ROYAL DANISH DEFENCE COLLEGE

#TheWeaponizationOfSocialMedia

@Characteristics_of_ Contemporary_Conflicts

DANISH DEFENCE

Thomas Elkjer Nissen

#TheWeaponizationOfSocialMedia

@Characteristics_of_
Contemporary_Conflicts

By Thomas Elkjer Nissen
Royal Danish Defence College

2015

Thomas Elkjer Nissen (ed.)

#TheWeaponizationOfSocialMedia
- @Characteristics_of_ Contemporary_Conflicts

Copenhagen March 2015
Royal Danish Defence College
Ryvangs Allé 1
DK-2100 Copenhagen
Denmark
Tel.: 3915 1515
Fax: 3929 6172
Editor in chief: Dean Ole Kværnø
Printed in Denmark by Rosendahls A/S
Front page photo: leopard2a HOK
Layout: Bent-Ole Kure
ISBN: 978-87-7147-098-7

CONTENTS

LIST OF FIGURES 4

DEDICATION 5

ACKNOWLEDGEMENTS 5

LIST OF ABBREVIATIONS 6

1. INTRODUCTION 8

2. THE STRATEGIC FRAMEWORK 15

3. SOCIAL MEDIA, CROSS-MEDIA AND NARRATIVES 35

4. EFFECTS-BASED THINKING ON SOCIAL MEDIA 58

5. THE WEAPONIZATION OF SOCIAL MEDIA 74

6. PERSPECTIVES 104

7. CONCLUSION 122

BIBLIOGRAPHY 125

END NOTES 137

LIST OF FIGURES

Figure 2.1. The information environment 24
Figure 3.1. Characteristics of social network media. 38
Figure 3.2. Typology of social network media 38
Figure 3.3. Approaches to cross-media content coordination 43
Figure 3.4. Levels of narratives 47
Figure 4.1. Activities and Effects framework. 61
Figure 4.2. Targeting effects 62
Figure 4.3. Types of analysis 64
Figure 4.4. Intelligence effects 65
Figure 4.5. Operational effects 67
Figure 4.6. Psychological warfare effects 70
Figure 4.7. Defence effects 70
Figure 4.8. Command and Control effects 72

DEDICATION

To my wife, Maria, for her tireless support throughout this effort.

ACKNOWLEDGEMENTS

The author would like to thank the staff of Royal Danish Defence College, several anonymous interviewees and contributors and especially Dr Steve Tatham and not least Dr William Mitchell (Royal Danish Defence College), for opinions, comments and input to earlier versions of this monograph.

LIST OF ABBREVIATIONS

ACO	Allied Command Operation
AOI	Area of Interest
BDA	Bomb Damage Assessment
C2	Command and Control
C3A	Communication, Collaboration, Coordination and Action
CI	Counter Intelligence
DARPA	Defence Advanced Research Projects Agency
CENTCOM	Central Command
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CMC	Cross-Media Communication
CNO	Computer Network Operations
CoG	Centre of Gravity
DC	Decisive Conditions
EBT	Effects Based Thinking
ENDF	Electronic National Defence Force
HFA	Human Factor Analysis
IA	Information Assurance
ICP	Intelligence Collection Plan
ICT	Information and Communication Technology
IDF	Israeli Defence Forces
IE	Information Environment
IHL	International Humanitarian Law
IO	Information Operations (also abbreviated: Info Ops) International Organisation
ISR	Intelligence, Surveillance and Recognisance
Lawfare	Legal Warfare
LIC	Low Intensity Conflicts
LOAC	Laws of Armed Conflict
MILDEC	Military Deception
MNF	Multinational Force (Iraq)
NATO	North Atlantic Treaty Organisation
OAF	Operation Allied Force
OPSEC	Operational Security
OSINT	Open Source Intelligence
OUP	Operation Unified Protector
PA	Public Affairs

PSYOPS	Psychological Operations
PsyWar	Psychological Warfare
RAT	Remote Administration Tool
RFI	Request for Information
ROE	Rules of Engagement
SA	Situational Awareness
SEA	Syrian Electronic Army
SIGINT	Signals Intelligence
SMS	Short Message Service
SOCMINT	Social Media Intelligence
TA	Target Audience
TAA	Target Audience Analysis
TCN	Troop Contributing Nation
UGC	User Generated Content
UK	United Kingdom
US	United States
UW	Unconventional Warfare
VOIP	Voice over Internet Protocol (IP)
VPN	Virtual Private Networks

CHAPTER 1

INTRODUCTION

Social Network Media has become an integral part of the conflict environment over the past 15 years and longer. Starting with what has been labelled the first "internet-war", that is, the Kosovo conflict in 1999, developments have steadily progressed ever since. Counter-insurgency campaigns in Afghanistan and Iraq, several conflicts between Israel and its Arab neighbours, particularly with Hamas in the Gaza strip and Hezbollah in Lebanon, and events in connection with the Arab awakening (or spring), especially the during NATOs operations in Libya, the on-going civil war in Syria, and most recently during the crisis in Ukraine, the world has seen social network media being used more and more strategically by multiple state and non-state actors to create effects in both the virtual and physical domains.

Western liberal democracies, however, still look at war in a classical manner and therefore fail to grasp the new realities of contemporary war and the nature of its goals. War is no longer about states against states (in the conventional sense), but about identity and identity claims, and about cosmopolitanism (inclusion) versus particularism (exclusion / nationalism). Contemporary wars are therefore more about control of the population and the political decision-making process than about control over territory. Contemporary wars are therefore not to be understood as an empirical category but rather as a logical framework in which to make sense of contemporary conflicts and their characteristics. Furthermore, as most conflicts and wars for western liberal democracies today are what is called "wars of choice", requiring a high degree of legitimacy, and multiple non-state actors are struggling to mobilize support and find new ways of fighting asymmetrically, social network media seems to have become the weapon of choice.[1] This is the case both because it is easy for nearly every

(1) Weapon by definition according to William H. Boothby: "A weapon is an offensive capability that is applied, or that is intended or designed to be applied, to a military object or enemy combatant. A destructive, damaging or injurious effect of the weapon need not result from physical impact as the offensive capability need not be kinetic". (Boothby, 2014, page 176).

actor to access and use, due to the democratisation of technology that the Information and Communication Technology revolution is facilitating, and because you can create effects that are disproportionate in relation to the investment. Effects that support the goals and objectives of the multiple actors "fighting" in the social network media sphere, including influencing perceptions of what is going on, can, in turn, inform decision-making and behaviours of relevant actors. Due to the global connectivity that social network media provides, the actors are no longer just direct participants to conflict. They can be whoever, civilians and activists included desires to create effects. This is also why terms as "remote warfare" and "social warfare" play an increasing role in contemporary conflicts, where social network media is now used for military activities. These activities are, but not limited to, Intelligence Collection, Targeting, Psychological Warfare, Offensive and Defensive Cyber-Operations and Command and Control activities.

The increasing strategic uses of social network media, and the effects achievable in and through the use of them, empower a multitude of actors and have a re-distributive effect on international power relations. This also affects the character of contemporary conflicts.

This development is clearly demonstrated in several contemporary conflicts such as in Libya, Syria, counter-insurgency operations in Iraq and Afghanistan and, lately, the conflict in Ukraine. They indicate that social network media and the cyber domain have framed past strategies and actions, and are likely to do so in future conflicts as well. There is also a visible trend of social network media being used for creating strategic effect in contemporary conflicts, which therefore to a higher and higher degree is to be seen as an "instrument of power", not least by non-state actors[2] but by states as well. It is therefore as a result necessary to appreciate the potential game-changing properties of social network media in today's global information environment in all policy, strategy formulation and operational planning.

There is, however, a much broader aspect to consider as well. Social network media technologies are pervasive and have an impact on every aspect of our lives. Issues such as security, privacy, terrorism and activism, and even

(2) Actor: person or organisation, including state and non-state entities, within the international system with the capability or desire to influence others in pursuit of its interests and objectives. (Source: NATO MC Position on the use of effects in operations (MCM-0041-2010), 20 July 2010, NATO UNCLASSIFIED, page 1-3)

everyday social interaction are now all influenced by social network media. At the same time new concerns about privacy arise due to new forms of activism and terrorism, e.g. cyber-activism and cyber-terrorism, emerge, and the responses to the becomes more pervasive. This also creates new concepts for using social network media. This tendency is also seen in contemporary conflicts where web-pages, internet based web-television, social network sites (e.g., Facebook and Twitter), blogs and upload services (e.g., LiveLeak and YouTube) are being used as sophisticated weapon systems. This is the case not only in the "contest of narratives" and perceptions but also when it comes to actual weapon systems or platforms designed to collect intelligence, single out targets, facilitate command and control, and other actors' access to it, not least when disseminating propaganda and conducting deception.

The emergence of new war-fighting concepts, and the evolution of existing ones, has necessitated a discussion of the terminology and policies of social network media and how this technology is brought to bear in conflicts. From cyber-activism to cyber-terrorism, different perceptions of this issue are easily observed. There seems to be a growing acceptance that, along with the social network media technologies, the lines between terrorism, cyber-terrorism, activism, so-called "hybrid warfare" and full-scale conflict have become blurred. The actors and their activities can co-exist in the same conflict domain, and alter agendas and affiliation very quickly, from day to day, as the conflict unfolds. While an act is regarded as terrorism by some, the same act may be considered as activism in the eyes of opposing groups, while in a third instance, it is viewed as operational support for a state actor. This is also the case in respect to social network media.

From an ethical to a political standpoint, the debate on social network media's political and technical impact on the future of terrorism, conflict and security goes on in various academic studies and other fields, but the aspects of how social network media are used as weapons in contemporary conflicts have until now not been well described – In other words, the "Weaponization of Social Media" has not yet reached the level of academic study that is necessary in order to supplement the existing body of research within contemporary war-studies, or the study of "New Wars". This monograph is therefore a contribution to this debate.

However, when dealing with this debate many questions arise. For example, should the use of social network media in wars and conflicts be viewed as a sub-set to the "cyber warfare" debate or as something new and substantively

different? It has been argued that most cyber activities do not reach the threshold of what can be classified as "cyber warfare"; and what is "cyber-warfare" anyway?[1] And, of course, how do we define social network media in a military or conflict context? Furthermore, since the theoretical framing of social network media in a cyber-warfare discourse only reflects its actual use in conflicts, and not the intended effect(s), a second theoretical frame is needed. The latter concerns the requirement for defining which theoretical approach best supports the intents and effects of the introduction of social network media to the battle-space.

Taking into account the argument about the purpose being to influence perceptions and behaviours, one intuitively thinks of social constructivism, but also this theoretical frame needs to be operationalized in order to have enough explanatory power to shed new light on the topic. There is therefore a need for creating a framework for the actual use and the intentions, as well as for the desired effects both on- and offline (on perceptions and behaviour as well as on systems and capabilities) in order to understand the role of social network media in contemporary conflicts – or in other words an "effects-based thinking" approach.

In addition, the question of the consequences of this development on other aspects of contemporary conflicts arises. Is this just a new weapon system or platform, which has materialized through the developments within Information and Communication Technology (ICT) and its concomitant practises, or has the introduction of a strategic and effects-based employment of social network media in contemporary conflicts, by multiple actors, actually altered or affected the character of these conflicts? Also, what effect does this have on political, legal and ethical aspects of contemporary conflicts? Finally the question of how military forces should address this field becomes prominent. What are the consequences and subsequent requirements for new policy and doctrine, and the materiel and organisation of military forces? That is in no way a trivial question, as today's military capabilities continue to be focused on conventional manoeuvre warfare, even as trends point towards the importance of multiple (or hybrid) threats as being predominant. Hybrid threats that are likely being multiplied or enhanced by multiple actors' use of social network media!

A project at the University of Sussex called "Defence, Uncertainty and Now Media" (DUN) points to some of the same challenges discussed above. The project states that "more recently, social media has been considered

particularly effective in this regard by virtue of its immediacy, mobility, and networked capabilities. Yet, simultaneously, the effect of this form of 'Now Media' (and media engagement) is unpredictable, uncontrollable and often immediate. Social media is especially volatile because it cannot be understood in the same way as mainstream media. This generates real uncertainty and risk (…). This can be articulated in a number of ways".[2]

- Firstly, the unpredictability and speed of information emerging through and in social media can (continuously) reconfigure political and public perceptions of defence activities in a manner that is detrimental to strategic objectives.
- Secondly, despite efforts to understand 'audiences' and 'users', particularly those related to defence operations, recipients and authors of social media remain unpredictable (and essentially unknowable).
- Thirdly, social media is considered to pose significant risk to the security of defence operations, particularly in terms of operational security and the lives of military personnel.

Although speaking about the impact of social network media on the British Armed Forces the concerns and risks can be transferred to the broader debate on how social network media affects the character of contemporary conflicts.

It is on this strategic backdrop that this monograph poses, and seeks to answer, the overall question of how social network media has been weaponised and how this development has affected the character of contemporary conflict. In doing so, the monograph will address questions such as what characterises contemporary conflicts, and how can social network media be understood within this theoretical framework? What is the role of social network media in a contemporary conflict framework, and how do they fit into the concept of "cyber-warfare". Which effects are sought and how are they created? And how does the introduction of social network media affect the character of contemporary conflicts? Furthermore, a meta-theoretical framework for understanding the effects in the form of social-constructivism will also be discussed throughout the monograph, directly and indirectly.

The scope of this monograph is therefore to look at the use of social network media in contemporary conflicts as a weapon system or capability

with the purpose of creating political, strategic, operational or tactical effects in support of policy objectives, hence the title: *The Weaponization of Social Media*. Most interesting is how it is possible to create "military" effects, e.g., *inform, influence, deceive, deter, disrupt and destroy* targets, or target audiences, in support of such policy objectives in and through social network media, which normally are created through the application of more traditional military capabilities in accordance with conventional war-fighting doctrines. One of the major differences, though, is that nearly all actors can do this in today's global information environment, due to the opportunities that the development within information and communication technology affords them.

THE MONOGRAPH'S STRUCTURE

The monograph is divided into seven chapters. The introduction, three chapters containing descriptive analysis, the main analytical chapter, perspectives and the conclusion. Each chapter finish with an interim conclusion containing a short summation of the key findings in the chapter and their relevance to the overall purpose of the monograph.

Chapter one – Introduction - contains the background for the monograph and discusses the main challenges associated with social network media in contemporary conflicts, as well as proposes a framework for analysing these challenges.

Chapter two – The strategic framework - provides the overall framework for understanding and analysing the role of social network media in contemporary conflicts. It will do so by discussing what characterises contemporary conflicts – or what has been labelled "new Wars" - and how the character of war, or conflicts, has changed along with the development within information and communication technology (ICT). This chapter will include what is understood by the term "the information environment" (IE), which is the domain wherein most of the activities associated with social network media exist. To frame the discussion, the chapter will also use the concept of "cyber-warfare" as a part of the framework for understanding social network media's role in contemporary conflicts, and in doing so, discuss the concept and narrow down its scope in order to operationalize it for the purpose of this monograph.

Chapter three – Social media, cross-media and narratives - will use and the operationalize theory from the first chapter – the effects framework – as

the basis for discussing the theory (characteristics, definition and typology) behind social network media, the concept of cross-media communication (CMC) and the concept of cross-media narratives in order to demonstrate how they are applied in conflicts for military (war-fighting) purposes through a case study.

Chapter four – Effects based thinking on social media – will provide an analysis of how social network media are strategically employed and for which desired effect(s). This will include an analysis of how social network media are used to achieve effects traditionally conducted through "mainstream" military activities, such as intelligence collection, targeting, computer network operations, psychological and unconventional warfare in this new domain – under the overall heading, or as a sub-set, of cyber-warfare, as discussed in chapter two. The chapter will, furthermore, as an introduction to this domain, discuss what is meant with "effects-based thinking".

Chapter five – The weaponization of social media - provides a discussion and analysis of how social network media affects the characteristics of contemporary wars and conflicts - informed by the initial chapters with descriptive analysis'.

Chapter six – Perspectives –provides a discussion of political, ethical and legal aspects of the weaponization of social media in order to include how this development can be seen in the framework of the "legal warfare" or Lawfare concept.

Chapter seven – Conclusion - summarises the main findings from the three chapters with descriptive analysis that directly inform the main analysis of social network media's impact on contemporary conflicts. The analytical' findings of the latter, along with the perspectives, will then be used to conclude the monograph.

CHAPTER 2

THE STRATEGIC FRAMEWORK

CONVENTIONAL WARS

Before we can discuss what characterises contemporary wars and conflicts, it is necessary to understand of the classical concept of war. This concept sees wars as being conducted between nation states (or inter-state war), which largely marked the cold war scenarios used for training military forces,[3] even though cold war actions mostly consisted of intra-state wars and so called proxy-wars. War, in its classical sense, is thus understood as a polarized contest, normally between two sides. In other words, a polarity exists, in which defeat and victory are mutually exclusive; these are defined in inverse relation to one another.[4] Even if war involves several actors, these are typically separated and aligned as two sets of allies. War is a traditional basic function that serves as a national "instrument of power" – to provide a military outcome that sets conditions for a political solution. Even if the military outcome is not absolute, the overall success or failure of a side in war is relative to an enemy.[5] In war, as it is classically conceived, military action is furthermore understood, and planned, in terms of its physical or destructive effect on the enemy, which again is understood as the opposing military force(s) and the strategic resources of the state that sustains this force.

One of the primary proponents of this classical conception of war is the German general Carl von Clausewitz (1780 – 1831), who wrote the seminal work "On War" in which he famously stated that "war is a continuation of political intercourse, carried out with other means".[6] War is a human phenomenon with its own logic and rationale. The purpose of military activities is to seek a political result, but via a specific military outcome (end-state) that is brought about by imposing one's "will" on the enemy, which in turn sets the conditions for the political result.[7] War, therefore, is also described as a clash of wills.

CONTEMPORARY WARS AND THEIR CHARACTERISTICS

Since the end of the cold war in the early 1990s, a debate has unfolded over to which extent contemporary, or new, wars differ from classical wars in

the Clausewitzian sense. With academics and scholars like Van Creveld, Münkler and Kaldor as some of the notable exponents of the New Wars debate, the overall argument that has been formulated is that the character of war has changed. Centred on Clausewitz and his core work "On War", the debate is about how the "nature of war" and "the character of war" has changed so much that a new logic applies, and that we are in a post-Clausewitzian era, where the Clausewitzian paradigm no longer applies.[8] Others like Smith and, latest, Simpson also argue that the character of war has changed and that Clausewitz perhaps should not be completely discarded, but at the very least updated, since the "nature of war", in its essence, remains the same.

The "new wars" debate is interesting and useful in order to understand that the role of social network media in contemporary conflicts is closely tied to the general description of the character of conflict that Kaldor, Creveld and Münkler puts forward, which also Smith and Simpson echo, Clausewitzian debate or not, there are numerous overlaps between the actor, method, economy etc. and the description and characteristics of social network media.

Mary Kaldor, for one, argues that "new wars", unlike "old wars", are characterised by the use of organised violence for different purposes, ranging from organised crime to large-scale violations of human rights, opposed to the traditional, exclusive (political) focus on inter-state wars.[9] According to Kaldor, the actors, the goals, the methods by which warfare is waged and the war economy in new wars are different from old wars.

New wars are to a lesser extent fought by states' armed forces than in old wars. Now, war is fought by networks of state and non-state actors, and include both state regular forces, paramilitary, private and contracted forces. Also the goals are different. Unlike old wars that were primarily fought over geo-political interests or ideology, new wars are fought over, among other reasons, "economic interests" and "identity"; and as Kaldor points out "identity politics are constructed through war".[10] The aim now is to mobilise political identity. The methods have changed as well, according to Kaldor. It is no longer a question of conventional forces seeking to obtain a decisive victory over another conventional force; it is now a question of obtaining control over populations. Finally, the economics of war have changed from being purely state-financed wars to also being financed by private / criminal interests.[11] An economic rationality that is also supported by Herfried Münkler in his book "The New Wars".[12]

According to Kaldor, western liberal democracies look at war in a classical way and therefore fail to understand the new realities of war and what the goals are. It is no longer about states against states, but about identity and identity claims and about cosmopolitanism (inclusion) versus particularism (exclusion / nationalism). The wars are therefore more about control of the population and political decision-making than about control over territory. But Kaldor also points out, that new wars are not to be understood as an empirical category but rather as a logical framework in which to make sense of contemporary conflicts and their characteristics.

Martin Van Creveld, just as Mary Kaldor, also argues that the way that primarily liberal democracies today view contemporary wars is fundamentally flawed! The view is based on strategic thinking that draws on Clausewitz. This, he argues, is an obsolete way of viewing conflicts and wars in a time where contemporary conflicts are characterised by war between ethnic and religious groups and where the notion of large-scale conventional warfare is at best an illusion. In his view, this form of strategic thinking has a consequence on states' capacities to project (violent) power, which is why a change in strategic thinking is necessary, in order to align strategy to the characteristics of contemporary conflicts.[13] States therefore, need to rethink the aims and objectives for employing armed force. What is the end-state, who are the actors (or audiences one could say), and how do they project power in order to prepare for future conflicts.

