples of which are shown in Figure 3-2. The diagrams depict examples of discussions that developed from a participant tweet and associated replies. Blue nodes denote tweets by the participant in question; red nodes are replies by other discussion members. Starting from left to right, the first four diagrams depict discussions that evolve in a string-like network – they are typically a sequence of tweet/reply and involve only two users: the participant and their respondent. The next two diagrams show discussions that branch out from the original tweet put out by a participant. Once again blue nodes represent tweets by the study participant; red ones are replies to the participant. The last diagram shows the discussion style of one particular study participant whose tweets generate responses from a vast number of followers. A blue node (in the center of the diagram, hidden behind the red nodes) representing the original tweet by the participant attracts a large number of responses, followed by replies to these responses by the participant (shown as blue nodes), that in turn attract more responses (red nodes) by other discussion members.

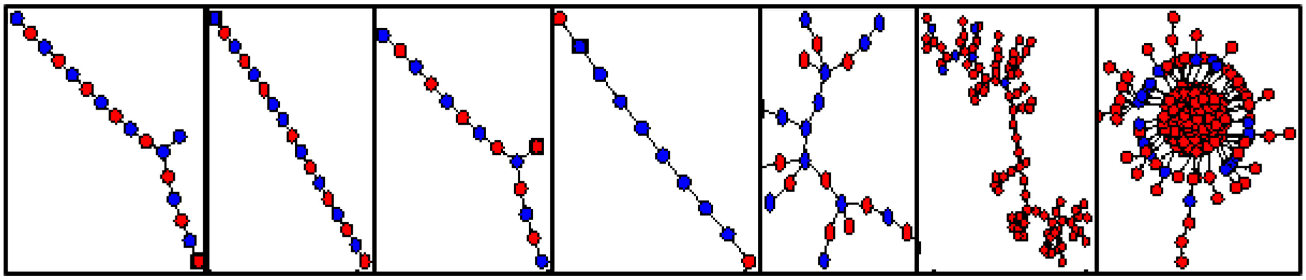


Figure 3-2: Different Types of Discussion Networks. Blue nodes are participant tweets.

This fine-grained analysis of discussion dynamics provides a way of describing the discussion styles of certain discussion thread initiators from the way the thread unfolds over time. An important preliminary conclusion is that certain network structures are an indicator of user popularity and their potential for exerting online influence.

3.4 CONCLUSION

Participation in the Research and Technology Group has proven to be of enormous benefit to DST Group's research program by nature of the exposure to real-world activities that transpired over the life of various NATO exercises. In particular, the unfolding of adversarial information campaigns in response to NATO military movements in Exercise Trident Juncture 15 and the wide use of botnets in these campaigns [27] has been very illuminating. The experience and knowledge gained contributed to further research on discussion dynamics and the roles taken on by Twitter discussion participants. The results coming out of this work have, in turn, contributed to NATO researchers' understanding of discussion networks and will help to develop and test successful messaging strategies for NATO.

Further, the improved understanding of the contested information environment has resulted in significant progress in the functionality of RAPID, the social media analysis experimental software being developed by the

University of Melbourne in collaboration with DST Group. RAPID has been demonstrated to NATO researchers and communicators and will likely be utilized in future NATO research activities.

3.5 THE WAY FORWARD

The engaged community of researchers in this Research Community, working closely with NATO Public Diplomacy Division and Joint Forces Brunssum, were able to rapidly transfer scientific understanding of critical problems in communication. This enabled NATO to make decisions rapidly and decisively about how it would meet these challenges. NATO stood up a Digital Working Group in November, 2016. In 2017, NATO Allied Transformation Command, with support of the Collaboration Support Office, established a Limited Objective Experiment at Joint Forces Command Naples to better explore the requirements of NATO forces and possibilities and affordances of scientific cooperation to speed transformation. This was the final cooperative activity of this Research Technology Group, creating a special technical demonstration at JFC Naples. Western scientists and military communicators spent four days discussing, teaching one another, and deepening connections.

October 2, 2017, a second Research Technology Group was authorized by NATO to continue these efforts: NATO Research Technology Group 293: Information Environment Assessment for Communications and Cyber-diplomacy. This effort will look at the next step beyond understanding adversaries, toward the goal of developing a strong scientific foundation to enable civil discourse and pursue a course of positive, ethical and effective community engagement, improve messaging, and the development of strong narrative.