One of Van Creveld's basic notions, when arguing that conventional war is obsolete, is that the presence of nuclear weapons prevents large-scale conventional wars.[14] This "new" weapon system is what makes wars new! Furthermore, he argues that they are "status-quo" weapons that stabilise the balance of power between states that have them, as it is irrational to use them. On the other side, however, with the absence of large-scale conventional wars, what he calls "Low Intensity Conflicts" (LIC) is the norm in contemporary conflicts. LIC will still be bloody and can lead to political change. Large states, however, have a hard time wining them.[15]

Creveld's view on contemporary conflicts is that they will most probably be fought over ethnic, religious and economic issues and personal interest of leaders, rather than over geography. Future conflicts, though, will still be violent, and wars will occur even though they will be in the form of LIC. These conflicts will be fought by primarily non-state actors (populations). In this equation, charismatic leaders will be very influential in instigating

and mobilizing for war. Contemporary conflicts are therefore to be seen from a top-down (collective motives) as well as a bottom-up (individual) perspective.[3] This does not mean, however, that state actors cannot be found supporting or even directing non-state actors.

Also the counter-insurgency theorist David Kilcullen, in his book "out of the mountains", highlights three areas where contemporary conflicts have changed character. They are more urban, technology is changing war and the democratisation of technology is empowering.[16] All three characteristics create conditions which facilitate more power to social network media in the future, as war is likely to be more about local power, money and control [over populations].

Contemporary conflict's conceptual boundaries are therefore hard to define. Pinpointing when something evolves from a crisis into a conflict or war, as the gradual shift happening in Syria (2011 to present) has shown, or what in reality is a "war" like the "war on terror" is increasingly hard to define. (The "long war" on terror as a continuous conflict subverts the traditional concept of war).[17] The distinction between war and peace is therefore difficult.[18] Likewise, it is hard to delineate between war and peace in the on-going conflict in Ukraine, and it is difficult to both bring about a decisive result on the ground and to say when the conflict or war is over. Conflicts may not be over with the conclusion of hostilities, as the conflict might be transformed into a perceptual or legal "struggle" for the right to write the narrative about who was right / wrong or won / lost; or through "Lawfare"[4] continue the war in the international legal system using international humanitarian law (IHL).[19] The general tendency is a movement away from situations in which the armed forces set military conditions for a political solution: in many contemporary conflicts, while the activity of armed forces often remains crucial to achieving a political result, military activity is not always clearly

(3) A critique of both Kaldor and Creveld is that identity/tribal/feudal and religious wars far outnumber inter-state wars historically. Inter-state wars have taken place from 1400 – 1500 and forward, and they are still outnumbered by intra-state wars. So the new war versus old war definition of Kaldor is somewhat weak.

(4) Lawfare, or legal warfare, is a term which the former US major general Charles Dunlap is accredited for having coined. Lawfare is "the strategy of using – or misusing – law as a substitute for traditional military means to achieve a warfighting objective". (Source: Charles J. Dunlap, Jr., Lawfare Today…and Tomorrow. In International Law and the Changing Character of War 315-325 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds.), US Naval War College International Law Studies, Vol. 87, 2011. Page 315)

distinguishable from political activity.[20] This applies before, during and after conflicts and becomes even more relevant as conflicts are both fought in the physical and the cognitive domain, including in the cyber domain, all at once, and sometimes only in the two latter. Here the outcome is not an effect on an enemy but on a strategic audience other than the enemy. Policy, strategy and the conduct of "military" activities must therefore be adjusted to influence these (non-military) audience(s), and military action must be considered in terms of their likely political interpretation by various audiences. To assist this interpretation, the use of use of psychological warfare, including cyber elements, deception operations and, of course, the strategic use of social network media plays an increasing role.

The control of the political space is therefore as important, if not more important, than controlling the physical space in contemporary conflicts.[21] As both Creveld, Kaldor and Münkler, as well as Emile Simpson, point out in different ways, contemporary conflicts are a competition between many actors in an extremely fragmented and complex political environment. The challenge, though, is that these conflicts are pulled into a traditional concept of war, where in contemporary conflicts political considerations now drive operations even at the lowest levels of military command and the use of armed force is for direct political outcomes, outside the traditional concept of war for which these military forces are trained, organised and equipped.

Adding to this, contemporary conflicts are taking place under conditions heavily influenced by pervasive media technology, political choices and international law. A part of contemporary conflicts are also that for most western liberal democracies they are "wars of choice", perhaps "necessity", but not "wars for survival". This means that political actors (states or international organisations), for a whole host of reasons, choose to involve themselves in a conflict or its solution, even though they are not forced to for national survival.[5] Though in the case of the Islamic State" (IS) in Iraq and Syria, some would argue that it is necessary to go to war with them for normative reasons. For those actors, and their constituents, these conflicts often will be geographically far removed from the state or organisation, normally with little direct impact on the state's population as a whole. This results in conflicts that are perceived as very distant, and the populations of

(5) Must remember though that what for western liberal democracies can be described as "wars of choice", can very well be a "war of survival" for the state that is affected by it. For example Iraq in 2003 or Libya in 2011.

the troop contributing nation (TCN) are only exposed to the conflicts via the media coverage and through social network media. This is why non-state actors also look at social network media as one of their "weapons" of choice when it comes to influencing the perceptions and behaviours of these constituents.

This very feature of contemporary conflicts and the disconnect between domestic politics and the conflict area are also addressed by the retired British Lieutenant-General Sir Rupert Smith in his book on modern warfare: "The Utility of Force", in which he discusses the concept of "war amongst the people". One of his main points is that the military term "theatre of operations" should be considered not just as a description of geography but as a theatrical "theatre" with audience participation. An audience consisting of the media, the local population, the enemy, the military force itself, TCN populations and other "strategic audiences" all have a say in the conflict, but not all of them can be affected directly by the military force.[22] David Kilcullen in his book "Out of the Mountains" goes a step further and argues that the fact that strategic audiences can have an impact in the theatre of operations, and can be affected from within it, constitutes "remote warfare" and that we should be talking about "virtual theatres" without a discrete area of geographical space as well.[23] This is also something that directly affects traditional strategy formulation, in regard to "theatre strategies" and subsequent military operational planning in which one among other elements looks at the Joint Operational Area (JOA) in geographical terms.

Smith's characterisation has also led him to describe modern wars and conflicts as a "spectator sport", referring to the "entertainment value" of war given to it through the way in which traditional media report on it. This, along with the technological development (drones, amour, network based operations etc.), means fewer casualties and suffering (on the TCN's side), but it also means a decreased threshold for what the publics will accept in general, in terms of blood and treasure spilled, due to a lack of identification with the purpose of the conflict participation. Wars of choice therefore require a substantially larger effort to gain and maintain public understanding and support for the policy for western liberal democracies. They must constantly legitimise their decision to employ military force. Legitimacy, therefore, is a key characteristic of contemporary conflicts and the question of a population's and the media's perception of what is legitimate therefore also becomes very important. This discussion on the domestic support versus media relations (in broad terms) also applies to the relation

between an international organisation and its member states and the local population in a theatre of operations, or in a conflict area, where the success might dependent on convincing the local population of whom to support. In this context, the perception of the situation can be more decisive than its realities when it comes to how the situation informs key strategic audiences' ultimate behaviour. This is also referred to as "Perceptions become Reality", drawing on W. I. Thomas's quote from 1923, "If men define things as real, they are real in their consequences".[24] If the media, population and or decision-makers believe it to be so – they will act accordingly.

Based on this premise, it is also self-evident that much of the thinking behind these dynamics is theoretically based in "social constructivism". In its classical form, social constructivism is about how ideas and beliefs inform actors' behaviour and why shared understanding between actors is important.[25] Alexander Wendt describes that "the distribution of power may always affect states' calculations, but how it does so depends on the inter-subjective understanding and expectations, i.e., on the "distribution of knowledge" that constitutes their conception of self and other".[26] This may not only apply to states, as Wendt describes it, but also to organisations and non-state actors, and perhaps even private individuals that act in the international environment in connection with crisis or conflicts. Social constructivism is also about how ideas define and can transform the organisation or structures in world politics, shape identities and interests of actors (state and non-state) and what is to be considered legitimate in international politics and thereby inform foreign policy choices.[27] In regard to legitimacy Barry Buzan also points out that states (and perhaps also non-state actors) possess legitimacy that is formed on the basis of perceptions of the actor and its acts in the international system.[28] Legitimacy, in turn, is also a non-material factor constituting power in the international system.[6] According to Wendt, the collective meaning or perception constitutes the normative and ideational structures that organise behaviour.[29] Or, in other words, this means that identity informs interests and, in turn, behaviour.

The theory gives us clear indications (policy prescriptions) with respect to what we need to influence knowledge, understanding and collective

(6) One of the issues that social constructivism criticizes neo-realism for is the claim that power is based on the distribution of material power and that neo-realism overlooks the value of power generated through social relations in the international system. (Jackson and Sørensen, 2007, page 162).

meaning (perception) of social networks in order to inform and prompt behaviour. To do so, there is a need to construct an interpretive structure (or strategic narrative) in which audiences can create meaning of what transpires. As Emile Simpson states, "War is a competition to impose meaning on people, as much emotional as rational (…) there may be a crowd watching, in which case to be seen to "win", if one cares for their opinion, one's rules need broadly to align with theirs, however, one must not confuse a mutual acknowledgement of a battle's meaning with the idea that war in this case provides a single interpretive structure".[30] One side can deliberately move away from an interpretive structure that is symmetrical[7] to the enemy's in order to achieve an advantage. This emphasises how the application and adjustment of the interpretive structure of war is of vital importance. When used in reality, creating interpretive frameworks or allocating different meanings to the same actions, through narratives and communication (in social network media), is as much an instrument of war as the use of force.[31] As the majority of contemporary conflicts do not reach definite end-states and their outcomes are defined in more subjective political – socially constructed – terms, the strategist (be that a political, military or non-state actor) has to combine the physical and the perceived,[32] to which end social network media play an significant role in contemporary conflicts. To stress this point, one can also look at Manuel Castells's theories on "communication power" and the role of networks. Castells's basic thesis is that the most fundamental form of power lies in the ability to shape the human mind, since he defines power as "the relational capacity that enables a social actor to influence asymmetrically the decisions of other social actor(s) in ways that favor the empowered actor's will, interest and values".[33] This definition of power is therefore very applicable to social network media and the use of them in contemporary conflicts. Castells furthermore argues that communication networks are pivotal to power-making in any type of network (e.g., political, corporate or social) and that "programming" (creating and gatekeeping networks) and "switching" between individual networks are fundamental sources of power.

(7) Asymmetric warfare has two connotations: the physical asymmetry and the interpretive asymmetry. The Physical asymmetry is so to say common sense. It is about gaining an advantage over one's opponent by fighting differently. The second type of asymmetry is about gaining an advantage through providing a different – asymmetric – interpretive frame that strategic audiences can use to make sense of the actions conducted, or to construct and provide a more compelling strategic narrative about what the conflict is about; i.e., who is right and wrong and what success looks like in order to influence perceptions, decision-making, mobilize support and prompt behaviour.

When trying to describe the character of contemporary warfare and what influences it, one therefore finds that concepts as legitimacy and credibility and issues as networks, media and domestic, international, regional and local public opinion, perception, attitude and behaviour are central.[34] The domain in which this struggle takes place in contemporary conflicts is collectively referred to as the "Information Environment", to which also social network media belong.

CHARACTERISTICS AND DYNAMICS OF THE INFORMATION ENVIRONMENT

The information Environment is analytically both a sub-set of the conflict area and a much larger phenomenon – with global reach. Looking at it from a sub-set to the conflict area perspective it is about who says what to whom through which media and with what effect internally in the conflict area. Especially the media and effect part is interesting; secondly, the content and the context in which it the communication takes place is interesting. The information environment as a much larger and even global phenomenon is about how information flows and can have effects globally due to the interconnectedness brought about by globalization and the developments within Information and Communication Technology (ICT), and as a sub-set to this development social network media.

The US Department of Defense, in its doctrine on Information Operations (IO), defines the Information Environment as follows:

> "The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as physical, informational, and cognitive. The physical dimension is composed of command and control systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information".[35]

This definition is, admittedly, both very military and very technical. It does, however, provide a usable framework for understanding the information "battle-space" and how both technology (including social network media), processes (technological and human) and content (images, words and the perception of observable action) fit together and creates effects.

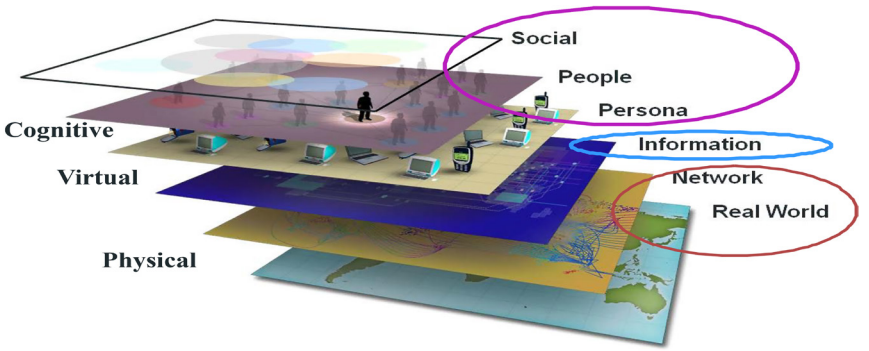

Figure 2.1. The information environment[36]

The battle-space today can be described as a contest that, besides the military one, also includes the political, social and economic contests even at the local (tactical) level, where actors seek to persuade audiences in such a way that the delivery of the political message is an end in itself. The importance of this factor has significantly expanded in the first decade of this century, not least due to the possibilities provided by the internet and the proliferation of mobile phones and other mobile devices, but also any number of other information media. The information revolution therefore accelerates and expands the information dimension of contemporary conflicts right down to the tactical level, and connects all levels from strategic to tactical in new end ever-changing ways. To include the creation of interlinked networks. This effectively reverses the role of information in contemporary conflicts, where information previously tended to be about the subsequent explanation of actions, it is now about using information as an action in itself.[37]

The information environment in contemporary conflicts is thus heavily influenced by pervasive media technology, political choices and the digital mass participation of people having a real-life impact. These characteristics have been brought about by the last two decades of development within information and communication technological, which allows a very wide range of audiences and or actors to capture (record), edit, and upload

information and imagery in virtually real time, whether the traditional news media are there to witness situations or not. Furthermore, modern communications technologies compress the levels of war shortening the distance between the tactical battlefield and the strategic decision-makers in capital cities. For example, the ability to communicate instantly means that tactical events or actions can take on unexpected strategic meaning or have so-called second and third order effects or consequences. This is also known as "time – space compression".[38] Web blogs, social network media sites and file-sharing sites as YouTube are examples of social network media platforms that empower individuals to potentially achieve strategic political and military effects. The easy upload of videos, without editorial interference (news media no longer act as exclusive gateways or gatekeepers), allows access to potentially a nearly unlimited audience. During natural disasters, for instance, it is often possible to experience an explosion in the use of social network media with people calling for help, others offering it, and again others translating tweets for humanitarian agencies. At the same time, news is distributed in the networks through on-site reports from individuals (citizen journalism), which again are picked up by mainstream news outlets' and reported as news-stories. The latter being a major challenge for news agencies in terms of attribution. Along with this, a lot of "noise" appears in the social network media created by people re-broadcasting existing content, creating their own content (so-called User Generated Content – UGC) and people that deliberately upload false content for whatever reason. The ability to cut through this noise and validate social network media information is therefore challenging in contemporary conflicts, especially when social network media content often finds its way to mainstream news outlets as the primary source to a story.

This availability of off-the-shelf, relatively affordable and portable, media technology therefore makes it possible for anyone; combatants, rebels, own soldiers, local nationals, own citizens and many others to act as "citizen journalists"[8] or what has been called "netizens".[9] Digital cameras,

(8) "Citizen Journalism" can be defined as: "The collection, dissemination, and analysis of news and information by the general public, especially by means of the Internet". Source: http://www.oxforddictionaries.com/definition/english/citizen-journalism (Accessed 13 MAR 14)

(9) "Netizen" is a composite word of citizen and internet. It is defined as: "A citizen who uses the Internet as a way of participating in political society (for example, exchanging views, providing information, and voting". Source: http://whatis.techtarget.com/definition/netizen (Accessed 13 MAR 14).

predominately in mobile phones and other mobile devices, and internet connected computers and tablets have therefore become essential weapons of war, especially in Low Intensity Conflicts (LIC).[10] The interesting question, though, is how social network media can be effectively used to shape the information environment and create effects in support of an actor's objectives, and how to mitigate or counteract such use of social network media by one's opponents and relevant third party actors.

The result of the empowerment created by ICT in the contemporary information environment is a matrix of real-time information flows that highlight the inadequacy of the traditional military chain of command, the news media and the decision-making processes of governments and International Organisations (IOs). It is a considerable challenge to maintain global awareness of what is happening in social networks and to respond in an effective and timely manner without reference to events in the physical domain.

This was especially evident during the so-called 2012 "media war" between Israel and Hamas. Both sides contested each other, digitally, by publishing pictures of the other party's wrongdoing, tweeting messages on a regular basis, and by posting YouTube videos in an attempt to portray the conflict to their advantage. Characterising the heated debates and the mass participation of ordinary citizens in this contest, the UK newspaper The Guardian wrote: "a high-intensity virtual war on the hearts and minds of all netizens was being waged".[39] This characteristic can also be seen in another case study on the "Islamic State" or IS in Iraq, which we will look at later. These strategies are increasingly at the forefront of terrorist organisation's strategies. According to terrorism expert Professor Gabriel Weimann (Haifa University), "about 90% of organized terrorism on the Internet is being carried out through the social media. By using these tools, the organizations are able to be active in recruiting new friends without geographical limitations."[40] Repressive regimes, as well, have discovered

(10) "Low intensity conflict is a political-military confrontation between contending states or groups below conventional war and above the routine, peaceful competition among states. It frequently involves protracted struggles of competing principles and ideologies. Low intensity conflict ranges from subversion to the use of armed force. It is waged by a combination of means, employing political, economic, informational, and military instruments. Low intensity conflicts are often localized, generally in the Third World, but contain regional and global security implications". (US Army Field Manual – FM 100-20 Military Operations in Low Intensity Conflicts, chapter 1).

spying software and ways to exploit and prevent activists' use of social network media. In Egypt, for instance, internet access was shut down for several days by Mubarak's regime. Later on, internet activists were harassed by the Egyptian security forces.[41]

In a world where conflicts are being dramatically re-shaped by the information revolution, and there is no neat polarity, the outcome of contemporary conflicts will involve a struggle for the perceptions of multiple strategic audiences who are un-aligned to either side.[42] In this struggle in the information environment, social network media facilitated by mobile devices linked to or being a part of the internet become very important. Being a part of the internet also makes it a cyber (war) issue. Whether organized violence has been applied or threatened remains a central distinction between military and non-military activity, though this is increasingly complicated by activities such as cyber-threats or operations.[43] This is especially the case when these activities or operations to a larger and larger extent are being regarded as "military operations".

Efforts to shape worldwide political perceptions according to the actors' security interests are, nonetheless, a characteristic of contemporary conflict. The problem, though, is how to define when something is a conflict or war when it comes to taking the struggle to the cyber domain – in which social network media resides.

THE CYBER WAR DEBATE

Defining "cyber-warfare" is no trivial task and many definitions currently exist, often very broad in scope, making it difficult to determine what it in reality is and when a cyber-attack is actually happening. Also if it is part of a criminal activity, political activism or actual war-fighting, and if so, if it can be categorised as war. The use of the word "war" also muddies the waters. There is therefore a need for separating cyber-crime, online vandalism, civil policy orientated "hacktivism" from what actually constitutes the use of cyber for warfare purposes.[44] Even though much of the first mentioned activities can be elements of armed conflicts, they do not constitute the use of military force per say. To narrow the scope of what we are dealing with, it is important to define the concepts of "Cyber-Warfare" and "Cyber-Attack" before we start discussing the role of social network media in contemporary conflicts.

Many definitions of cyber-warfare exist in literature. One of them has been developed by Adam Liff, who defines cyber-warfare as: "the deliberate hostile and cost-inducing use of CNA [Computer Network Attack] against an adversary's critical civilian or military infrastructure with coercive intent or to extract political concessions, as a brute force measure against military or civilian networks in order to reduce the adversary's ability to defend itself or retaliate in kind or with conventional force, or against civilian and/or military targets in order to frame another actor for strategic purposes".[45]

This definition firmly puts cyber-warfare within a more conventional war-fighting paradigm and does not separate cyber-activities from conventional use of military power as something completely different. It does also mean that cyber-warfare is not only something that goes on in "cyber-space" in isolation, as that would not constitute "war", but as something that will be conducted in concert with "real-life" physical activities. It likely will be a question of combining "armed attacks" with "cyber-attacks" in order to simultaneously create effects in both domains. Cyber-attack will, in this understanding, therefore most likely be conducted in the framework of conventional kinetic attack or other "military" activities, used as an opening salvo to disable defences in immediate advance of a conventional attack, providing an offensive advantage.[46]

A pure "cyber-attack" on the other hand can be defined as: "activities that are carried out over information networks ranging from hacking and defacing of webpages to large-scale destruction of the military or civilian computer-based systems, networks or infrastructure".[47] The use of social network media for creating military effects, either alone or in concert with other (physical) military activities, can also be framed or explained within these two definitions.

Firstly, according to the definition of cyber-warfare, then social network media are used deliberately hostile manner and can be cost-inducing through the use of CNA-like activities or hacking. Although these activities mostly are targeted against an adversary's, sometimes private, civilian or military communication and information infrastructure, it is still with coercive intent or to extract political concessions through manipulation and excreting influence on decision-making processes. Social network media are not, on the other hand, particularly adept as a brute force measures against military or civilian networks in order to reduce the adversary's ability to defend himself (unless it is a question of so-called 'psychological

defence' e.g. the achievement and maintenance of information resilience against propaganda within own population or armed forces). But social network media can be used against civilian and/or military targets in order to frame another actor for strategic purposes. This was, for example, seen very clearly in connection with the downing of MH17 over Ukraine, where social network media was used extensively to implicate multiple actors and to create confusion about what in reality happened.[48]

The cyber-warfare definition, however, only provides clarity for some elements of what effects can be created in and through social network media, as it only encompasses the effects resulting from direct action in either the cognitive or physical network domains, e.g. what Thomas Rid, besides espionage, labels subversion and sabotage.[49] It does not encompass other "warfare activities", or effects, as actual intelligence collection, support to targeting and the facilitating / supporting warfare activities associated with command and control. For further depth, we secondly have to look at the cyber-attack definition. Stating that it is activities that are carried out over information networks clearly implies that this also can be a question of social network alone. Further pointing out that it ranges from hacking, as discussed above, and defacing of webpages to large-scale destruction of the military or civilian computer- based systems, networks or infrastructure. The latter, though not being of particular relevance when talking about social network media in terms of 'destruction', is interesting in terms of affecting systems, networks and infrastructure. Particularly in respect to the distribution of malware in order to facilitate tracking and monitoring (intelligence collection) and mapping networks and content flow for targeting purposes (of both networks and individual user profiles). In respect to targeting, this can be a question of identifying "personas" (virtual actors) as well as "persons" (humans behind one or more personas). Affecting networks can also be a question of actual attack on the social network media profiles / accounts themselves or the network or servers on which they reside. The predominant and most talked about utilisation of social network media in warfare is, however, to extract political concessions through manipulation and exerting influence on decision-making processes (leading to actual behaviour) and to frame or deceive other actors in and through social network media. In other words, this denotes psychological warfare purposes. Surely, as social network media, first and foremost, are for communication and dialogue, they can also be used to communicate coordinate and synchronize actions and messages making them useful for 'command and control' as well.

A large challenge, though, is the question of attribution of cyber-attacks. There is no standard for how much evidence for the attribution of the attack is required for a particular type of response by the state attacked.[50] Normally, when talking about physical armed attacks, it is fairly straightforward to pinpoint the origins of the attack, but doing the same in relation to cyber-attacks, however, can much more difficult. The possible cooperation of non-state (proxy) actors in a state-sponsored cyber-attack further complicates attribution. Especially in Low Intensity Conflicts, cyber-warfare will probably take the form of proxy-warfare.[51] This has been evident when looking at the hacking activities in the conflicts between: Hamas – Israel, Russia – Georgia and now in Ukraine. It is therefore not only a question of tracing from where the attack originates (geographically or hardware-wise), it is also a question of establishing organisational links to a specific actor, in order to attribute the attack to an "agent of the state", a state itself.[52]

However, qualifying cyber-activities as military activities or operations, and nesting them within a framework of what the US DoD terms "Cyber Warfare", i.e., "the use of computers and the internet to conduct warfare in cyberspace", allows us to look at social network media and how they are used in contemporary conflicts in an analytical way. The US DoD definition of cyber-warfare, however, is rather broad, which means that it would be useful to narrow the definition down somewhat. Similarly, it does not make any reference to the use of mobile devices. It does, however, allow for the analysis of the use of social network media for warfare purposes.

As Liff and several others argue, and quite rightly so, a major cyber-attack that will bring about sudden massive disruption of critical infrastructure, or even bring down a government, will most likely not happen. What we are left with, then, is a cyber-domain that is highly politicised and used by state and non-state actors to exercise activism and military operations that include "cyber-attacks" to create political or military effects. These attacks and other activities, however, will be used in conjunction with many other forms of pressure; from physical activities (for example, special operations forces) over economic, social, cultural and diplomatic initiatives to targeted psychological influence on specific actors. But, as mentioned above, it is very hard to attribute the parts of the activities that go on in the cyber domain to a specific actor, although the actor obviously supports its desired effects. Even though it is possible to see whom certain actions might benefit, they can very well be carried out by groups or individuals who are sponsored by, claim affiliation with, or proclaim independently to support, for whatever

reason, a state or organisation. The effects achieved, however, supports this state or organisations interests or policies.[53] Leaving the state or organisation with "plausible deniability" in terms of the attribution and legal liability, if it so desires.[54]

Cyber-warfare can be a low cost, effective means of political coercion or brute force and act as an asymmetric weapon. Cyber-warfare capabilities in this context may also affect perceptions and bargaining dynamics, which is why, as Liff also points out, "waging strategic information warfare might prove useful for actors whose political objectives are limited in scope, who can control vulnerability to retaliation, and who possess a willingness to take risks".[55] Especially in a contemporary setting, information and communication technology and the rise of mass self-communication and self-organising systems or networks allow individuals, social movements and more organised actors to enter the public space and influence or shape it. This is important as most contemporary conflicts are as much about people and their decision-making as they are about territory. Furthermore, in highly networked societies, cyber-attacks could cause economic or political consequences and non-violent effects that could exceed the harm of an otherwise smaller physical attack.[56] In short, the ways in which digital connectivity is empowering a wide range of globally networked social movements with a significant strategic potential for using cyberspace for the mobilization of contention in support of diverse causes, and for challenging governments supported by hacktivism, is a new characteristic of contemporary conflicts.[57] Cyber-warfare activities therefore effectively help create perceptions, influence the understanding of what transpires and prompts state, organisational, media and individual behaviour in contemporary conflicts.

INTERIM CONCLUSION

As discussed earlier, the theoretical framework for understanding social network media's role in contemporary conflicts consists of three major elements: Firstly, understanding what characterises contemporary conflicts and where social network media resides in that context. Second, what characterises the global information environment: how did it develop in the past; and how will it develop in the future. Third, and finally, what role will social network media have in "cyber-warfare".

Contemporary conflicts are characterised by being different from traditional conflicts in several ways – even though some things admittedly remain the

same. Nonetheless, it can be argued that a new logic applies when it comes to contemporary conflicts. The reasons for conflicts (the ends), who fights [or is engaged in] them (the actors), with which methods (ways and means) they are fought or how power is projected, and how they are financed has changed. But also where conflicts are fought (urban areas) and the impact of technology's democratization are changing the characteristics of contemporary conflicts.

The use of organised violence still occurs, but for many different reasons, not only as inter-state war over strictly geo-political issues. The issues that drive conflict and war today are multiple (as they have been historically as well). They range from ethnic, religious, economic, identity and identity claims to more classical geographical issues, but they are more about the control over populations, decision-making and the political space than they are about a geographical area, even when looking at Ukraine.

Contemporary conflicts therefore also need to be viewed from both a top-down and a bottom-up perspective, as the actors involved in today's conflicts are both state and non-state actors all the way down to individuals, who empowered by modern pervasive information and communication technology, are able to influence how a conflict develops and are perceived, especially by political decision-makers. As contemporary conflicts are also characterised by being "wars of choice", perhaps "necessity", but not "wars for survival" (for liberal democracies, less so for some authoritarian regimes) and by that they are fought "amongst people" resulting in many spectators and audiences to the conflict, who all have a say in its outcome. This makes issues such as legitimacy, credibility, perceptions, and public opinion, prerequisites for acting in contemporary conflicts, since much of what informs different audiences behaviour is inter-subjective understanding and meaning created in social networks (physical or virtual) through arguments (logical and emotional) and communication. This very characteristic also makes the global information environment a vital battle-space in contemporary conflicts.[11] Pervasive media technology and the democratisation of this technology, to include social network media, accelerate and expand the information dimension of contemporary conflicts allowing digital mass-participation of many groups of actors having a real-time effect. But also people's willingness and ability to use social network

(11) Understood as an engagement domain such as Air, Sea, Land, Space and Cyber-space.

media to their advantage, and their rapid embrace of technology in a way we have never witnessed before – even in the most rural or poorest communities - is an important factor. The empowerment of the many, however, also makes it a struggle for the political perceptions and the mobilization of multiple audiences – even globally. It is a struggle that, to a very high degree, goes on in the cyber domain. Whether that constitutes cyber-warfare is debatable, but a part of contemporary conflicts is cyber-warfare that according to Thomas Rid takes the form of online espionage, subversion and sabotage. Most of this, though, will probably take place under the threshold of what constitutes war and will predominately occur on social network media, in the cyber domain, which, in turn, will be an asymmetric weapon platform. Most notably in the context of what in the wake of the Ukraine crisis is called "hybrid Warfare". This is so despite the fact that malware and hacking can "destroy", and their effects can physically manifest themselves on the economy and classical targets, as in the case of a bombed factory.

The means with which conflicts are fought have therefore changed. It is no longer a question of large-scale formations of conventional military forces facing each other, even though they are employed to put pressure on decision-makers. In the event they are employed against an asymmetric opponent, it becomes a question of using a combination of diplomatic, economic, legal, psychological and cyber activities to achieve the desired effects.

It is, however, not only a question of why, by whom and how conflicts are fought. It is also a question of how they evolve. More and more conflicts are predominately fought out in urban areas, where there is more developed information infrastructure and access to the internet.

These changed characteristics also make it hard to define what war is – unless you, like Thomas Rid, use a classical, and very rigid, Clausewitzian approach – when wars start (have transformed from a 'crisis' to a conflict or war) and when they end as they cover both physical, informational (media, cyber and cognitive), legal and economic elements that are hard to classify but are, nonetheless, parts of warfare.

The nature of warfare remains the same, however. War is messy and at its heart is about deterring, and ,ultimately, destroying one's opponent's will and ability to wage warfare – directly (militarily) or indirectly (politically, legally, economically or in terms of information). The character of war is, however,

ever changing. Mostly with the developments in technology, the urbanisation of conflicts and multiplication of distinct actors, but also in regard to norms and legal issues as well as the increasing power of information when it comes to shaping the outcome of conflicts. Furthermore, the use of social network media is an integral part of contemporary conflicts, which creates new realities and possibilities for creating effects on the strategic audiences and the media which again affect the way actors behave and fight in this new reality, affecting the distribution of power in contemporary conflicts.

From this overall strategic framework it can be generally deducted that social network media plays an increasing role as in contemporary conflicts, as these conflicts are increasingly urbanised and urban areas have better information infrastructure, due to the developments within ICT and its democratisation, allowing access to the internet and thereby social network media. This access to social network media empowers a whole variety of actors, who would not previously have had the opportunity to affect the conflict – both internally and externally to the conflict area. This again results in a re-distribution of power. Partially because the traditional news media has less and less access to conflict areas (for financial and security reasons), and therefore depend more on information from people already within the area (e.g., citizen journalists). This gives a whole series of actors the means and opportunities for influencing key strategic audiences' understanding of the conflict. And as these conflicts are about perception, legitimacy and credibility, those about "information warfare" more than about controlling territory initially, policy objectives are obtainable through diplomatic, political, legal, informational / psychological and cyber means – supported by armed action or activities – why social network media can play an important role in this kind of warfare.

One thing, however, is the strategic framework and understanding of which overall role social network media plays in contemporary conflicts and how they affect the characteristics of them; another is understanding how to forge social network media strategies.

CHAPTER 3

SOCIAL MEDIA, CROSS-MEDIA AND NARRATIVES

SOCIAL NETWORK MEDIA

Having entered an era of media convergence that makes the flow of content across multiple social network media channels and platforms almost inevitable, it is important to look at the characteristics, typology and definition of social network media in order to further understand their role in contemporary conflicts and how they are used. It is further important to look at the evolving cross-media communication (CMC) methods and how strategic narratives are projected in social network media, and how these to concepts can contribute to understanding the "military" use of social network media in contemporary conflicts. Firstly, however, it is necessary to look at the characteristics, typology and definition for social network media.

Characteristics

As social network media continue to evolve, their uses change and expand, so do the characteristics, possible typologies and definition of social network media. In part, this is due to the fact that social network media relate to the technology and platforms that enable connectivity and the interactive web content creation, collaboration and exchange by participants, the public, and the media. As platforms and software change, so do their utility and the practise around them. Nonetheless, some fundamental characteristics can be derived and a definition can be developed.

Firstly, we will be looking at the general characteristics of social network media that can help define them in a conflict framework.

Social network media share some defining characteristics. They are all online technologies and practices that people use to share content, opinions, insights, experiences, perspectives, and media themselves. They are characterised by easy access, global reach, and the rapid (close to real-time) flow of multimedia information. This results in an aggregation of users with common interests that is able to conduct one-to-one and one-to-many two-way conversations. The social network media are virtually unlimited with respect to time and space, providing an effective platform for easily

aggregating common interests from a broad demographic spectrum. This includes new aggregate configurations which might not have connected, had it not been for the existence of social network media. This, in turn, also means that new and different types of (target) audiences appear. Social network media are, in other words, media for social interaction, and can therefore be utilised for of influence.

It is inexpensive to develop and maintain an online presence that enables the use of social network media, thereby reducing normal barriers for wide-spread technology. Social network media can be accessed from other inexpensive platforms, such as mobile telephones and other mobile devices, which also inherently spread and become available to large groups of people, including in areas with otherwise limited resources. To include developing countries and areas and conflict areas. Social network media furthermore allows for information and conversations to reach a broader audience without geographical limitations, making social network media one of the most permeating features of the global information environment, as discussed in the previous chapter. Other characteristics are the possibilities for automation, repetition of information and permutation of content, or the creation of user-generated content (UGC) based on as well "own" generated content and other users' updates, postings, tweets etc. in different combinations. It does also provide, however, possibilities for anonymity, impersonation, and for the distortion of content to a degree that it (intentionally) misrepresents the original intent of the content.[58]

As the uses of and practice around social network media change and expand, so does the cognition of the users. Online behaviour affects perceptions, and the way the users perceive the utility and purpose of social network media therefore change along with changes in the technology. Some studies, however, made on online vs. offline behaviour in crisis situations suggest that people basically will have the same behavioural pattern; they will be supporting, curious, exploiting or helping.[59] Other empirical indicators, e.g., from Syria and in the Arab awakening in general, show that practices adopted during a conflict situation might affect the way that people view and use social network media after the conflict. Examples of changing online behaviour in regard to own safety for fear of surveillance and monitoring of their online activity include the use of specific protection software or changes toward a more restrictive threshold for what is deemed acceptable content to upload.

The affordability and the ever-increasing magnitude of effect and reach, which is asymmetric to traditional media, also create new and constantly changing dynamics. The latter characteristic also means that approaches and methodologies for using social network media for operational purposes constantly must be assessed and evaluated to fit the current conditions. According to the media researcher Coombs, the biggest difference between social network media and traditional media (as news media) is that a two-way-communication is now possible and they (social network media) have enabled near real-time communication.[60] In addition to this, is the social network media's ability to empower ordinary people to become so-called "citizen journalists". This is the case because the production of news no longer exclusively belong to newspapers or other news networks. Rather, news providers can be whoever watches ongoing events on the ground, hears about them, or even re-produces second-hand accounts of them and publishes them directly on social network media, delivers them to news media, or the news media might pick up on them of their own accord and turn them into news stories. Social network media's characteristics have also been summed up by Collings and Rohozinski in six points.[61]

	Characteristic	**Description**
1	Pervasive	With over 1.5 billion internet users and with more that 60% of the world's population having access to mobile phones, and increasing, social network media usage is pervasive.
2	Ubiquitous	Smart phones, internet-enabled handheld devices (like Ipads) and GPS devices all increase in numbers which, in turn, increase the number of network-enabled devices on which social network media can be accessed. This also facilitates migration of content from digital camera (in smart phones) to upload sites like YouTube, Twitter and Blogs where the content is picked up and played back by satellite television (including pod-casting), resulting in further distribution in social network media.
3	Instantaneous	Social network media is close to "real-time". Messaging (incl. SMS / MMS) can spread around the globe almost instantly and is thereby faster and can reach a larger audience that traditional media. They can therefore be used for mobilizing for and organising / coordinating events real-time.

4	Interactive	Social network media facilitates interactive communication through not only messages, but also through "comment" functions, enabling conversations and feed-back, which in turn can promote (sense-making) common learning and correction of content. It can, however, also consolidate radical views or re-enforce false information.
5	Socially specific	They leverage social connections based on shared interests and existing networks.
6	"Sticky"	As social network media is pervasive, fast, interactive and leverage existing (and trusted) networks messaging, conversations and other content can be more "sticky" than that of what is distributed in traditional media, which is often view to be biased. Through participation in information aggregation, crowd-sourcing information, or just following events, content can stick with the audiences.

Figure 3.1. Characteristics of social network media.

Typology

Besides describing the general characteristics and functionalities of social network media they can also be divided into different types. There exist several types of typology of social network media, though. One of those, proposed by Kaplan and Heanlein, argue that social network media can be divided into six different categories.[62]

	Type	**Example**
1	Collaborative projects	Wikipedia
2	Blogs and micro-blogs	Blogs and micro-blog sites like Twitter
3	Content communities (Upload-sites)	YouTube, Flikr, LiveLeak, Instagram
4	Social networking sites	Facebook, Vkontakte or LinkedIn
5	Virtual game worlds	World of Warcraft, Call of Duty or Grand Theft Auto
6	Virtual social worlds	Second Life

Figure 3.2. Typology of social network media

It is not the specific examples of the types that are relevant. With more than 600 different social network sites in existence and the emergence and disappearance of several of them continuously, it is a question of identifying

which of the types that either alone or in combination (cross-media) with others can reach the intended audience (in existing networks), best carry the content and thereby best achieve the desired effect. Which type and specific platform that is relevant is both dependent on the geographical region in which the conflict takes place, and within that context also the purpose and the specific audience. The latter pointing to the importance of target audience analysis (TAA), even though this is challenging, to say the least, when it comes to social network media.

Definition

Capturing all these characteristics, along with typology, in one definition is not a trivial task and for that reason there have also been many attempts at defining exactly what social network media are. Most of these definitions have, like the majority of the literature, been focused on the private social or more commercial use of social network media. But, to an extent, they have also focused on how social network media changes news coverage including coverage of wars and conflicts. But definitions have yet to focus on the "military" use of social network media for operational purposes.

The characteristics and typology as discussed above can, along with a series of existing definitions, be used for deriving a definition of social network media that can be used for understanding their use in contemporary conflicts in an operational – or weaponized - way.

Firstly, looking at how the EU has defined social media in one of its internal guidelines, where they are defined as "online technologies and practices to share content, opinions and information prompting discussion and build relationships. Social media services and tools involve a combination of technology, telecommunications and social interaction. They can use a variety of formats, including text, pictures, audio and video".[63] This definition emphasises the technologically facilitated sharing of content and the building of social relationships to foster discussion.

For another definition, one can look at Kaplan and Haenlein, who define social media as "a group of internet-based applications that build on the ideological and technological functions of web 2.0., and that allow the creation and exchange of user-generated content".[64] Also, this definition emphasises that technological base of social network media and the sharing, but adds that it is the users that create the content. Furthermore, this definition indicates that there also is a distinct ideology behind the

user behaviour when it comes to social network media which is different from other media.

In like manner, NATO, in its guidelines on social media use within Allied Command Operation's (ACO) organisation, defines social network media; "social media are designed for dissemination through social interaction using internet- and web-based technologies to transform broadcast media monologues (one-to-many) into social media dialogues (many-to-many)".[65] This definition, besides the technological aspects, unlike the first two points to the convergence of content from "information dissemination" (monologues) to "communication" (dialogue). The definition, however, not unlike the second, also emphasises the social aspect.

And finally, a fourth definition suggested by Collings and Rohozinski states that "new media are those consumer-level digital devices and the forms of instantaneous, interactive communication they make possible because of their integration with global communication networks".[66] Also this definition, as much of the three previous definitions, puts emphasis on the technological base of social network media, and furthermore adds "networks" to the body of definitions.

Throughout the four definitions' key features, such as technology, network, content creation and sharing, interaction and communication, none of them, however, points to how this translates into tangible actions or behaviours that can advance policy or operational objectives and effects. The latter being at the heart of the discussion when it comes to the weaponization of social network media. Based on the discussion of social network media's characteristics and typology along with the key features of other existing definitions, a definition for the use of social network media in a conflict framework can be derived:

"Social network media refers to internet connected platforms and software used to collect, store, aggregate, share, process, discuss or deliver user-generated and general media content, that can influence knowledge and perceptions and thereby directly or indirectly prompt behaviour as a result of social interaction within networks".

CROSS-MEDIA COMMUNICATION

As alluded to in some of the characteristics, the typology and the definition activities in social network media does not go on in only one of the platforms

or sites at any given time. The content migrates, is changed or modified (becomes user generated content), and there are hyper-links and references connecting platforms and content to each other, both as a result of deliberate communication strategies and as a result of user-generated content and use, linking and sharing. This functionality is also referred to as "Cross-Media Communication".