Chapter 4 – REFERENCES

[1] Cooper, R. An Interview with Adm. Thad Allen (USCG-Retired). Defense Media Network, November 16, 2010. Accessed 10 June 2018. https://www.defensemedianetwork.com/stories/an-interview-with-adm-thad-allen-uscg-ret/.

[2] Lader, D. (2006) Understanding Social Theory, (Second Edition) London: Sage.

[3] Solis, B. Social Media is About Sociology, Not Technology. Blogpost. August 28, 2007. Accessed 29 July 2019. at https://www.briansolis.com/2007/08/social-media-is-about-sociology-not/.

[4] McLuhan, M. (1964). Understanding Media: The Extensions of Man. (New York: Mentor), reissued 1994, Cambridge, Massachusetts: MIT Press.

[5] Moore, Gordon E. (1965-04-19). Cramming More Components Onto Integrated Circuits. Electronics. Retrieved 2016-07-01.

[6] The Economist. Special Report: The Data Deluge. The Economist Magazine. 25 February 2010. Accessed 29 July 2019: https://www.economist.com/leaders/2010/02/25/the-data-deluge.

[7] Morozov, E. (2012). The Net Delusion: The Dark Side of Internet Freedom. New York: Public Affairs Press.

[8] Castells, M. (2012). Networks of Outrage and Hope: Social Movements in the Age of the Internet. Cambridge, UK: Polity Press.

[9] Hall, S. (1973). Encoding and Decoding in the Television Discourse. Europe Colloquy on the Training of Critical Thinking in Television Language. University of Leicester.

[10] Wikipedia. Second EDSA Revolution. Accessed: 2 January 2018. https://en.wikipedia.org/wiki/Second_EDSA_Revolution.

[11] Geertz, C. (1973). Thick Description: Toward an Interpretive Theory of Culture. In, The Interpretation of Cultures. NY: Basic Books.

[12] Allhoff, F., Henschke, A., and Strawser, B.J. (Eds.). (2016). Binary Bullets: The Ethics of Cyberwarfare. Oxford University Press.

[13] Floridi, L., and Taddeo, M. (Eds.) (2014). The ethics of information warfare (Vol. 14). Springer Science & Business Media.

[14] Lucas Jr, G.R. (2013). Can There Be an Ethical Cyberwar? Conflict and Cooperation in Cyberspace, pp. 195-210.

[15] Dipert, R.R. (2010). The Ethics of Cyberwarfare. Journal of Military Ethics, 9(4), pp. 384-410.

[16] Sternstein, A. (2015). Russia’s Troll Army is Making Life Harder for US Spies. Defence One, August 17. Accessed: 28 July 2016. http://www.defenseone.com/technoloqy/2015/08/russias-troll-armv-makinq-life-harderus-spies/119179/.

[17] Parfitt, T. (2015). My Life as a Pro-Putin Propagandist in Russia's Secret Troll Factory. Daily Telegraph, June 24. Accessed: 28 July 2016. http://www.telegraph.co.uk/news/worldnews/europe/russia/11656043/My-life-as-a-pro-Putin-propaqandist-in-Russias-secret-troll-factorv.html.

[18] Mattox, J.M. (2002). The Moral Limits of Military Deception. Journal of Military Ethics, 1(1), pp. 4-15.

[19] Lawrence, A. (2015). Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign. Stop Fake, April 03. Accessed: 28 July 2016. https://www.stopfake.org/en/social-network-analysis-reveals-full-scale-of-kremlin-s-twitter-bot-campaign/.

[20] Kowalski, R.M., Limber, S.P., Limber, S., and Agatston, P.W. (2012). Cyberbullying: Bullying in the Digital Age. John Wiley & Sons.

[21] Oh, O., Manish, A., and Rhagav R. (2011). Information Control and Terrorism: Tracking the Mumbai Terrorist Attack Through Twitter. Information Systems Frontiers. 11 March 2011. Vol 13:1, pp. 33-43.

[22] Agarwal, N., and Kirin, K.B. (2017). Blogs, Fake News and Information Activities. In, Digital Hydra: Security Implications of False Information On-Line. Riga, NATO Strategic Communications CENTRE of Excellence. Accessed: 2 Jan 2018. https://www.stratcomcoe.org/digital-hydra-security-implications-false-information-online.

[23] Van Dijck, J. The Culture of Connectivity. A Critical History of Social Media. New York, Oxford University Press, 2013. ISBN 978-0-19-997077-3.

[24] Darczewska, J. (2014). The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study. Point of View, Number 42. Warsaw. May 2014. http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.