The term describes the communication of an overall story, production, or event, using a coordinated inter-linked combination of platforms. Platforms in this context are to be understood as both physical devices mobile phones and other internet enabled devices and online sites and social network media platforms. The degree of coordination and cross-over between the platforms varies greatly. Cross-media can be conceptualized from an outward as well as an inward perspective: outward towards the users, and inward within the using organisations themselves[67]. Basically the same, or minor variations of, created content is placed or pushed onto different platforms in different formats. E.g., a minor re-edit of the audio from a video clip uploaded to YouTube is re-used for a podcast or a script adapted for a website or an SMS, and in its simplest form, the exact same content is delivered on multiple platforms such as mobile, web-TV and broadband web podcast and as content on a social site as Facebook or a micro-blog as Twitter in a coordinated form. It can also be content produced alongside a main production and delivered on different platforms from the main production. This 'extra' cross-media content is naturally different from the main property and not necessarily dependent on it - temporally or editorially – but supports the theme of the main production, or the overall strategic narrative.[68]

The truest form of cross-media is where the story (based on the strategic narrative) or service structure is specifically authored to prompt the audience's behaviour using a strong target audience analysis (TAA) based on a "call-to-action" across media devices and platforms. The content placed on the other platform is critical to staying in touch with the experience and the narrative bridges encourage the audience to investigate or move to another media form/platform where further content can be found. This content may then be from another and, by the audience, more trusted source, enhancing credibility and resonance through attribution. Obvious examples include an interesting Twitter feed with relevant information including a link to where further information and content can be found. This could be

a web-TV show (streaming), a podcast or subscription emails. The trigger, or bridge, is the critical component in motivating the cross-media action[69].

An aggregation of the methods can also involve that the content is distributed across many platforms in a nonlinear way and is producer, or sender, 'hands-off! (Letting the audience connect the dots themselves). This is to create an environment, much like an online game, that the participant/s 'lives' inside of the left and right of arc of the story (strategic narrative), following their own path and therefore personalizing the overall impression (perception) they get from "connecting the dots" based on fragmented but still mutually supporting pieces of information. A cross-media property is the co-creative and collaborative interaction with the audience across many devices, which evolves and grows a life of its own. The contextual environment created by the use of strategic narratives (which gives direction and guidance to the individual pieces of information) are a key part of leading the audiences across devices and platforms or around the narrative fragments. Although heavily coordinated, the cross-media triggers and invitations are set up for the audiences' themselves to create their own bridges, and thereby their own social-network- media-based story or narrative about what goes on in a conflict and what should action should be taken.

Ideally, in cross-media story-telling, each social media network platform is used for what it does best so that a story might be introduced in a video-clip on a "up-load" site, expanded through a blog or v-blog, SMS, and postings on social media sites, and potentially it might be exploited through game play. Alternatively, through the use of links to other related sites or single stories (e.g., news-stories or blogs) as a form of meta-text that conveys meaning or supports the sender's narrative, themes or messages. Each entry, or story fragment, needs to be self-contained enough to enable autonomous consumption and reaction (prompt behaviour).[70] Redundancy between entries or pieces of information increase audience interest. Offering new levels of insight and knowledge therefore prompts more interest and sustains audience loyalty. Such a multi-layered approach to cross-media narrative projection will enable a more complex, more sophisticated and more resonant narrative to emerge within the constraints of a conflict information environment.

As stated earlier, cross-media is a term describing the communication of an overall story, production, or event, using a coordinated combination of

platforms with internal references. This can, in summary, be done in social network media through four different approaches:

Approach	Method
Push	To ”push” the same content with minor differences on all platforms.
Extra	To provide “extra” content produced alongside a main production and delivered on different platforms.
Structure	To create and project a “structured” story in order to drive the audience to continue to other platforms.
Hands-off	By “hands off” distribution of content across many platforms in a nonlinear way give the audience a possibility to create the story themselves, by connecting the dots.

Figure 3.3. Approaches to cross-media content coordination

For something to be “cross-media”, as Dr Carol Miller (Pennsylvania State University) notes, it has to adhere to at least four principles: Firstly, the project must exist over more than a single medium. Secondly, it must be at least partially interactive. Thirdly, the different components must be used to expand the core material, and fourthly, the components must be closely integrated.[71]

Even though this description of cross-media communication is focused on the interlinked use of social network media and platforms, CMC is also about linking and connecting more traditional media (TV, radio, printed products and other media items) together with social network media in order to get the broadest possible exposure and impact on the target audience. Social network media might have a large role to play in the contemporary information environment, most people, however, still also turn to traditional media for information. One aim of cross-media communication planning of social network media is therefore also to ensure that news agencies get hold of content so they can lift into mainstream media coverage. Coverage that in turn will be mirrored and possibly go viral on social network media with an even much larger effect. The content must, however, be based on the strategic narrative.

NARRATIVES AND CROSS-MEDIA COMMUNICATION

When talking about strategic narratives, it is important to recognize that there are three different aspects of narratives that can conflict when seeing

them in the framework of social network media. Firstly, most theory on strategic narratives and narratives in the framework of contemporary conflicts is centred on state actors' politically "constructed" narratives, which tend to be top-down and very linear in their nature. Secondly, the information environment is saturated with "existing" narratives, including opposing actors and interests' narratives, which the politically driven narratives compete with; and thirdly, cross-media narratives, especially when projected in social network media, are prone to develop "a life of their own" and become uncontrollable, as they will become subject to UGC and will not have an ending. But firstly, it is worthwhile to look at strategic narratives as they appear in a traditional strategy or strategic communication context.

Strategic Narratives[72]

There currently exist many definitions of what constitutes a strategic narrative. Many of these, however, converge around the same key dimensions of the concept. Regardless of which definition one choses, strategic narratives can be used to either describe what can be labelled as an *"institutional narrative"* describing the *raison d état* of a state or organization, or it can be used to describe the "why and how" of a specific strategy, making it a *"theatre narrative"*.

For the purpose of this monograph, I have chosen to put forward a definition by Miskimmon et.al, where they define strategic narratives as "a means for political actors to construct a shared meaning of international politics and to shape the perceptions, beliefs, and behaviour of domestic and international actors".[73] Yet it is also important to point out that "a narrative is a system of stories that share common themes, forms, events, and participants, and create expectations for how those elements can be assembled to satisfy a desire that is rooted on conflict".[74] This approach to strategic narratives indicate that a they are not just single stories, but several stories that together make up – or support - the narrative, and that all actions taken as a part of a strategy are "storied", thereby becoming part of a larger overarching strategic narrative, and that these actions have communicative effect. Furthermore, it stresses that the interaction between these stories is complex and can lead to unintended consequences that potentially may end up undermining the strategic narrative if not coherently constructed in support of strategy.[75]

Strategic narratives both help inform and communicate actions. Informing the strategy and its associated actions ensures coherence with political

intentions – or in other words ensure coherence between words and deeds (even though the strategic narrative is normally constructed as an integral part of the strategy formulation process). Communication explains why the actor is actively involved in a conflict, which other entities the actor is up against, and how the actor seeks to resolve the conflict, or what the actor aspires to achieve. The basic concept of a strategic narrative is therefore that it offers a framework through which conflicts' past, present and future can be structured in order to help establish and maintain power in the international system and to shape the context and the system itself.

However, an actor cannot hope to have a monopoly on telling the story. There is competition between the strategic narratives of several actors in the international system; not only about words but also about actions that symbolize the strategic narrative, which the strategic narrative is about. As noted in a UK military doctrine on Strategic Communication:

> "In the global information environment it is very easy for competing narratives to also be heard. Some may be deliberately combative – our adversaries for example, or perhaps hostile media. Where our narrative meets the competing narratives is referred to as the battle of narratives, although the reality is that this is an enduring competition rather than a battle with winners and losers".[76]

Strategic narratives should therefore focus on alternative futures, based in the present situation and informed by the past, taking the audiences current views and expectations into account (existing narratives), rather than focusing on the differences between the competing narratives. On the one hand, the strategic narrative is ideally created as an integral part of the strategy formulation process. On the other hand, you find existing narratives that relevant stakeholders (local in theatre or internationally) use as a framework to make sense of the world around them - existing narratives that the strategic narrative should both tap into and seek to influence.

Strategic narratives are used by actors as a tool through which they can articulate their interests, values and aspirations for the international system and to change the environment in which they operate, manage expectations, and extend their influence.[77] Basically, narratives work as frameworks that allow people to make sense of the world, policies, events and interactions.[78]

Levels of Narratives

As mentioned above, strategic narratives exist on several levels (e.g., "institutional" and "theatre"). Looking firstly at the institutional level, it sets out the narrative for the actor from the executive level's perspective. It is relatively enduring and is very closely related to the actor's basic values and core beliefs. An institutional narrative is not necessarily explicitly defined and written down in, for example, a national strategy, a constitution or the core documents of an organization. It can be implicit or intuitively understood by the ones living it – the population of a certain state, or members of an organization, through the accumulated actions over a prolonged period of time. The institutional narrative is, in other words, formed by history based on the developing values of a given actor, and as such it will continuously inform policy choices and strategies of the actor articulated in theatre strategies and theatre narratives.

A theatre narrative, on the other hand, is closely connected to a specific theatre strategy. The theatre narrative both draws upon and supports the core values and visions expressed in the institutional narrative. It is therefore informed by and supports parts or all of the institutional narrative – and vice versa.

Both the institutional and the theatre narrative are made up of or supported by a series of interlinked stories each telling or showing a part of the narrative, in support of a given strategy. Even though the stories can develop or evolve over time to fit the current situation and reflect developments or satisfy the need for emphasizing certain elements of the narrative, the (core) narrative stays the same.

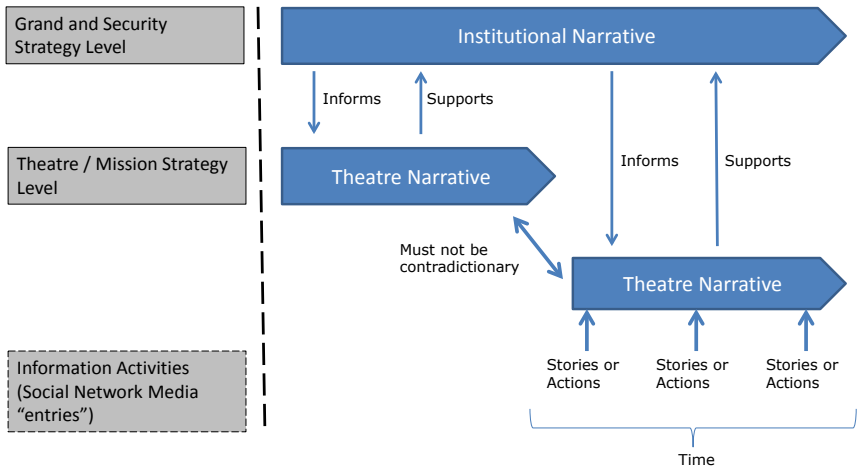

Figure 3.4. Levels of narratives

However, even though cross-media communication is based on a "strategic narrative", a series of distinct characteristics makes cross-media narratives different from the normal conception of narratives as described above. Firstly, more emphasis is on the "supporting stories", which also tend to be shorter (e.g., a 140-character Twitter feed or perhaps a six- second video message on Vine). Secondly, there are multiple actors in the information environment that through UGC can affect how the narrative is contextualized and hence perceived by different audiences; and thirdly it is challenging to define an ending to the narrative.

Cross-Media Narratives

As noted above in the section on cross-media communication, cross-media narratives and stories told through social network media are different in character compared to the more classical linear story-telling that has been symptomatic for "strategic communication" and main-stream media. This is also pointed out by Bryan Alexander and Alan Levine when they note that:

> "Today, with digital networks and social media, this pattern is changing. Stories are now open-ended, branching, hyperlinked, cross-media, participatory, and unpredictable. And they are told in new ways: Web 2.0 storytelling picks up these new types of stories and run with them, accelerating the pace of creation and participation while revealing new directions for narratives to flow".[79]

This is also clear when looking at what Jeff Gomez defines as a trans-media narrative: a "process of conveying messages, themes, or storylines to a mass audience through the artful and well-planned use of multimedia platforms".[80] Put differently, it is a question of a single narrative being supported by a story-element or components told through different media. Cross-media narratives are first of all characterised by being centred on social network media and the supporting stories being self-contained and smaller or in another word you can talk about the stories being "micro-content". Each of these self-contained "micro-content" stories are able to project a core piece of the overall narrative either directly or indirectly. Partly because they are developed or designed to be re-distributed across multiple platforms and partly because they are designed to the medium.

The fact that they are designed to be re-distributed across multiple social media platforms also result in audience participation and to some extent co-creation of the narrative through content associated conversations, as it spreads throughout networks or possibly goes viral. This also includes tagging and bookmarking the content so that other networks or audiences can find the content and be exposed to the narrative or parts of it. The narrative can also be distributed through hyper-texting, again creating new ways of exposing the audience to the narrative. This though also points to another characteristic of cross-media narratives; distributed story-telling. The narrative's supporting stories are told through multiple sites or platforms from different angles. This could include either official accounts (e.g., Facebook or Twitter) or blogs, micro-content uploaded to existing platforms in relevant networks or personal accounts.

This way of creating narratives in social network media also involves risks of course. Audiences can, due to co-creation and UGC alter the story and add content directly or through commenting or replying to the original story hence altering the experience for other participants in the conversation thereby depriving the author of the control over the narrative. This, in turn, also affects the narrative as a framework for sense-making as the narrative and its supporting stories become open-ended as the "story-world" loses its boundaries. It becomes hard to control just how far the story goes.[81]

But also at a more technical level you find challenges. Mostly a host of information design challenges as the individual story elements or components (text, images, video, audio and for that matter also other

media) all requires different product development styles and have different production cultures associated to them as Jenkins et al. also highlights:

> "Each medium has its own affordances, its own systems of representation, its own strategies for producing and organizing knowledge. Participants in the new media landscape learn to navigate these different and sometimes conflicting modes of representation and to make meaningful choices about the best ways to express their ideas in each context".[82]

This latter point is often a challenge for more "linearly thinking" government institutions, especially military organisations and their Public Affairs (PA) and Information Operations (Info Ops) departments. Lastly, also the question of how to maintain audience interest in a narrative scattered across multiple platforms and design is a challenge when projecting a narrative in social network media.

Nevertheless, despite the challenges involved with working with cross-media narratives in social network media using cross-media communication approaches, it is important for understanding how effects, at an operational level, are achieved in and through social network media in contemporary conflicts. Not least effects associated with psychological warfare and deception. The latter, much debated though, many observers have claimed that the Islamic State (IS) in Iraq and Syria have been very good at conducting as an integral part of their terror campaign throughout 2013 and 2014.

ISLAMIC STATE IN IRAQ A CASE-STUDY ON NARRATIVE BASED CROSS-MEDIA PRODUCTION[83]

Today social network media is the weapon of choice for terrorist groups. It facilitates recruiting, enables target-selection, and provides a conduit for propaganda, to include the dissemination of interlinked stories (words and images) that supports their narrative, recruitment and fundraising. This is to a very high degree also the case for the Islamic State (IS) in Syria and Iraq today. A significant part of IS's activities is their online propaganda activities that advance their narrative. Just how they are doing this from a cross-media and narrative perspective is an interesting case study into the weaponization of social media. From looking at their strategy, overall narrative, strategic (information) objectives, target audiences (TA) and associated social network media use we can see the contours of a very

calculated and professional social media information campaign which resembles modern cross-media marketing or political PR campaigns.

From a strategy point of view, IS has employed social media to gain the attention of mass-media and strategic audiences, inflate and control its messaging in support of its narrative in order to recruit and radicalize followers, deter their opponents and to raise funds. This strategy amongst other thing displays an understanding of the importance of having a single vision (the Caliphate) and a common purpose. It also shows an understanding of how to exploit user experience and visual mediums (infotainment) in order to gain attention and engage their followers and other strategic audiences in an emotional way. At the same time, they manage to construct their "self-expression" in a way supportive of their narrative, while displaying an understanding of how to disrupt an opponent's narrative and online activities by exploiting their messaging in order to position themselves and their 'brand' amongst other jihadist factions in the Middle East. [84]

The strategy also builds on the notion of "Force Multiplication" through the use of social media in order to make IS seem more powerful than it perhaps is in reality. Part of this is to create a large-volume online presence to assure visibility with strategic audiences, besides gaining mass-media attention and thereby further exposure of their message. This also serves another purpose that is to create the impression of a large mass of followers, in turn, creating social proof or fake peer-endorsement, potentially leading to even more "real" followers. This is, among other ways, achieved through the use of "disseminators", who are individuals, who although not officially affiliated to IS, spread their tweets and other postings to their followers, who for some number in the thousands.[85]

The strategy also relies on having these "disseminators" using hashtags crafted to look like grass-root initiatives exploiting "astro-turfing" techniques, in some cases also hijacking existing hashtags, and thereby lending third party credibility to the narrative. Not least "hashtag hijacking" where IS uses # of trending topics to get attention from audiences how would normally not search for IS content or #.[86] IS also utilises techniques normally associated with political campaigning, sending up "test-balloons" in order to track and gain feed-back on potential ideas, terms and graphics. This can also be viewed as a form of both target audience analysis and pre-test of products (both messages and images) in support of the campaign.

In terms of strategic narrative, the creation of a Caliphate that marks the return to the original version of Islam, including the introduction of Sharia law, is central to IS. "Muslims everywhere, they say, are besieged by everyone else. Muslims suffer these abuses because they have not been sufficiently rigid, literalistic and merciless. The restoration of a "caliphate" is a religious duty – as are the draconian laws and vicious terrorism that the Islamic State practices. It presents a diagnosis for real and imagined Muslim woes and a prescription: to embrace its assault on Syria, Iraq and, eventually, all other Muslim states. (…) The Islamic State offers the vision of a utopian Muslim universalism in an undifferentiated and gigantic caliphate across the Islamic world, without distinctions among individuals except their degree of zealotry".[87]

This is a centralised narrative, but a diversity of voices is used to spread the inter-linked stories and messages supporting it. There are, however, some apparent contradictions to the narrative when looking at some IS messaging. On the one hand you find images and accounts of mass-graves, beheadings and seized territory with the deterring messages: "oppose us and we will behead you or crucify you" embedded in them.[88] But on the other hand you also find "Hearts and Minds" like imagery and messaging on social activity, including delivering food to combat areas and other community work and ISIS's apparent love for cute kittens (on pictures of hand weapons). This can be viewed as a cheap tricks or clichés to brand themselves as anything but monsters, but also as a historical reference to Huraira (a companion of the prophet), who is known for having been fond of cats,[89] with the underlying message, still in support of the narrative, that IS fighters are humans but will pursue their opponents with a vengeance.

Form the narrative and associated messaging, it appears that IS's strategic objectives with the social media campaign are:

- Setting the international media agenda in order to gain attention and visibility of their message(s).
- To control the narrative
- To counter western, Shia Muslim (rival jihadist factions) and regime "propaganda" against IS.
- To position themselves in contrast to other jihadist factions and project themselves as more powerful then they perhaps in reality are.
- Connect supporters in online networks.
- Recruit new members and supporters.

- Intimidate and deter opponents (Iraqi / Syrian soldiers and civilians as well as rival jihadist factions).
- Demonstrate capacity and coherent command and control.
- Raise funds

IS seems to have at least six strategic audiences:

- Sympathisers and supporters (gain and maintain support).
- Potential recruits (especially disenfranchised youth in the west in order to mobilize support and recruit "foreign fighters" to come to Iraq and Syria).
- Potential donors.
- International media (gain attention).
- Local audiences in Iraq and Syria (to include Iraqi soldiers and civilians and other rival jihadist factions).
- Wider international community (to include the 'Umma').

The social network media use also indicates that they are relying on both a top-down approach as well as being comfortable with bottom-up initiatives (disseminators, or "fan boys", acting in IS interest). According to Rose Powell you can identify four levels of on-line activities. All four levels use the centralised strategic narrative as the framework or as direction and guidance for their use of images and messages in the different social media platforms supporting their propaganda activities. The content is therefore initially very coordinated, but as it makes its way either vertically downwards or is re-tweeted, re-posted or adapted to local circumstances and networks, the content changes result in some loss of control of the message, and hence the narrative.

The top-level consists of IS official Twitter and other social media platform accounts where most video is centrally uploaded. These video clips appear very professionally produced and in many cases resemble Hollywood stile productions. They include among other techniques slow-motion sequences and first-person-shooter like graphics. IS does, however, also use other and much simpler yet still violent videos'.

The second level consists of regional or provincial accounts posting both live reports from attacks (words and images) and localised messaging, in some cases including live-feeds and live-steaming.

The third level consists of individual fighters that post updates about their experiences on what is meant to appear as personal accounts. These are more personal, emotional and therefore appealing to, e.g., young potential recruits.

The fourth level is more or less outside the control of IS media "management" and consists of sympathisers and supporters (the disseminators) either re-tweeting or re-posting IS content or their user-generated content (UGC) based on the official IS messaging. Sometimes translated into their local language, including in the West.

The platforms used are most notably Twitter, including at times an (android and apple) app "The Dawn of Glad Tidings" (which has apparently been removed by now) to promote its messages and images and the use of hashtags and links,[90] Facebook profiles, Instagram and YouTube accounts and the Skype-like platform Viber. These platforms are interlinked at the top-level, and at lower levels links are used to connect to content. IS is also using links to selected outside articles and images from respected news-outlets that support their message or overall narrative in order to gain further credibility for their claims.

Some messaging and content production is also crowd-sourced / crowd-distributed (and translated). This indicates IS having access to highly skilled multi-media designers and state-of-the-art software (such as Adobe applications as InDesign, Photoshop etc.) The bottom-line is that IS, when it comes to the strategic utilisation of social media, seems to be in the lead at the moment, although they are increasingly challenged at their own game.

Although IS's narrative and messages are simple they resonate because they are coherent, idealistic and fill a void. But most important of all, it promises, and appears to be delivering, tangible and striking political and military successes so far. Yet they are increasingly challenged in the social network media sphere! With the Foley beheading video, cracks in their social media advantages began to appear. Their messaging and distribution of the video was opposed by many online, especially on Twitter initially, by private individuals, then by governments warning against re-tweeting and other sharing and later by Twitter as a company when it arbitrarily started a campaign against the re-distribution of the video (by removing tweets and suspending accounts) and actively tried to identify and close IS's Twitter accounts. Also YouTube and Google continually restrict IS operations by shutting down accounts and profiles that are in violation with their "terms

of use", when made aware about these violations by other users. This forced IS to move their activities to other social network media platforms as Diaspora.[91]&[12] It is, however, only temporarily as IS social media posts uploaded on other networks will find their way back into Twitter through, e.g., other "disseminators", and IS will also create new Twitter accounts. Both Iraqi and Syrian, as well as western, intelligence services also target IS social media (propaganda) sites and have allegedly taken some of them down. Once this happens, new ones pop up very quickly, albeit, hosted on a different server. According to the Canadian 'Citizen lab'[92], however, not all IS sites, or supportive sites, in Iraq are targeted. Some are, perhaps intentionally, left functional even though the Iraqi government severely restricted the average Iraqi's access to the internet and cut off social media and video sharing sites as a response to IS's operations in Mosul and Tikrit during May 2014. This could indicate a gain-loss calculation by the Iraqi intelligence services in a desire to collect information and track users rather than cut off messaging.[93]

These are challenges that IS try to mitigate through constantly developing their strategy and platform use to evade censorship, avoid deception and detection by, e.g., Twitter's spam-algorithms, in order to keep information flowing, but also by having followers post IS content on their own accounts and by having "disseminators" distribute content.

Taking a more general view, however, on the IS social media campaign, comparing it with other actors in the arena, one finds that even though they might be adept at using social media and apparently have a sound strategy for its utilisation, they cannot, however, rely on the social media campaign alone. In order to create the desired effect they will have to continuously match their words with deeds and not only through significant, yet still limited, acts of terror, but through gaining mainstream traction in the Umma. In a conflict framework, IS are early adopters of the social media technology and the cross-media approach and the informational advantages it affords them. But the question is if they can keep up this advantage as they are increasingly challenged (both on- and offline) at their own game

(12) Diaspora is a decentralised network where data is stored on private servers that cannot be controlled by a single administrator. Not even the platforms' creators can remove content from the network as they do not control the independent servers hosting the content.

by the regimes in the Middle East, Western intelligence services and their rival jihadist factions that do not agree with their proclaimed Caliphate?

INTERIM CONCLUSION

The Information and Communication Technology, and in particular social network media, has as it has developed, both technologically and conceptually in regard to its use, made it possible for everybody with an internet connection, both from within and without the conflict area, to watch how a crisis evolves and escalate and also how to affect it. Any given person outside the conflict area, who otherwise would not have been an actor, or in any other way been a part of the conflict, has the ability to actually have an effect on the way that the crisis unfolds, at least at a micro-level, but even at the macro-level, as the IS case study indicates. This development shows that the use of social network media in conflicts has changed the character of communications in crisis situations. This is impacting people, states and organisations in an increasingly global fashion, and as a result, expectations are now extremely high as to how states and international organisations respond to a crisis and communicate throughout it. Before decision-makers become aware of individual incidents in a crisis, there will most likely be cameras "on scene", able to "broadcast" the incident in near real-time. In the absence of reliable information, a state or organisation cannot act in an appropriate manner, leaving it behind the curve (or with a slower OODA loop).[13] This does, however, not stop media from picking up on it and reporting it "live", perhaps minute for minute, increasing the pressure on the state or organisation to act.

This also has an impact on how military forces or non-state actors can use social network media for operational purposes. The developments highlight the need for military organisations (and non-state actors) to not only have a presence in social network media, but to have (strategies) doctrine, organisation and capability enabling them to "operate" in the part of the cyber-domain to which social network media belong. This entails the capacity to use social network media as both a *sensor* and an *effector* in order to achieve desired effects, effectively weaponizing social network media.

(13) OODA loop stands for Observe, Orientate, Decide and Act. It was invented by US Colonel John Boyd to describe decision-making processes in operations. According to Boyd, decision-making is a cycle of OODA which repeats itself and the one with the fastest OODA loop will have an advantage.

Today, social network media pervades nearly all aspects of daily life, especially in urbanised areas. This is also true in contemporary conflicts. However, regardless of being part of a conflict situation or not, social network media shares a series of characteristics. First and foremost, they are online platforms that facilitate interaction, collaboration and the exchange of ideas, information and opinions. In other words, they are about sharing multimedia content, which the users also can alter and re-distribute within their own networks, through conversations, commenting and user-generated content. Due to the speed and nearly unrestricted range, this interaction can also empower users to achieve effects on other users, potentially worldwide. Social network media can, hence, in this context, be defined in this manner:

"Social network media refers to internet connected platforms and software used to collect, store, aggregate, share, process, discuss or deliver user-generated and general media content that can influence knowledge and perceptions and thereby directly or indirectly prompt behaviour as a result of social interaction within networks".

At an operational or conceptual level the weaponization of social media also entails adopting a cross-media communication approach to planning how the target audience should experience the multimedia content and be encouraged to participate in the conversations through exposure to several interlinked media and platforms. This, among other things, is a question of whether one should just re-mediate the content across multiple platforms, or adapt content to individual platforms according to the possibilities and limitations they have and to which degree and how the audience can interact with the content. This includes trying to utilise known user behaviour and basic characteristics of that behaviour within respective networks. For example, by exploiting people's constant search for complementary information, different perspectives and emotional fulfilment from sources already within their established networks and preferred information sources. This also requires taking a time aspect into planning considerations. This includes appreciations on whether content is to be released in sequences or simultaneously on several platforms, and if the release should be scheduled, real-time or perhaps "on demand".

One aspect of the utilisation of social network media in contemporary conflicts is therefore how to prompt the audience to participate in the networks and conversations and how to guide them to and through the

different platforms. Another aspect is the strategic narrative approach to the content on these platforms. As guiding framework strategic narratives might be politically or ideologically constructed by the different actors but when employed in social network media special appreciations must, however, be made. Cross-media narratives in social network media are more open-ended and the possibility for audience participation can create new "twists" on the narrative, which essentially is uncontrollable for the author. Nevertheless it is still a question of a single narrative being supported by story-element or components told through different media. Cross-media narratives are being supported by self-contained stories or "micro-content". This micro-content is, despite the fact that the audience can change it, supportive of the overall narrative, but different from more classical, narrative-driven strategic communication characterised by distributed dissemination by multiple actors. These characteristics are also visible when examining how The Islamic State (IS) in Iraq and Syria use social network media to project their narrative about the "caliphate".

One thing is the philosophy of (the social constructivism informed) cross-media communication based on a strategic narrative when planning the use of social network media to create specific effects in the information environment from a conceptual point of view. Another is the specific effects needed to be achieved in order to support specific operational objectives through an effects-based approach to, or conceptualisation o, the planning of "military" activities in social network media.

CHAPTER 4

EFFECTS-BASED THINKING ON SOCIAL MEDIA

EFFECTS-BASED THINKING

As shown throughout this monograph, the use of social network media in contemporary conflicts is about creating specific effects in and through easily accessible internet based platforms. This requires some sophisticated planning – particularly if a cross-media approach is being considered. Conceptually it is about how to plan the sequential and inter-linked use of multiple platforms toward a common objective and how to use cross-media narratives as the central framework for all content. Both these elements in the conceptual approach of course relate to how to create desired effects. In other words, it is about the strategic "informational" architecture behind predominantly the "psychological warfare" aspects of social network media use in contemporary conflicts. There are, however, also a series of other types of effects that can be created in and through social network media in contemporary conflicts at a more operational and tactical level. Effects that are associated with other "military" or war-fighting activities as targeting, intelligence collection, offensive and defensive operations, to include computer network attack or hacking, and command and control activities, all in a planned and coordinated manner. It is about the cumulative consequence of one or more actions across the "engagement space" (social network media) that leads to a change in the situation in one or more of domains: the political, military, economic, social, infrastructure or information (PMESII), or as Hans Henrik Møller puts it:

> "Effect-based thinking is therefore a philosophy that includes a much broader understanding of the creation of effects than merely combat and the physical destruction or neutralization of target sets. Effect-based thinking as a consequence involves the full use of all instruments of power or influence that are political, economic, social, psychological, etc., and involves governments, nongovernment organizations, and agencies across nations in order to shape the decisions of friends, foes, and neutrals, thereby improving effectiveness".[94]

Although Møller is writing about NATO's use of military, political, economic and civilian instruments of power to achieve effects, the quote might just as easily explain the range of possible applications of social network media to create effects within the same four domains.

Effects-based thinking in principle

In principle thinking about how to achieve effects in and through social network media is a philosophy that complements other existing and more established "military" planning philosophies. It involves focussing on outcome rather than the means, and is therefore inherently focused on determining the effect(s) that must be created in order to influence the perception, behaviour and capabilities of specific target audiences in order to achieve this desired end-state. It can also focus on changing the context in which a situation is understood and the associated discourse.

Effects-based thinking is also about considering the engagement space as a system (or system of systems) in which all actors and entities interact to create effects that can all impact on that system. To understand this environment – which is highly complex – the various narratives and their key exponents – the influencers – need to be identified as well as the effects they are seeking to achieve. There are likely to be numerous different actors in this environment and its worth taking a moment to consider which views the military is likely to espouse.

"MILITARY" ACTIVITIES AND DESIRED EFFECTS

In his article, "Cyber war will not take place", Thomas Rid, as also discussed earlier, introduced three activities within which all cyber activities fall: Espionage, Subversion and Sabotage. Those three categories, although covering a lot, are not, however, deemed sufficient to describe all the activities and effects sought to be created through the use of social network media in contemporary conflicts. There is therefore a need to develop or design an "effects framework" for organising and describing activities and effects in order to systematize the analysis of both the theoretical and the empirical aspects of social network media in contemporary conflicts.

The effects framework, shown in figure 4.1 below, is based on several sources. It can be seen that it includes Thomas Rid's three categories (espionage, subversion and sabotage) but is much broader. In particular, it makes use of some of the issues raised by British academic Shima D. Keene in her book on "Threat Finance", in which she categorises terror-organisations'

use of social network media in five distinctly different categories: Target Selection; Information Operations; Psychological Operations; Recruitment and Fundraising.[95] In addition to Rid and Keene's contributions, the effects framework includes empirical observations from Iraq, Afghanistan, Libya, Syria and Ukraine in regard to contemporary use of social network media for "military" purposes. Furthermore, NATO's terminology on effects has helped shape the framework.[96] According to NATO, an effect is defined as "a change in behaviour or physical state of a system (or system elements) that results from one or more actions, or other causes".[97]

The framework consists of six core activities where social network media, as discussed above, can be utilised for a series of "military" activities, whether by state or non-state actors (even down to the individual level), such as Intelligence collection, Targeting, Psychological Warfare, Cyber-Operations and Command and Control.

Targeting being a question of finding or identifying which social network media profiles and accounts that should subsequently be either monitored, attempted influenced or attacked (hacked). Intelligence collection means the focused search for and analysis of information from social media networks and profiles including content and conversations, but it can also be a question of, for example, "crowd-sourcing" information either overtly or covertly. Psychological Warfare is of course a question of the dissemination of messages and images to influence target audiences' perceptions, attitudes and behaviour. This can also include deception. Operations can be the targeting of social network media platforms and accounts either with the purpose of breaching, e.g., password-protected chat-rooms, altering the content on a profile or completely rendering it unusable. And lastly, Command and Control is a question of using social network media for communication and coordination and synchronization of activities. A common denominator, however, is that all these activities, regardless of whether they may have both on- and offline effects, can be conducted in and through social network media.

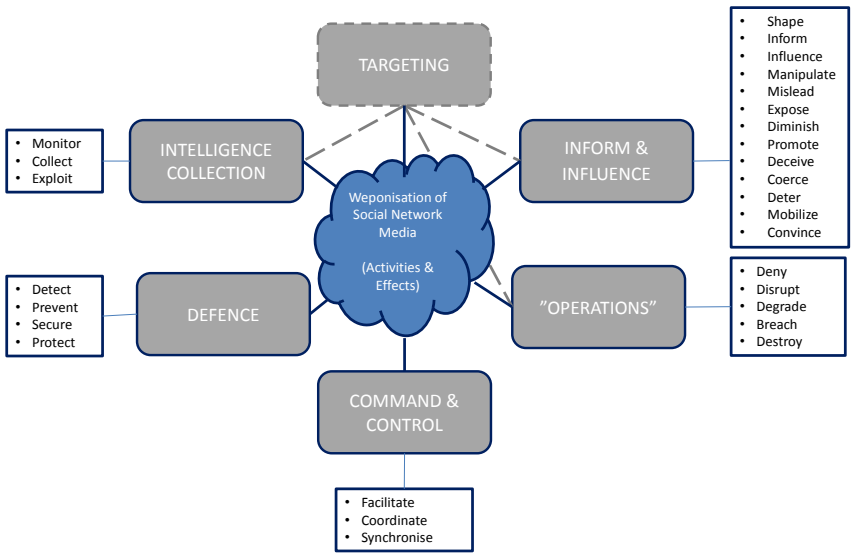

Figure 4.1. Activities and Effects framework.

Targeting

Targeting is an activity or process that can be described as the guidance concerning the coordination of target nominations (targets and target audiences) in support of the creation of desired effects. It is therefore a process to coordinate and synchronise the desired effects with the other activities, conducted in or through social network media, which should create the effects in time and space. Increasingly, targeting is now not just about the selection of conventional military targets but also includes a recognition that effects can be achieved in other ways – some of those may be through social network media – and thus targeting is increasingly being regarded as a full-spectrum activity with hard kinetic power at one end (in this regard, e.g., Hacking or defacing a social network media account) and softer effects at the other (such as deception). The use of social network media for intelligence therefore affords actors with more options in regard to monitoring, tracking and targeting of potential persons, groups, nodes or networks, platforms and content (e.g., existing narratives and actual messaging) of interest. Intelligence collected can thus be used to nominate targets – be that social media profiles, sites, accounts, computers behind these (system level), where to place information (words and images) and other content, influence conversations, how to link things and / or directly address target audiences in order to influence their perception, attitude

and behaviour (on- and offline). Finally, intelligence collected from social network media can be used for identifying and nominating targets in the physical domain based on geo-tacked pictures and updates and more. Conversely, information from social network media conversations can also be used for "Bomb Damage Assessment" (BDA) in order to verify the effect of traditional employment of weapon systems (e.g., air delivered munitions, artillery etc.).

Activity:	Effects verbs:	Explanation / definition:
Targeting		Guidance concerning the coordination of target nominations in support of the achievement of effects.

Figure 4.2. Targeting effects[98]

Intelligence

Intelligence can be seen as the product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning countries or areas of interest, to include specific domains that are not geographical in nature, such as the global information environment. But Intelligence collection is also an activity in itself. In respect to social network media, intelligence is about monitoring online activity and behaviour in order to collect and aggregate information and data on and from networks, sites and platforms considered as social network media, including the persons and personas behind them. This is all in order to analyse this information and data to generate knowledge and understanding in general and in particular in order to support the targeting process. Some of what differentiates intelligence collection in social network

media from other intelligence activities is the possibility for overt or covert crowdsourcing[14] and the mapping of narratives.

Intelligence analysis of social network media can include but is not limited to Trend, Network , Sentiment, Geo-, Content, Behavioural, Systemic and Information analysis. All of these analysis forms can, in turn, contribute to more specific target audience analysis (TAA) and content development in support of psychological warfare or selection of targets for "cyber-operations" in and through social network media.

Analysis type	Description
Trend analysis	Tracking changes and spikes in key variables over time and comparing these.
Network analysis	Looking at relationships, links and social networks and their propagation over time. Additionally the connectivity of the people has to be taken into account. You have to ask the question "Who is talking to whom and how often?" to find out where the key players in the network's hierarchy are located.
Sentiment analysis	Exploring verbally and graphically expressed feelings, attitude, and emotions towards a certain topic.
Geo-analysis	Finding out where things are happening.
Content analysis	Extracting themes, key words, semantics, meanings, sentiments; exploring communicator's intent ("Why?") and ways of communicative expression.
Behavioural analysis	Tracking user's website visitation, browsing and interactions.

(14) The idea of social network media is closely linked to the concept of crowdsourcing, a neologism between the terms "crowd" and "outsourcing". According to journalist Jeff Howe, who invented the term in 2006 crowdsourcing represents the act of a company or institution taking a function once performed by employees and outsourcing it to an undefined (and generally large) network of people in the form of an open call. This can take the form of peer-production (when the job is performed collaboratively), but is also often undertaken by sole individuals". The fact that social network media platforms (e.g. YouTube, Wikipedia, iStockphoto or InnoCentive) are successful, prove that normal people are willing to create content or to solve problems on the internet. Something that can also be exploited in connection with conflicts. (Source: Howe, Jeff, The Rise of Crowdsourcing, The wired Magazine, June 2006. (Accessed 26 MAR 14) http://www.wired.com/wired/archive/14.06/crowds.html. (Accessed 26 MAR 14) and Howe, Jeff, Crowdsourcing: A Definition, June 2006. (Accessed 26 MAR 14) http://crowdsourcing.typepad.com/cs/2006/06/crowdsourcing_a.html.)

Systemic analysis	Holistically look at dependencies and influences between different analytic methods in order to gain a comprehensive operational picture.
Information Extraction	Extracting themes, named entities, key words, meanings, sentiments, rhetoric, etc.
Target Audience Analysis	TAA is the process of profiling an audience to understand what motivates them and assess what behaviours they may engage in.

Figure 4.3. Types of analysis

Social network media analysis is therefore a strategic tool for uncovering insights into the posted content, trends, networks and online behaviour of audiences and other stakeholders. In the context of systemic intelligence collection and analysis, it offers a detailed picture of networks, actors, and related communication (interaction), with the help of monitoring tools, all of which has to be tailored to gain a comprehensive understanding of the social network media information environment. It also provides possibilities for mapping who the disseminators, influencers or key opinion-makers are and how they drive the conversation around topics of interest, and people's conversations and actions online that can be mined for insights and understanding. What also makes social media particularly interesting within an intelligence context is the possibility for collection of real-time data – depending on the speed of monitoring and analysis software. In addition to this, social network media allows for intelligence collection and analysis without boots on the ground, or even physical presence in the area of interest (theatre of operations), this feature of social network media (analysis) makes it particularly interesting from a "remote warfare" point of view, which is when access to an operational area is initially contested or even impossible for several reasons (political mandate, Rules of Engagement (RoE) or for security reasons), or when mostly non-state actors desire to create effects within a conflict area. Libya and Syria are good examples of this. Basically it provides options for leveraging online sharing and conversations in "theatre of operations", which ultimately can lead to engagement with, or targeting of, current and future audiences and influencers.

Activity:	Effects verbs:	Explanation / definition:
Intelligence	Monitor	Observe and check the progress or quality of (something) over a period of time; keep under systematic review.
	Collect	Systematically seek and acquire information. (E.g., to assemble, accumulate data or information)
	Exploit	Make use and derive benefit from a resource. (E.g., attempts to gather information that will enable the conduct of operations to induce other effects; to gain access to adversary systems to collect information or to plant false or misleading information).