[25] Chernov, S. (2013). Internet Troll Operation Uncovered in St. Petersburg. 18 Sep 2013, St. Petersburg Times, Issue #1778 (37). Accessed: 10 September 2014. http://www.sptimes.ru/index.php?action_id=100&story_id=38052.

[26] Nimmo, B. 4Ds of Russian Disinformation. Anatomy of an Info-War: How Russia’s Propaganda Machine Works, and How to Counter It. March 19, 2015. StopFake.Org website blogpost. https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it.

[27] Agarwal, N., Al-khateeb, S., Galeano, R., and Goolsby, R. (2017). Examining the Use of Botnets and their Evolution in Propaganda Dissemination. Defence Strategic Communications, 2 (Spring 2017), pp. 87-112. http://www.stratcomcoe.org/academic-journal-defence-strategic-communications-vol2.

[28] Robins, G. (2015). Doing Social Network Research. London: Sage Publications.

[29] Resnyansky L., Falzon L., and Agostino K. (2012). From Transaction to Meaning: Internet-Mediated Communication as an Object of Modelling. In: 8th International Conference on Social Science Methodology, Sydney Australia, 9 – 13 July, 2012. Conference Proc. Vol II. Accessed: 10 February 2017. http://conference.acspri.org.au/index.php/rc33/2012/paper/view/371/32.

[30] McCurrie, C., and Falzon, L. (2017). Twitter Users as Information Spreaders: A Comprehensive Literature Review. DST Technical Report, DST-Group-TR-3401.

[31] Falzon, L., McCurrie, C. and Dunn, J. (2017) Representation and Analysis of Twitter Activity: A Dynamic Network Perspective. In: Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM '17) ACM 1183-1190 DOI: 10.1145/3110025.3122118.

[32] Lim, K.L., Jayasekara, S., Karunasekera, S., Harwood, A., and Falzon, L. (2018). RAPID: Real-time Analytics Platform for Interactive Data Mining. WWW '18, April 2018, Lyon, France.

[33] Vanni, M., Kase, S., Karunasekara, S., Falzon, L., and Harwood, A. (2017). RAPID: Real-Time Analytics Platform for Interactive Data Mining in a Decision-Support Scenario. Proceedings Volume 10207, SPIE Next-Generation Analyst V, Anaheim, California, USA, May 2017, doi: 10.1117/12.2263748.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-HFM-248 AC/323(HFM-248)TP/868	ISBN 978-92-837-2192-5	PUBLIC RELEASE

5. Originator Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Information Technology for Crisis and Disaster Response

7. Presented at/Sponsored by

Final Report of NATO HFM-248.

8. Author(s)/Editor(s)	9. Date
Rebecca Goolsby, US; Katie Woodward, UK; Pille Pruulmann-Vengerfeldt, EST; Justin Hempson-Jones, GBR; and Lucia Falzon, AU.	November 2019

10. Author's/Editor's Address	11. Pages
Multiple	46

12. Distribution Statement There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Adversarial information campaigns
Bots
Crisis
Digital working group
Disaster
Disinformation
Euromaiden
Hacking information
Manoeuvres
Narrative
NATO
Propaganda
Social influence
Social media
Trident juncture

14. Abstract

The world of crisis, conflict and disaster has become deeply intertwined with information technology. When this research technology group was formed, 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 civil crisis, violence and disaster response. Understanding how to assess the information environment for these events became a critical capability.

Military and government entities have been disadvantaged in developing effective approaches to managing information technologies. The conflicts in Ukraine and the annexation of Crimea precipitated rapid changes in NATO's approach. Adversarial information operations evolved rapidly during this period. Understanding how to blend these capabilities into the workflows, constraints, and urgent needs of NATO operators was a less-than-clear proposition.

This effort explored new methods and approaches for using novel information technologies to assess the information environment surrounding social crises, conflicts and disasters. Further, it sought to facilitate the rapid transition of scientific and technical knowledge to NATO public affairs and related organizations through technical demonstrations and discussions with NATO operators.

This report will discuss the development and study of the new information environment as a conflicted space. It will examine the new conflict and its information technology components, its derived strategy together with NATO's response. It will document the key successes of this effort, including participation in Trident Juncture 15, contributions to the development of new technologies to benefit NATO and to the creation of the NATO Digital Working Group.

NORTH ATLANTIC TREATY ORGANIZATION

NATO
OTAN

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS
STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen. M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

NATO
OTAN

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2192-5