Figure 4.4. Intelligence effects

Cyber-Operations

Cyber-Operations can generally be divided into three separate but complementary activities; Computer Network Attack (CAN), Computer Network Exploitation (CNE) and Computer Network Defence (CND).[15] The first two can furthermore be categorised as "offensive" and the third as "defensive" (the defensive will be discussed later). The offensive operations referees in this contest primarily to activities associated with "computer network attack" (CNA), as described in the in the cyber-warfare definition discussed earlier. This can include Distributed Denial of Service (DDoS)

(15) According to NATO doctrine on Information Operations CAN, CNE and CND can be described as follows:
"Computer Network Attack. Software and hardware vulnerabilities allow computers, storage devices and networking equipment to be attacked through insertion of malicious code, such as viruses, or through more subtle manipulation of data, changing the characteristics and performance of the devices or the expression and display of the information contained therein. This capability is enhanced by the increasing use of commercial off-the-shelf software in military systems" (including social network media technology). "**Computer Network Exploitation**. (…) the ability to get information about computers and computer networks, by gaining access to information hosted on those and the ability to make use of the information and the computers/computer networks" (without being detected). "**Computer Network Defence**. The purpose of CND is to protect against CNA and CNE. CND is action taken to protect against disruption, denial, degradation or destruction of information resident in computers and computer networks or the computers and networks themselves. CND is essential to maintain decision-making capability; as well as maintaining a defensive posture, it will use monitoring and penetration protection techniques to detect, characterise, and respond to an attack, instigating containment and recovery action as required". (Source: NATO Allied Joint Publication – AJP 3.10 Information Operations, NATO 2009. https://info.publicintelligence.net/NATO-IO.pdf, page 1-11 (Accessed 9 FEB 15).

attacks on websites (example Blog), the breaching (hacking) of pass-word protected chat sites, e-mails or cell-phones, with the purpose of later exposing the content; intrusion on news agencies' cable news and altering news stories; or altering content and imagery on, e.g., a Facebook profile, etc.; or pinching identity information like usernames and passwords. It can also be intrusion into, e.g., databases in order to, undetected, extract information for intelligence purposes, also known as "computer network exploitation" (CNE).[99] All of these "offensive" activities can be conducted in social network media by all types of actors, state and non-state, and is typically aimed at technically preventing other actors from using specific social network media platforms, at least temporarily. This can be to prevent other actors from communicating with each other, coordinating and synchronizing actions in time and space, accessing information or distribution messages and propaganda.

Activity:	**Effects verbs:**	**Explanation / definition:**
Operations	Deny	Refuse access to. (E.g., to prevent someone from accessing and using critical information, systems, and services. Damage done to the functionality is only temporary, but all aspects of the functionality were affected. A functionality's operation is impaired over the short term, but the damage extends to all facets of the functionality's operation.)
	Disrupt	Disturb or interrupt. (E.g., to break or interrupt the flow of information, to use force or other non-lethal means to shatter the cohesion of a (target) audience and prevent them from functioning effectively. Damage done to the function is temporary, and only portions of the function were affected. A function's operation is impaired over the short term and the damage does not extend to all facets of the function's operation.)

	Degrade	To lower the character or quality of an adversary C2 or communications systems, and information collection efforts or means; or to degrade the morale of a unit, reduce the target's worth or value, or reduce the quality of adversary decisions and actions.
	Breach	Make a gap in and break through. (E.g., in a firewall, a password, or other defence or security measure.)
	Destroy	Put an end to the existence of (something) by damaging or attacking it. (E.g., to damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.)

Figure 4.5. Operational effects

Psychological Warfare

One of the potentially fertile areas for weaponizing social network media is the psychological warfare (PsyWar) area. Psychological Warfare refers in this context to those activities associated with influencing a target audience's values and belief system, their perceptions, emotions, motives, reasoning, and, ideally, their behaviour. Self-evidently, this involves inducing perceptions, attitudes and behaviours favourable to the originator's objectives. This might be done either overtly or covertly. Covert operations under one are sometimes referred to as "black operations" or "false flag tactics", and could involve untruthful attribution of information or the source behind specific information (content) or outlets (social network media platforms).[100] This is counter to NATO doctrine but has been well demonstrated by Russia's recent incursions into Ukraine and the Crimea. Target audiences for such operations could be governments, organizations, groups, and indeed even individuals. Such was the case in 2008 when Georgia's President Saakashvili was directly and personally targeted.[101] PsyWar can also include activities such as Deception, Propaganda and Subversion. Utilising cross-media communication methods PsyWar conducted in and through social network media can be very effective, particularly when used in combination with more traditional means of communication and media, as seen with Islamic State.

However, this description of PsyWar can be problematic since it suggests a high level of the use of clandestine methods and activities normally associated with "propaganda", a term which has a distinctly, and unfair,

negative connotation.[16] In most western military doctrine, there is normally a distinction between activities that seek to "inform" the media - "Public Affairs" (PA) or Media Operations - and those more concerned with "Influencing" the media as part of a process of reaching opposing or hostile audiences – which in military terminology is more commonly known as, psychological operations (or PsyOps). There therefore exists a debate over "Inform" versus "Influence" functions, at least in western liberal democracies, as it is contrary to the most basic values of not lying to the press and the public. This self-same debate is emerging over the use – by militaries –of social network media – is this use to influence or just to inform? – and to what extent should our own soldiers be allowed to use social network media? The latter issue is also tied to operational security (OPSEC) concerns, and considerations over the sustainment of social network media competences within own forces by a potential ban on the use.[102] Regardless of the political, legal and ethical debates within western liberal democracies and their militaries over the use of social network media, non-state (and some state) actors use social network media very actively for propaganda purposes (the IS case study in the previous chapter is a case in point) and do not delineate between the concepts of Inform and Influence. They use social network media exclusively for Influence purposes.

(16) Philip M. Taylor, in his book "Munitions of the Mind" from 1991, described propaganda as a value neutral process and defined it as "a process of persuasion which utilizes any available means (media) to persuade people (target audiences) to think and/or behave in a manner desired by the source in order to benefit the interests of that source, either directly or indirectly".

Activity:	Effects verbs:	Explanation / definition:
Psychological Warfare	Shape	Develop in a particular way. (E.g., to determine or direct the course of events; to modify behaviour by rewarding changes that lend toward a desired response; to cause to conform to a particular form or pattern).
	Inform	Give information.
	Influence	The capacity to have an effect on the character or behaviour of someone or something, or the effect itself. (E.g., to cause a change in the character, thought, or action of a particular entity. (Selected projection or distortion of the truth to persuade the opposition to act in a manner detrimental to their mission accomplishment while benefiting the accomplishment of friendly objectives.))
	Manipulate	To handle or control with dexterity or to control or influence cleverly or unscrupulously.
	Mislead	Cause to have a wrong impression about someone or something. (E.g., to create a false perception that leads someone to act in a manner detrimental to mission accomplishment while benefiting accomplishment of friendly objectives).
	Expose	Make something visible by uncovering it. (E.g., to reveal something undesirable or injurious).
	Diminish	Make or become less. (E.g., to reduce the effectiveness of an activity; this is similar to degrade, without the lethal overtones.)
	Promote	Further the progress of; support or encourage.
	Deceive	Deliberately cause (someone) to believe something that is not true.
	Coerce	Persuade an unwilling person to do something using force or threats.
	Deter	Discourage (someone) from doing something by instilling fear of the consequences. (E.g., to prevent a potential or actual adversary or other target audience from taking actions that threaten coalition interests)

	Mobilize	Organize and encourage (a group of people) to take collective action in pursuit of a particular objective.
	Convince	Cause to believe firmly in the truth of something. (E.g., to overcome by argument, to bring to belief, consent, or a course of action).

Figure 4.6. Psychological warfare effects

Defence

Defensive operations refer to the protection of own social network media platforms, sites, profiles and accounts in the form of "computer network defence" (CND) at the technical or system level. Information assurance (IA) – a term that denotes the continuous efforts to ensure the integrity of information posed – and at the human level Operational Security (OPSEC) and Counter Intelligence (CI) are both terms designed to prevent the loss of sensitive information and counter external threats. Defensive activities can include the use of, e.g., encryption, anti-tracking and IP-concealing software in connection with social network media.

Activity:	Effects verbs:	Explanation / definition:
Defence	Detect	To discover or identify the presence or existence of a threat. (E.g., an intrusion into information systems).
	Prevent	To keep from happening or arising, or render unable to do something. (E.g., to deprive of hope or power of acting or succeeding).
	Secure	To have provisions against attack or to make certain something or somebody remains safe and unthreatened.
	Protect	To keep safe from harm or injury or measures taken to protect or prevent something. (E.g., to keep from harm, attack, injury or exploitation. To maintain the status or integrity of a system. To take action to guard against espionage or capture sensitive equipment and information).

Figure 4.7. Defence effects

Command and Control

Lastly social network media can be used for Command and Control (C2)[17] purposes. In respect to social network media, C2 is about internal communication, information sharing, coordination and synchronisation of actions and facilitates more agile decision-making. Command and Control generally applies to endeavours undertaken by collections of individuals and organizations of vastly different characteristics and sizes for many different purposes. The most interesting and challenging endeavours are those that involve a collection of military and civilian sovereign entities with overlapping interests that can best be met by sharing information and collaboration that cuts across the boundaries of the individual entities.[103] This is often the case when looking at, e.g., non-state actors, who like opposition groups in Syria, have a need for distributing information, internally and externally, and for coordinating and synchronising actions, and in some cases giving commands or direction and guidance (D&G) to other groups or entities. Particularly when these groups or entities have no formal structure or are dispersed over large geographical areas, social network media can afford them with means and capabilities to conduct C2 activities. They have, though, to be very cognisant of operational security (OPSEC) issues.

Command and Control is scalable. At an organisational level, C2 is about shaping the organisation and determining its purpose and priorities. Information and output from this process can, of course, be distributed through social network media to the rest of the organisation. The more interesting elements are, however, at the "mission" level. At the mission level, C2 is about employing the organisation's assets and capabilities (people, systems, material and the relationships between them) towards a specific objective or task.[104]

(17) Command and Control in NATO is defined as: "Command and control (C2) encompasses the exercise of authority and direction by a commander over assigned and attached forces in the accomplishment of the mission". The doctrine goes on to state that "Command includes both the authority and responsibility for effectively using available resources to achieve desired outcomes. Command at all levels is the art of motivating and directing people and organizations into action. The art of command lies in conscious and skilful exercise of command authority through decision-making, and leadership. Using judgment and intuition acquired from experience, training, study, and creative thinking; commanders visualise the situation and make sound and timely decisions. Effective decision-making combines judgment with information; it requires knowing if to decide, when to decide, and what to decide. Timeliness is the speed required to maintain the initiative over the adversary". (Source: NATO Allied Joint Doctrine (AJP) 03 (B) – Operations, paragraph 0147 + 0148).

NATO's research project (SAS-050) identifies three critical dimensions of command and control. (1) How decision rights are allocated throughout the organisation. (2) How to determine the permissible interactions between elements in the organisation, and between the organisation's different elements and outside organisations and entities. (3) How information flows are distributed.[105]

Activity:	Effects verbs:	Explanation / definition:
Command and Control (C2).	Facilitate	Make (an action or process) easy or easier.
	Coordinate	Bring the different elements of (a complex activity or organization) into a harmonious or efficient relationship – or to negotiate with others in order to work together effectively.
	Synchronise	Cause to occur or operate at the same time or rate (in time and space) or cause (a set of data or files) to remain identical in more than one location.

Figure 4.8. Command and Control effects

INTERIM CONCLUSION

Irrespective of the character of an organisation – national armed forces, rebel / insurgent group, political activists or some other form of non-state actors, the principles of effects- based thinking, as described in the introduction, can be applied to all their activities. All actors, state or non-state, can benefit from collecting intelligence or basic information, selecting targets and achieving effects on these targets, be it physical, informational or cognitive; and furthermore, protecting or defending themselves against other actors' similar activities and utilising the possibilities for communicating, coordinating and synchronising their activities in the manner that social network media affords.

Even though this monograph has divided them into six distinct activity areas (intelligence, targeting, psychological warfare, operations, defence and command and control), they are all mutual supportive, and at least two, often more, will be conducted simultaneously to create the desired effects (often

in concert with activities in the physical world). In any case, the maximum effect is achieved through a high level of planning and coordination.

The desired effects, associated with each of the activities as depicted in figure 4.1., can be achieved either on social network media itself (the platforms or networks) or through social network media on humans in order to affect perceptions, attitudes and ultimately behaviour. The one half of the desired effects therefore target the system level (technology). This half is therefore implicitly linked to "cyber-operations" and, e.g., "computer network attack" but can very well also have cognitive effects. The other half of the desired effects therefore target the informational and social levels of the information environment. The achievement of effects at the systemic level can also be the precondition for the achievement of effects on the informational and or social level(s).

One thing, however, is the theory behind an effects-based approach to using social network media as a weapons platform in contemporary conflicts; another is how it has been done so far empirically.

CHAPTER 5

THE WEAPONIZATION OF SOCIAL MEDIA

The previous chapter dealt with how one theoretically could approach the activities and effects possible to create in and through social network media. This chapter will look at how social network media in reality has been utilised for creating "military" effects in contemporary conflicts. Firstly, looking at the development over the last approximately fifteen years and, secondly, by looking at a series of empirical examples of the different activities and effects from Afghanistan, Iraq, Israel, Syria and Ukraine, etc., in order to discuss how social network media has been weaponized and how it affects the characteristics of contemporary conflicts.

THE SOCIAL MEDIA BATTLE-SPACE OF SYRIA AND WHAT WAS BEFORE

"The Syrian conflict is the world's first cyber civil war. Cyber communications are central to strategy and tactics employed by both Assad and the rebels".[106] This statement was put forward by Rafal Rohozinski, who is leading the Canadian based firm SecDev Group's efforts on monitoring internet activities in Syria. He goes on pointing out "that it is hard to overstate how heavily both sides depend on cyber tools to articulate their narrative, stories, themes and messages. The war has integrated kinetic and information warfare tactics in an unprecedented way"[107]. The internet and, especially, social network media are used for Command and Control (C2) purposes, providing lines of communication between dispersed groups for coordination and synchronization of tactics on the ground. It is also used for intelligence purposes, including surveillance and reconnaissance, obtaining and maintaining Situational Awareness (SA) through, e.g., "crowdsourcing" of information from denied areas and to receive training and advice on military matters from actors outside Syria. Last, but definitely not least, the cyber domain and social network media are used by all actors to wage Psychological Warfare in order to influence and shape perceptions, attitudes and behaviours of audiences, both inside Syria and internationally. Striving to make their voice heard and to silence that of the opposition. The Syrian civil war is thereby the first to occur in the full throes of the modern information environment saturated by cyber, where mobile technology,

social network media and tech-savvy digital natives[108] have created a potent mix influencing the character of the conflict.[109]

The use of the cyber domain for warfare is not new, though. The first signs of this tendency were seen for real already back in 1999 under the NATO-led Kosovo Air Campaign (Operation Allied Force) over Serbia and Montenegro, where the use of e-mails began to be a widespread way of communicating information about what was happening on the ground during the air campaign. The BBC reported back then: "There is a problem with the personal accounts of the war – how do we know they are true? It is easy to spot the propaganda Web-sites [sic] of the actors such as NATO or the Serbia Ministry of Information, but e-mails are supposedly individual points of view rather than concerted campaigns attributable to the actors. Yet they could be written en masse by government press officers or by hoaxers in California".[110] Operation Allied Force is often claimed to have been the first "internet war", where the use of the internet, and whatever cyber tools existed then, for the first time played a noticeable role and had an ability to influence aspects of how the war was fought. The tendency has since been increasingly visible as the technology has developed and afforded multiple actors with an even larger online toolbox or capability for waging war in the cyber-domain. As Christopher Burnett wrote in 2000:

> "We are engaged in a social netwar. The information age of the late 20th Century has enabled activists to work together globally while maintaining local autonomy. The power of this movement arises from its structure; namely a decentralized network capable of instant communication, collaboration, coordination and action (C3A). The implications of this movement are profound and amount to what has been called an 'associational revolution' among non-state actors that may prove as significant as the rise of the nation state".[111]

With the war starting in Iraq in March 2003, and later on in Afghanistan, the use of social network media started to play an ever-increasing role. Terror organisations and insurgent groups began using social network media to undermine the legitimacy and credibility of the US led Multinational Force (MNF), targeting the will of troop contributing nation's populations and political decision-makers to discontinue their presence in Iraq. The objective for the insurgent groups was to shift the centre of gravity (CoG) away from the physical battlefield and into the cognitive domain – through words and images on social network media.[112] A consequence of this was that terror

organisations and insurgent groups now had direct access to their intended audiences. This minimised their reliance on mainstream news media, who had acted as gatekeepers, to get their message out and achieve one of their strategic objectives; undermine their opponent's political will, while at the same time building support for their cause. Another consequence was that the audiences were no longer restricted Iraq internally, but became global. Already from an early point in time in Iraq, this showed itself to be a major challenge for western military forces, which had not yet fully learned to fight in the social network media domain of the information environment.[113] As Dr Niel Verrall from UK Defence Science and Technology Laboratories (DSTL) also points out when he questions "whether military commanders fully understand and appreciates the range of activities where social media could provide added value and demonstrate operational impact".[114]

By 2005, Al-Qaida had fully realised this. Illustrated by an alleged correspondence between the then number two in Al-Qaida, Ayman al-Zawahiri, and the leader of Al-Qaida in Iraq, Abu Musab al-Zarqawi, intercepted by US intelligence: "I say to you: that we are in a battle, and that more than half of this battle is taking place in the battlefield of the media. And that we are in a battle in a race for the hearts and minds of our Umma" *[Muslim community]*. Firstly, it shows that Al-Qaida as an organisation is well aware of the importance of media to their fight. Secondly, that the fight is as much internal as it is external, when it comes to affecting perceptions and behaviours.

Terror organisations now use social network media extensively for all elements of their 'operations'. This was exemplified by the Westgate Mall attack in Nairobi, Kenya, in September 2013, when the Somali Al-Qaida affiliated terror-group Al-Shabaab live-tweeted the attack from at least two different Twitter-accounts, and of course the Islamic State's use of social network media as previously discussed.

Other conflicts in the Middle East between Israel and Hezbollah in Lebanon (2006) and between Israel and Hamas in Gaza (2009 and again in 2014), respectively, also show how social network media was used to varying degrees of success by all parties. Initially the Israeli Defence Forces (IDF) was not particularly adept at using social network media, giving Hezbollah an advantage arguably so large that it enabled Hezbollah to portray itself as the both victim and victor of the conflict in 2006. Lessons identified from the 2006 Lebanon war allegedly drove the IDF development of an "offensive"

capability within social network media. This capability development continued up to the 2009 Operation Cast Lead in Gaza against Hamas rule, effectively changing the way the IDF conducted its information operations to include the use of social network media. Little attention, however, has been devoted to Hezbollah's exploitation of information as a kind of 'war-fighting function' with social network media as the weapon of choice.[115] The IDF has continuously developed their social network media capability ever since.

The 2006 Lebanon war between Hezbollah and Israel showed early on how social network media was successfully used in a contemporary conflict by a non-state actor to mitigate a conventional military disadvantage. Hezbollah was militarily outclassed by the IDF in all areas, yet they managed to exploit tactical engagements between the IDF and Hezbollah fighters on the ground through an information-led strategy creating strategic effects through primarily social network media. Hezbollah essentially out-manoeuvred the IDF land campaign in the information environment and thereby denied Israel the achievement of its strategic objectives. Effectively shifting the Centre of Gravity (CoG) from the physical battle to the information environment, Hezbollah succeeded in creating and sustaining regional and international pressure that eventually forced Israel to cease its operations before achieving its stated strategic objectives. Hezbollah heavily leveraged social network media to influence the political will of key global strategic audiences, including the Israeli population. Hezbollah "packaged" (recorded / filmed, narrated and disseminated) tactical events to include both own successes and Israeli mistakes and major kinetic destruction of sites in Lebanon in a well-coordinated multi-channel cyber-strategy. The desired effect(s) was to demoralise the Israelis, mobilize internal, regional and international support and, in turn, erode support for Israeli policy, recruit new members and at the same time undermine IDF credibility. At the same time, Hezbollah also managed to exploit Israeli soldiers' unauthorised use of cell phones during the operation by turning hacked and intercepted information from cell phones into propaganda products, effectively exposing compromising cell phone conversations and images. Hezbollah also used social network media for command and control and to defend their main information distribution channel (Al-Manar TV) from IDF cyber-attacks. Information (propaganda products) was, besides being aired over Al-Manar TV, re-distributed regionally and globally through PowerPoint presentations, video-clips and photos with an attached story in e-mails, video up-load sites, social media and blogs. Through the cyber-information

strategy, Hezbollah effectively was able to claim a strategic victory despite the absence of a clear military victory.[116]

In the 2009 Hamas-Israel conflict, the hostilities on the ground were mirrored by cyber-informational and social battles for hearts and minds in the social network media sphere.[117] Both sides extensively used, among other social platforms, blogs, Wikipedia, YouTube, Twitter and Facebook to tell their different versions of the events, and to a high degree coordinated the online social network media activities with traditional media and diplomatic activities. The IDF furthermore, besides setting up a new organisation[18] to handle this aspect of the conflict, developed their traditional Psychological Operations (PSYOPS) activities even further. PSYOPS were not just a question of radio broadcasts and leaflet drops but also included SMS text messaging to Hezbollah combatants and Lebanese non-combatants, which meant taking PSYOPS into the social network media sphere.[118] Both Hamas and the Israelis also mobilised "patriotic hackers" and online activists to engage in a cyber-battle for control over the social network media sphere. This was done through "force multiplication" activities, such as creating supportive online communities and networks as well as through direct computer network attacks on, or hacking of, the opposition's social network media accounts and platforms. While this electronic battle in the social network media sphere went on, the traditional media was to a large extent denied access to the battlefield, effectively leaving social network media as the primary source of information for many. Israel also succeeded in shaping the news coverage itself through turning the sheer use of social network media for warfighting purposes into a "process story" in mainstream media. Through the mainstream news' coverage Israel also got their content out indirectly. In turn, this attracted even more attention to their online presence and their social network media accounts and platforms. This tactic has to a great extent been mirrored by the Islamic State in their 2014 social network media efforts.

(18) Israel created, based on the recommendations from the so-called "Winograd Commission" a National Information Directorate (NID) to deal with "Hasbara" (explanation) tasked with amongst other things coordinate core messages with Jewish communities, bloggers and other backers using on-line networks. The NID was shortly after the Operation Cast Lead started backed up by the "IDF Spokespersons Unit" that amongst other things became very active on YouTube, Facebook and Twitter. (Source: Caldwell, Murphy and Menning, 2009, page 6-7.)

It is, however, not only in "inter-state"-like conflicts such as Israel-Hezbollah (2006) and Israel-Gaza (2009) that the use of social network media in conflicts has developed. During the so-called "Twitter Revolution" in Iran, in 2009-2010, in connection with election protests and riots over the presidential election, social network media also played a noticeable role as a tool for political mobilization and distribution of documentation on regime's abuses to the outside world. This directly affected the policies of the international community and individual nations such as the United States. The US government allegedly asked the company behind Twitter to delay a software update in order to facilitate the continued use of the platform by the Iranian demonstrators.[119] The Twitter Revolution was the first instance, which received major international attention, of social network media being used for large scale political mobilisation, but certainly not the last.

Starting in late 2010, a wave of anti-authoritarian uprisings and rebellions, originating in Tunisia, and then spreading to Egypt, Libya, Bahrain, Yemen and Syria and destabilising several other Middle-Eastern regimes, transformed the political landscape of the Middle East.[120] "The Arab Spring" or the "Arab awakening" is also often associated with the widespread use of social network media. It is, however, much debated if social network media started the "uprising" or mainstream television started it – in media terms. Social network media, nonetheless, for certain helped spread and sustain it, and quickly became the tool of choice for organising and coordinating events throughout the Middle East. As well as distributing information and documentation about the events. The uprisings themselves were based on more deeply rooted causes.

However interesting, what started the Arab awakening is not the focus here, but rather how the social network media, due to their digital connectivity, was used to mobilise the predominantly urbanised youth in these countries.[19] Throughout the uprisings the use of social network media continuously developed in response to the dynamics of the situation, including the quick circumvention of any attempts to limit communication, by the quick exploitation of new technological developments. For example,

(19) It is worth noting that the increased connectivity, and the effects of it, is only brought about by the improved access to electricity, lower-cost mobile technology and changes in how the internet in general is organised, it is also due to the fact that most of the users are urban, relatively tech-savvy youth. All factors that are preconditions for the exponentially growing effect of social network media in contemporary conflicts. (Source: Kilcullan, 2013, page 170 & 199).

the introduction of new technology as "speak-to-twitter" based on analogue landlines, when regimes (as the Egyptian one) had cut off access to the internet and mobile connections in order to avoid further mobilization of the "masses". It took only two days for Google engineers to build a system, based on international telephone numbers that people could call and leave a voice message that would be transformed into a Twitter feed. This enabled protesters in Egypt to send tweets even though the internet was shut down.[121] It also allowed for outsiders to listen to the tweets on www.twitter.com/speak2tweet. This case also shows that for-profit companies are active participants in the contemporary conflict information environment. A tendency that has evolved since to a point where employees of these companies today are targets for, e.g., terror organisations like the Islamic State in Syria and Iraq due to the active role they play in combatting the distribution of terror propaganda on platforms like Twitter, for instance.

The Arab awakening also shows that "Virtual platforms provides not only free speech. They can also mobilize a large mass of people. You have to know that you're not the only one on the court who demonstrates against the System".[122] This observation illustrates the ability of social network media to create perceptions of "critical mass" that again create a sense of security and provide "social proof" for individuals to join a movement or participate in an event. Initially, whether real or unreal is not an important distinction, the perception of the critical mass's existence informs behaviour in real life. These mechanisms, brought about by the agile and strategic use of social network media, and the constant development of technology and software to support it, are in a very real way able to create changes! Changes in who is empowered and in the distribution of power itself within the international system in contemporary crisis and conflicts.

As a part of the Arab awakening, the situation in Libya went from protests in mid-January 2011 to a civil-war-like situation in February 2011. The world saw here how the Libyan rebels used the internet to mobilize protesters, and to gather internal, regional and international support. The rebels, however, also actively used the internet, and in particularly social network media, for gaining military knowledge from the outside. One, now rather famous, e.g., of this is involves three persons from different parts of the world; one in Finland, one in England and a rebel fighter on ground in Libya. The latter lacking knowledge about how to engage a specific weapon system (Grad 122 mm Multiple-Rocket Launcher). He put out a "request for information" not to his peers but through crowdsourcing. Between the three

of them, via a Skype call over mobile phones they found a solution, based on their collective knowledge, that enabled the rebel fighter to engage and successfully destroy the rocket launcher in real time.[123] The Libyan conflict also illustrated how international news organisations used social network media, sometimes as the primary source of information for their coverage of the conflict. For example, Al-Jazeera used Twitter-feeds extensively to substantiate their stories about how the conflict in Libya unfolded on the ground. Furthermore, the conflict in Libya also showed some of the first tendencies for using social network media in a more operational way. NATO allegedly used social network media for intelligence collection, targeting and Bomb Damage Assessment (BDA) as a supplement its more traditional military intelligence capabilities.

The use of social network media for operational purposes, though, is filled with challenges, including the severe difficulties associated with attribution and authentication of content. One small case from Syria shows this clearly. In 2010, it caught the attention of the world media when the news about a Syrian lesbian blogger in Damascus spread globally very quickly. Just as quickly, however, the world found out that "she" was a "he", more precisely, a middle-aged American man named Tom MacMaster, based in Scotland.[124] This case illustrates just how difficult the attribution of the information disseminated on social network media really is. The Syrian conflict, however, offers many other examples of how social network media has been used by the regime, rebels and a variety of external third parties. These examples also illustrate how actors continuously develop their capabilities based on experiences from earlier conflicts to weaponize the use of social network media in order to achieve "political" or "military" effects.

THE ACTIVITIES AND EFFECTS

As discussed in the previous chapter the weaponization of social media translates into "military" activities such as targeting, intelligence, psychological warfare, cyber-operations (offensive and defensive), and command and control in support of the achievement of political or military effects created in and through social network media. These effects are achieved in either the "physical" domain (e.g., components, software, platforms, networks and information systems (e.g., deny) or information itself (e.g., manipulate)) or in the cognitive domain on supporters (e.g., mobilization), the undecided (e.g., convince) or on the opposition that can be entrenched, (e.g., deter). Often concerns the creation of emotional responses that can go viral in order to rally local and international support or

inform and affect the discourse or narrative about a conflict. The following sections on each of the activities, as described in chapter four, offers some more empirical examples on the specific effects achieved in and through social network media in recent conflicts.

Targeting

Prominence in social network media makes people, as well as their platforms and accounts, targets in contemporary conflicts. Finding and affecting or influencing an opponent's presence in social network media is therefore an integral part of cyber-warfare, and hence of contemporary conflicts. As seen in Libya, Google Maps and cell phones were used to map regime positions, which were then passed on to NATO, which used the information to nominate targets and engage these with air power.[125] To use this approach, however, requires intelligence preparation, as the information retrieved from social network media needs to be verified by other intelligence sources before they can be used for targeting for air operations. US Central Command (CENTCOM) in Tampa, Florida, is very aware of this constraint. Urgent Twitter messages with targeting information have multiple times been sent from Syria, calling for CENTCOM to initiate bombing missions against Islamic State units and installations outside, e.g., the Kurdish town of Kobane. Using @Centcom, #Kobane and #USHearKobane, Kurdish fighters have tried to get CENTCOM's attention and provide targeting information and data.[126] At a much more practical level, also as seen in, e.g., Syria, information from social network media has been used by various actors to target individuals posting information on their accounts and to single out accounts and profiles for computer network attacks or hacking. The latter is possibly also the case regarding the group "CyberCaliphate's" hacking of CENTCOM's Twitter and YouTube accounts in January 2015, supposedly on behalf of the Islamic State.[127]

Intelligence

Online and offline worlds are coalescing and subversive threats are converging in ungoverned spaces, such as cyber-space. Achieving situational awareness therefore requires looking at both spheres in order to understand what is going on – one of the spheres alone is not enough.[128] Intelligence gathering, obtaining and maintaining situational awareness and understanding through social network media is hence increasingly referred to as "Social Media Intelligence", or SOCMINT. The term's justification is debatable, as it rather represents a mix of Signals Intelligence (SIGINT) and Open Source Intelligence (OSINT), with elements of Computer

Network Exploitation (CNE) and Computer Network Attack (CNA), than it constitutes a specific category in itself. Nonetheless, it is a question of seeking to map out social relationships between persons, personas and networks, and figuring out how they influence or are influenced by politics, economy and society.[129] Online social networks can, if systematically studied, reveal broader societal cleavages that exist within and across a country and mapping these can reveal configurations of the political field previously not known that, in turn, can lead to alternative segmentation (division into target audiences) based on social network media connections (follow, mention, re-tweet, etc.); a segmentation and insight that subsequently can be used in the targeting process.

One of the most discussed techniques is crowdsourcing. This could involve creating a network of bloggers to crowd-source information about ongoing events.[130] Or creating pages like the US site: 'citizen global',[131] where people in specific areas of the world can upload and thereby document whatever is on their mind through text, images, videos etc. The material can then be used for selecting stories to push in mainstream media, such as radio, or on the web, in order to influence audiences in the area based on relevant information to which they can relate.

The use of Twitter to crowd-source technical intelligence on weapon systems (such as the Libya example) is becoming increasingly widespread. Also crowd-sourcing information from followers (supportive audiences) that scrutinize the opposition's social network media accounts and platforms in order to find false information and doctored imagery to support counter-propaganda (defensive) activities is also seen more and more.[132] One example of this is that the IDF constantly try to remain aware by monitoring the web sites and the different platforms (social network media) of relevant actors to make sure that rumours are immediately discovered and mitigated before they go viral.[133] In other words, the use of social network media monitoring for early warning purposes. Crowd-sourcing is also being used for collecting simple information on opponents' social network media presence from one's followers, as it has been seen in Syria where, e.g., the Syrian Electronic Army (SEA) have had detailed instructions on their Facebook page dealing with how to report opposition Facebook pages.[134]

Internet (live streamed news reports on web-TV) and social network media (e.g., Journalists tweeting from crisis areas) is also being used by non-state actors without sophisticated Intelligence Surveillance and Recognisance

(ISR) assets to conduct Bomb Damage Assessment (BDA) of, e.g., their rocket attacks. Apparently done by both Hamas in the Gaza strip and Hezbollah in Lebanon, to assess the impact of rockets fired into Israel. This can furthermore be supported by the use of open source software and applications such as Google Earth, for plotting the locations of impacts.[135] But more sophisticated actors like NATO have also used social network media information as a supplement to other ways of conducting BDA in Libya. In Syria it has been used as a way to verify, at least partially, other social network media reports of collateral damage, where no other sources are available.

Psychological Warfare

PsyWar is probably the most widespread way of creating effects in and through social network media in contemporary conflicts, and is conducted by virtually all actors. PsyWar in and through social network media is aimed at the cognitive domain and is heavily based on human factors analysis (HFA) and target audience analysis (TAA). It is basically aimed at maintaining the support of the loyal, convincing the uncommitted and undermining the opposition. This is achieved through influencing people's perception of what goes on and, in turn, affect their online and offline behaviour by playing on emotional and logical arguments drawn from existing conversations, history and by tapping into existing narratives. This can be done by informing audiences about facts, but it can also be a question of exposing the opposition's wrongdoings or embarrassing actions, influencing by providing specifically chosen words and images (where the release is synchronized in time and space with other activities) and by giving out misleading or false information and even through deception.

Firstly, looking at how social network media are used to "expose" opponents' wrongdoings or to embarrass them. Non-Governmental Organisations (NGOs) and Human Rights movements, but also groupings that wish to de-legitimise a regime, have for example used "Geo-Bombing" to expose a regime's wrongdoings. This means that they have added imagery of human rights violations and testimony on YouTube and linked them with Google Earth and Google Maps.[136] It is also seen that information stemming from hacking mobile phones, Facebook accounts, Skype conversations and e-mails have been leaked to the media, or onto other social network media sites, in the hope they will go viral and then either undermine an opponent's credibility or legitimacy, or create a hype (in the media) where perceptions not realities matter when the agenda and news discourses are being set.

The latter is illustrated by the Russian-Ukrainian crisis where both a US diplomat's "Fuck the EU" quote,[137] and a phone conversation between the Estonian Foreign Minister and the EU's Head of External Action Service (EU's Foreign Service) Lady Ashton was recorded and released[138] – allegedly by Russia – in order to undermine the credibility of the EU as an actor in the crisis (first released on Vkontakte, and then pickedup by a Russian television station). A counter-move was made by some Estonians, who allegedly accessed a mobile phone conversation between Russian diplomats in Africa congratulating each other on the success in Crimea. All of these exposures were released on social network media. Whether or not the content is correct, however, is not always that important when it comes to PsyWar utilisation of social network media. Merely influencing the media discourse, and thereby ensuring that a specific story dominates the airwaves for a while, can be an objective in itself in order to divert media attention away from other current issues.

Regime counterattacks on the rebels, or rather the effect of them in the "Twitterverse" and their effect on public opinion through mainstream media (primarily Al-Jazeera) was a turning point in the conflict in Libya in 2011. Would this effect have occurred without social network media – most likely yes - but it would have required mainstream news media's presence in the country, which the regime tried to avoid.[139] As a result, what was tweeted played a large role in informing international news discourses. Similarly, grainy cell phone imagery of Gaddafi's body, videotaped and uploaded in real-time and reaching YouTube within minutes and shortly after international media (Al-Jazeera) had an enormous influence on the decision-making of the remaining parts of the Libyan regime and further resistance collapsed within hours.

Influencing through social network media is probably one of the central issues when it comes to "weaponization" and the techniques to do so are constantly being developed. One such approach to influencing through social network media is *'nudging',* which is about facilitating choices. In their 2008 book "Nudge - Improving Decisions About Health, Wealth and Happiness", Cass Sunstein and Richard Thaler refer to what they call 'choice architects', who organise contexts in which people can make – free - decisions by giving people a 'nudge' that can alter their behaviour.[140] Another new term is "Twiplomacy" referring to politician's use of Twitter to influence and persuade their supporters and potential voters and to talk about "the opposition", but also to break news instead of in traditional news releases.[141]

Much of the key to influencing in social network media is found in "cross-media communication", as described earlier in this monograph, and aim at mobilising audience behaviour.

During the "Arab spring" spill-over from Egypt, due to the connectivity in the region, may in part have mobilized people in Libya. When it comes to mobilizing people, however, social network media can in general be used to unite a fragmented silent majority and help it to find its voice. The purpose can be to build counter-movements to regimes or groups with opposing views by empowering groups and individuals.[142] This can simply be a question of strengthening their self-confidence or to provide "social-proof", in turn, prompting a desired behaviour. As Frank Webster argued in 2003: "the public are no longer mobilized to fight wars as combatants, they are mobilized as spectators – and the character of this mobilization is of the outmost consequence".[143] Many actors are therefore also seen to mislead and misinform in and through social network media, often via proxies, in contemporary conflicts to create this mobilising effect.

During Operation Cast Lead in 2009, both the IDF and Hamas tried to foster impressions of support from the general public for their respective policies and actions, as well as to create a sense of nationalism, which may not have been as extensive as alluded to.[144] Unknown or false attribution of online content (false flag / black operations) can also be a part of this. The IDF's use of students to systematically post favourable commentary on articles and framing comments is one example of this.[145] But also Hamas had people systematically writing positive comments on blogs and news articles online and doctored images or used old photos taken out of context to mislead audiences.[146] This technique is allegedly also widely used by Russia – or Russian sympathizers – in Ukraine the Baltic state's news outlets online. The latter is known as "Trolling", referring to online trolls whose only purpose is to spam negative or critical news articles or social media posts and updates with comments.[147]

Another way to mislead in social network media is to flood social network media with tweets containing favourable content from credible sources and thereby amplifying its effect by constantly re-tweeting the content in multiple languages (dependent on the strategic audiences), with different looking links and hashtags, in effect dominating the conversation.[148] This technique will create the impression of many people having the same opinion or attitude in order to create legitimacy for a specific point of view.

This can technically be done through, e.g., "botnets"[20] or "sock puppets".[21] Botnets have been seen in, e.g., Syria where the regime allegedly produced more than 4 million tweets and re-tweets over a four-month period in 2012, before the botnet was brought to Twitter's attention and subsequently shut down.[149] The content was pre-dominantly tweets from pro-regime news outlets in order to draw attention to them while at the same time provide plausible deniability for the regime (hence the problem of attribution of online activity). The other example, sock puppets, is where one person can control many (in the hundreds) separate identities, using fake online personas, based all over the world to create a false consensus in online conversations, crowd and smother undesired commentary that does not support own objectives. It can also be used to respond to emerging online conversations with any number of coordinated messages, blog-posts, chat-room posts or other updates.[150] It, like botnets, involves false geo-locations and attribution to create credibility. Misleading or misinforming activities in social network media is, albeit, very close to actual deception.

The Taleban in Afghanistan have several time tried to deceive Australian and other ISAF[151] forces by trying to become friends with them on Facebook in order to gather information about operations, names, ranges, locations, etc. The Facebook accounts were apparently all owned by western-looking very attractive young women.[152] This has also been seen in the Middle East where actors, possibly Hezbollah or Hamas, have set up fake Facebook accounts impersonating young attractive Jewish girls in the attempt to get Israeli soldiers to give information of military value. The same methodology has been seen in Syria where Facebook accounts have appeared to belong to

(20) "A botnet is a collection of computers, connected to the internet, that interact to accomplish some distributed task. Although such a collection of computers can be used for useful and constructive applications, the term botnet typically refers to such a system designed and used for illegal purposes. Such systems are composed of compromised machines that are assimilated without their owner's knowledge. The compromised machines are referred to as drones or zombies, the malicious software running on them as 'bot.'"
(source: https://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets)

(21) A sock puppet, in the context of online communications, is a fake identity created to promote someone or something through blogs, wikis, forums or social networking sites such as Facebook or Twitter. Sock puppets are often created to improve the status of some entity or to promote a particular viewpoint that is expected to be helpful to that entity. Fake identities are created to circumvent site bans, increase product sales, improve or tarnish reputations, spread disinformation and stifle dissent, or to artificially stimulate demand for a product or service is known as sock puppet marketing. (source: http://whatis.techtarget.com/definition/sock-puppet)

human rights organisations offering news about the humanitarian situation but when logging onto the site using Facebook one's username and password has been "pinched" and potentially used for either intelligence or targeting purposes or for distributing propaganda to your social network using your Facebook account.

Lastly an example of the use of social network media for creating PsyWar effects could be deterrence. This can be a question of targeting individuals through social network media, seeking to expose accounts and intimidate the owners into silence either on- or offline.[153] This could take the shape of either a cyber-attack defacement of their social network media profile or account by replacing the original content with threating messages or through simply posting these messages on own profiles and accounts and use links or other means to make the audience or target aware of it.

Cyber-Operations

Operations, mostly in the form of various forms of hacking, aimed at social network media accounts, platforms, systems and networks and the information residing on these are often tactical actions with strategic aims. This can include computer network activities directed at social network media in support of tactical operations on the ground. Through, e.g., targeted attacks on Twitter accounts and Facebook profiles used real-time by a terror-organisation during a terror-attack, like the ones in India (Mumbai) and Kenya (Nairobi), in order to prevent the terrorists from communicating their actions to the outside world, while police or special forces conduct direct action attacks against them.

Attempting to manage or shape perceptions through trying to control what is available online and what is not can serve as another example of "operations" directed at social network media. The Russian-Georgian war in 2008 started on 7 August, but computer network attacks on social network media started already on 27 July, or 10 days before the conventional military confrontation between Russian and Georgian forces started. Although not verifiably attributed to Russia or an agent of the state of Russia, it has often been claimed that Russia was behind the attacks. The shaping activities consisted of DDOS attacks, defacing and distribution of malicious software. The desired effects seemed to be aimed at creating confusion and hampering the Georgian governments command and control and especially its ability to disseminate crisis management information to the Georgian public.

Operations directed at social network media have also created even more tangible offline effects. One example of this is SEA's computer network attack on the news company AP's Twitter account, releasing a false tweet claiming the White House had been bombed and that the US president was injured. This one tweet resulted in a US$ 1,365 billion dip on the S&P 500 index within minutes.[154] This effect was not sustainable, however, and the market was quickly restored when it became apparent that the information was false.

Operationally, social network media also afford some new and unique opportunities for "Unconventional Warfare" (UW), or what is called "Military Assistance" (MA). The US Special Operations Command (SOCOM) defines UW in the following manner: "Unconventional Warfare consists of activities conducted to enable a resistance movement or insurgency to coerce, disrupt or overthrow an occupying power or government by operating through or with an underground, auxiliary and guerrilla force in a denied area".[155] Basically, unconventional warfare, increasingly also linked to what is called Hybrid Warfare,[22] is about supporting an uprising or rebel group. In this context, instead of having Special Operations Forces on the ground depriving an actor of plausible deniability of any involvement, an actor can now support a rebel group or the like with intelligence, training, targeting information, and facilitate both offensive and defensive activities and support, including command and control capacity, through activities in and through social network media. This can also include out of area training and mentoring them in this use and the provision of specified software. Short of actual weapons training and mentoring on ground, a state, or for that matter a non-state actor, can deliver intelligence and online solutions like cloud-solutions and protection software and thereby achieve many of the same objectives and effects as normal unconventional warfare or military assistance, but with much fewer physical and not least political and legal risks.

(22) Hybrid Warfare: Hybrid warfare is a military strategy that blends conventional warfare, irregular warfare and cyber warfare and information warfare. This approach to conflicts is a potent, complex variation of warfare. Hybrid warfare can also be used to describe the flexible and complex dynamics of the battle-space requiring a highly adaptable and resilient response as any enemy that uses simultaneous and adaptive employment of a complex combination of conventional weapons, irregular warfare, terrorism and criminal activity in the battle-space to achieve political objectives. (source: based on http://en.wikipedia.org/wiki/Hybrid_warfare (accessed 26 SEP 14). Furthermore, many of the activities conducted stay under the threshold of what can be defined as war.

In connection with Unconventional Warfare activities, the delivery of anti-censorship and censorship circumvention tools to rebels or opposition parties becomes more and more prevalent. Especially when "open-internet" policies fail, the US will use own capabilities to penetrate firewalls and censorship tools to go around restrictions in repressive countries in order to facilitate access to social network media.[156]

Social network media also help creating conditions for other activities, such as Public Diplomacy (PD), in order to tap into existing conversations on platforms already used by local audiences. Platforms which can be very different form the ones normally used in western countries.

Operations can also be a question of attempting to hamper other actors' ability to use social network media for their "war-fighting" purposes by conducting operations against an opponent's capabilities by, e.g., denying access to accounts and platforms. One example of this from Syria is where SEA, by attacking opposition groups' area-specific Facebook accounts, tried to deny the opposition the possibility of reporting news about on-going events on the ground to outside observers.[157] Denying and completely shutting down internet access, despite of all the challenges associated with this, seems to be oppressive regimes' favourite method for defending themselves (for more on this, see discussion in chapter six on the "dictator's dilemma").

Defence

As discussed above, a part of unconventional warfare, or the "military" use of social network media in general, can also be to use or provide encryption and circumvention systems, tools and software in order to avoid detection, monitoring and tracking and thereby avoid potential physical repercussions. Lack of appreciation of "operational security" (OPSEC), and lack of awareness about basic cyber-security have cost many rebels, in particularly in Syria, their lives.[158] In contemporary conflicts, nearly everybody has access to and uses social network media for many different purposes. This includes troop contributing nations to international missions, their soldiers and families and news media as well as the warring factions, local populations and third parties to include non-state actors and activists. This use of social network media results in that OPSEC and other defensive issues are of growing concern. Amongst these concerns is, of course, hostile intelligence collection and online deception (e.g., fake profiles, false content attribution and pinching of identity information).

Deception-detection is, based on the tools and techniques described above, therefore a very challenging issue for all actors. As discussed earlier, the use of botnets and sock puppets and different ways of hiding your true identity online makes it very difficult to detect and attribute false messaging in social network media. This has also led to numerous government and academic studies into how to detect deception on platforms such as Twitter.

One study looking into this issue was conducted at Georgia Tech's School of Public Policy, and it found that there are four characteristic online behaviours of Twitter "hyper-advocates", such as, e.g., the Islamic State's "disseminators". Firstly, they are sending high numbers of tweets over short time periods. Secondly they are re-tweeting while themselves publishing little original content. Thirdly, they are quickly re-tweeting other's content, and fourthly they are coordinating with other, seemingly unrelated, accounts to duplicate, or near-duplicate, messages on the same topic simultaneously.[159]

Another study made by the Canadian SecDev Group points to another set of indicators concerning online deception that show that shortened URLs in tweets appear differently but lead to the same URL (e.g., a specific news story or press-release). There is also little interaction with other Twitter accounts; all posted links refer to the same two or three news outlets and the central account do not follow other accounts. The relaying (re-tweeting) accounts follow most of the same accounts, having the same tweeting and re-tweeting behaviour over a 24-hour period and generating thousands of hash-tags (#) based on the same three letters.[160]

Also the US Department of Defense research institute DARPA (Defence Advanced Research Projects Agency) has a programme called "Social Media in Strategic Communication", which looks at, e.g., detection of deception and misinformation in social network media.[161]

All three studies suggest, however, that examining online behaviour is more important than content when detecting deception. Besides this, the identification of clusters of "users", that has the same or similar political "ideologies", whose aim is to create an "echo chamber" to increase perceived legitimacy of an actor or other source and amplify some issues and minimise others, also is a way of identifying online deception.

One thing, however, is the personal risks to users of mobile devices and social network media in relation to conflicts, such as being identified and

targeted, for example, and the risk of being deceived online. Another thing is the OPSEC-concern when it comes to own troop-movements and the risk of plans and intentions being compromised. During the recent IDF Operation Pillar of Defence (summer of 2014), the IDF encouraged Israeli citizens not to post information and images of IDF movements on social network media so as to prevent Hamas from collecting intelligence and obtaining early warning about where and when the IDF was going to operate. The IDF was, of course, worried that citizens inadvertently would reveal possible targets to Hamas. The IDF also asked people not to post on social network media where and with which effect Hamas rockets landed in Israel, so as not to give Hamas confirmation and measures of effectiveness (Bomb Damage Assessment). The IDF's information campaign on own citizen's online behaviour could very well be compared with World War II's "Loose Lips Sink Ships" information campaigns conducted by the Allies.

The awareness of one's own population of the risks they might pose to own troops by inadvertently revealing information about their movements is one thing; another is the OPSEC challenge associated with operating in foreign countries where there is less incentive to act favourably toward the military force. Here Sir Rupert Smith's analogy, which we discussed in chapter two regarding a "theatre of operations" as a theatrical theatre and the population as the audience or spectators, comes into play. Regardless of how tight security might be around the planning and preparation of a operation, it might, in the current global information environment, very well be exposed at a very early stage of the execution of this operation, due to persons on the ground coincidentally witnessing the movements and posting them on social network media. This is a threat both to troop movements and concealment, revealing which types of units are present in a theatre of operations. The latter was the case with the identification of Russian special forces (Spetsnaz) in the Eastern parts of Ukraine, which was based on both soldiers' own postings on social network media and locals' photos of them, which were subsequently uploaded with hashtags, making them easy to find for outsiders seeking information about the situation in the area. This could also have been the case for the US NAVY SEAL team tasked with raiding Osama bin Laden's compound in Pakistan. Their movements, or rather the noise from their helicopters, were discovered and live-tweeted by a local citizen. Although he at the time was unaware about the exact nature of what he was witnessing, it is not unthinkable that someone able to warn the residents in the compound was following his tweets; especially if he was hash-tagging them with something that would

identify the geographical location of what was going on. Today, actors aiming at obtaining and maintaining situational awareness through social network media would monitor both geographically and issue related (e.g. hashtags etc.) posts in order to gain early warning as a part of OPSEC and counter-intelligence activities. These appreciations must therefore be a part of all operational planning, both in respect to intelligence collection and in respect to mitigating OPSEC risks that stem from social network media.

If one's operation is compromised on social network media, it is also plausible that that someone would have used social network media to communicate this and coordinate further actions; or, in other words, use social network media for command and control.

Command and Control

Social network media have for long been used by terror-organisations for communicating and coordinating efforts and thereby for command and control purposes. It has, however, emerged in a much more systematic form in Syria, where remote command and control nodes played a large, practical coordination and logistical role.

An example of this utilisation of social network media is the Mumbai terrorists that had a "control room" in Karachi where social network media, among other media, such as mobile devices, was used to coordinate the actions of the terrorists, partly based on feed-back gained through the monitoring of mainstream news coverage of the terror-attack, and partly based on conversations about the event in social network media. Similarly, in the conflict in Libya, Twitter was used to coordinate information, medical requirements, radio frequencies and telephone numbers along with new satellite frequencies for TV stations that were being jammed. These are all examples of social network media being used for command and control purposes.[162]

More traditional social network media has also been used for synchronizing and coordinating the "combat power" of dispersed non-state actors, facilitating a unified uprising, as seen in Libya and in connection with the organisation of demonstrations in Iran and Egypt. This degree of coordination and connectivity used to be exclusive to state armies with sophisticated Communication and Information Systems (CIS) equipment. Now non-state actors can use social network media, combined with special yet still accessible software, to acquire the same capability. Modern armies

are now also using social network media-like platforms for command and control purposes, although often on closed or secured networks in the form of chat-room and messenger functions embedded in military CIS in order to improve agility.[163] Social network media hereby helps level some of the asymmetry between state and non-state actors, at least on the C2 front.

This type of "open" – social network media based - command and control arrangements furthermore makes it difficult for conventional armed forces to attack C2 networks of non-state actors, as there are no centralised networks, nodes or physical targets to attack. An attack would also be associated with a variety of legal issues, as the infrastructure and platforms basically are civilian. With respect to the legal issues it could be argued that if used for "military" purposes, social network media becomes dual-purpose technology.

Social network media used for command and control can also be a question of enabling the use of "swarming"[164] tactics through publishing or informing, mobilizing and coordinating otherwise dispersed non-state actors' behaviour towards a specific target in time and space, even though they are not under the command of one single entity. They might just have a common interest. Due to the very short time available social network media leaves little to no warning time for, e.g., government security forces to respond to such an event. Remote command and control nodes therefore effectively create a digital or virtual "hinterland" for non-state actors, wherefrom they can crowd-source information and coordinate swarming of "targets of opportunity", as well as coordinate with other actors. Examples of the latter could be NATO and rebel communication in the Libya case, as discussed earlier. On the other hand, potential participants in a demonstration or a riot cannot know, due to time constraints on attribution verification that the ones calling for a demonstration are really whom they claim to be. Allegedly, Iranian authorities have used this technique too, by using social network media to organise a protest demonstration. However, when people showed up they were met by riot police and security agents.

The use of social network media for operational purposes, within all six distinct activity areas is, however, associated with a series of opportunities as well as with some limitations and inherent risks.

LIMITATIONS AND RISKS

All though social network media presents a series of opportunities for creating "military" effects for state as well as non-state actors, there are at the same time certain limitations and risks associated with the operational use of social network media. The use of social network media for intelligence purposes can, for instance, only be a supplement to other intelligence collection activities. Likewise, it is associated with a series of legal challenges. Due to the massive amounts of data exchanged on social network media, it is probably not possible to monitor, track and map all connections, content and behaviour within a network. Hence, even though supported by analysis software, intelligence collection through social network media, like other intelligence collection assets, must be focused on specific topics (prioritised intelligence requirements), and targeted on areas or individuals / profile-accounts. Although the risk is only to portray a fragment of the totality of the traffic in a network. Due to the sheer volume of traffic online, the actor collecting information through social network media will also likely be limited by resources. The overall utility of information gathered through social network media is also affected by the speed of which things develop online versus the speed with which the information can be analysed, verified and utilised in operational planning or for, e.g., targeting.[23] Another limitation in this context is the analysis of the peculiarities of social media content like abbreviations, slang and idiosyncratic dialects that are commonly used.

Besides the organisational and technological limitations and risks that are associated with the use of social network media for operational purposes, some things stand out in particular. Importantly, online behaviour and content can be false and subject to deception and manipulation in multiple ways. Many actors, especially in conflict areas, desire to be anonymous or impersonate as someone else, e.g., to spread propaganda and misinformation or for the purpose of deception. This can, however, also be attributed to operational security reasons for personal protection.

(23) At the same time, there are certain limitations which social media analysts should be aware of. Concerning the provision of real-time information, the British journalist Nik Gowing talks about a tyranny of real time and a so-called F3 dilemma: "You can be First, you can be Fast. But in entering the race for the information space how Flawed – how mistaken and inaccurate – might you be?" To react on real-time data means taking a risk at being wrong or too hasty. (Source: Gowing, Nik: 'Skyful of Lies and Black Swans. The new tyranny of shifting information power in crises'. In RISJ CHALLENGES, 2009, page30.)

The content can also simply contain wrong information, either on purpose or because the content has mutated and is now misrepresenting the original content through being used in user-generated content in different ways. Furthermore there is a risk that parts of one's intelligence collection plan (ICP)[165] can be compromised and what you are looking for (intelligence requirements) and why (intentions and plans) can be revealed to opponents or third parties. This is particularly the case with crowd sourcing. Security protocols and operational security must therefore be applied, even though the collection of information from social network media is predominantly open source intelligence (OSINT). Also due to the risk of being subject to online deception, manipulation of information (written content, pictures, and video) and impersonation (source attribution) the verification of information gathered is imperative. On the other hand, some of this verification can come from analysing large quantities of image data from the same area. If hundreds of pictures and video from a particular place or incident exist, it is harder to manipulate. Also the use of software to reveal to which extent a picture has been used elsewhere and is now used in a wrong context can assist in this. There are many examples of pictures from other conflicts being used in current conflicts out of context. E.g., Hamas using pictures from Lebanon claiming they are from Gaza, pictures from Iraq being used as proof of war crimes in Syria and pictures from Kosovo are being used by Pro-Russian rebels in Ukraine claiming Ukrainian war crimes. The common denominator is that the pictures are taken from internet sources and used in social network media user generated content.

Regardless of the limitations and risks associated with the use of social network media for operational purposes, however, it is simply a fact that these media and the technology that facilitates them are a part of the contemporary conflict environment. In other words, they have been weaponized!

HOW HAS SOCIAL NETWORK MEDIA BEEN WEAPONIZED

What does it then means to "weaponize" something? By "weaponization" is meant the adaptation (something existent or developed for other purposes) in such a way that it can be used as a weapon (platform / system) in order to achieve "military" effect(s).[166] Such a thing could be a chemical or bacillus that is modified to be used as a weaponized chemical agent (e.g., gas) to produce weapons-grade Uranium for Nuclear weapons, or just dirty bombs, use or adapt existing computer-code to crate military effects in the cyber domain (e.g., Stuxnet), or as in this case use and or modify social network

media algorithms, code and platforms for "war-fighting" purposes. As the cases above demonstrate, then social network media are being used in contemporary conflicts for targeting processes, intelligence gathering, psychological warfare, both offensive and defensive operations as well as for command and control activities.

HOW HAS THIS AFFECTED THE CHARACTER OF CONTEMPORARY CONFLICTS

Social network media has afforded state and non-state actors alike "stand-off" capability for delivery of effect, or in other words a "remote warfare" capability. This development has effectively changed how warfare can be waged and how costly it is. These factors allow a variety of actors (state and non-state) a voice in and an ability to affect the battle-space (which has become global). At the same time, the increasing transparency, speed and the flow of information, challenge the traditional actors' (states and militaries) role in contemporary warfare. This has created new methods of exercising strategic influence (from the distance). These changes sit uncomfortably with oppressive regimes, as well as with traditionally thinking western militaries, because the new information power, brought about by the weaponization of social network media, effectively re-distributes power. Already in 2006, Audrey Kurth Cronin argued that the digital connectivity was changing the process of mass mobilization in warfare, enabling what she calls 'the electronic levee en masse'.

> "A mass networked mobilization that emerges from cyberspace with a direct impact on physical reality. Individually accessible, ordinary networked communications such as personal computers (…) and cell phones are altering the nature of human interaction, thus also affecting the shape and outcome of domestic and international conflict".

Despite having been written in the early days of social network media's use in conflicts, her argument points to a change in the character of conflict brought about by "a democratisation of communications, an increase in public access, a sharp reduction in cost, a growth in frequency, and an explosion of images to construct a mobilizing narrative".[167] To this end, the Canadian SecDev Group in their paper "backgrounder – The Hard Realities of Soft Power – Keeping Syrians Safe in a Wired War" highlights three ways in which the internet and social network media have affected the character of contemporary conflicts.[168] Firstly, that cyberspace is a strategic high ground;

secondly, that it is all about fusing information from two domains to gain and maintain situational awareness to understand the conflict; and thirdly, that strengths and weaknesses online are also strengths and weaknesses offline.

> Cyberspace is a strategic high ground. Access to the internet matters and oppressive regimes need cyberspace to coordinate activities between elements of its security forces and so do rebel groups. All parties to a conflict need to maintain loyalty amongst their supporters to win over the uncommitted and undermine their opponents through propagating their narrative of the war. The internet is therefore also a strategic battle-space where hackers supporting, affiliated to or embedded in all the actors seek effects on other actor's information and information systems. The internet (cyberspace) and in particular social network media is also important to ordinary people living in conflict areas to a degree where the access to information is a resource on level with food, shelter and medical supplies.[169]

> This quote concerns a sort of fusion. Online and offline worlds are coalescing and gaining a situational awareness and understanding requires insight from both worlds and the merging of this information. One side is not sufficient. Relying on traditional Intelligence, Surveillance and Reconnaissance (ISR) assets will only give a part of the picture, as so much of the conflict has now gone viral and because the viral part has an immense impact on the physical world, much will be overlooked and early warning along with understanding of dynamics will be lost by focusing on just one dimension (e.g., the physical one).[170]

> Strengths and weaknesses online are also strengths and weaknesses offline. The distinction between online and offline security is fading. Exposure online can have grave consequences offline. Not only for non-combatants, citizen journalists and non-state actors in a conflict area, but likely also for people supporting these outside a conflict area (remote warfare 'combatants'). Access to opponents' social network accounts and e-mail accounts are today so important for intelligence services that it is a standard issue or question under interrogations, in places such as Syria, to ask to for account names and passwords.[171]

Also David Kilcullen highlights three areas where contemporary conflicts have changed their character, impacting the role of social network media. Conflicts are more urban, technology is changing war and the democratisation of technology is empowering.[172] All three characteristics respectively create conditions that facilitate more power to social network media in the future, as conflicts are likely to be more about local power, money and control [over populations] than about territory. This gives social network media an exponentially larger role than if we were talking about cold war conventional conflict in a less "connected" world.

The latter is often discussed in military circles as something that will cause a return to training for (e.g., the "back to the virtues" dogma). The next "conventional" war, however, will be fought in a social-network-media-saturated global information environment. In this environment, the conventional commander will find himself exposed to "Social Media ISR", his IP based C2/CIS systems attacked and his units swamped by more or less randomly ad hoc entities mobilized through social network media, while having to constantly consider the political strategic backdrop of his mission. A political backdrop that, in turn, constantly is debated in and informed by conversations in social network media.

The use of social network media has also affected the delineation between military and civilian participation in conflicts and the delineation between domestic and international spheres has become blurred. This has effectively, due to the 'virtual theatre' concept, made everybody potential "virtual combatants". Along with the expanded availability of social network media in conflict areas, also regular people, NGO and other voices are being heard louder than before. They (e.g., citizen journalists) can document the war battle by battle and potentially influence media agendas, political discourses and the public's perception.[173] The latter issue is of particular importance when looking at how the character of conflicts has changed with the introduction of social network media. Media agendas (and not least the media's sources) are to a high degree now informed by social network media, making them a hugely powerful tool. This, however, also presents an unprecedented challenge for the media in terms of source criticism or validation of the attribution and the validity of the information picked up from social network media.

The de facto contemporary use of social network media and how, as discussed above, social network media characteristics and utility in general

fit into the characteristics of contemporary conflicts add up to a significant shift in the way conflicts are likely to be fought in the future. Connectivity has important implications for the practice of war, but it does not substantially alter its nature as much as is commonly supposed.[174] The character has, however, changed. Albeit, it is not a 'game-changer'[175] if one looks at the "conventional war" paradigm. It has not changed much between states, but it changes relations amongst non-state actors and between states and non-state actors in a rather significant way.[176] The largest change is in the external actor's access to delivering effects on the (global) virtual battlefield. Internal actors (at even the lowest levels) now have the ability to influence public opinion[24] in countries contributing to conflict resolution (or the opposite), based on the notion of the criticality of public opinion in "war of choice" is another significant change.

What makes it difficult to measure just how much social network media is actually affecting the character of conflicts today is also what has made the debate about their effects subject to critique. One has to look at the accumulated effect of the use of social network media in conflicts in support of political and or military objectives - not the single major social network media driven events that "turn the tide of war". Activities in social network media can create decisive conditions (DC)[25], in the end they are not, however, likely to be decisive overall. Nonetheless, they will most likely be a significant element in future conflicts, not least as an element in a "Hybrid Warfare" strategy, which is why no actor in future conflicts can disregard social network media, and must have capabilities to engage in this sphere as well.

Nor is social network media equally effective in every scenario. Its effect is dependent on time, space, human knowhow, and, to some extent, communications infrastructure and the intensity of the conflict. In pre-conflict scenarios, the potential impact is highest through influencing perceptions, informing decision-making and mobilizing internal and external support. There seems to exist a "window of opportunity" for using

(24) Either directly through social network media or via social network media through mainstream press coverage of its content or mere use.

(25) Decisive Condition = "A combination of circumstances, effects, or a specific key event, critical factor, or function that when realised allows commanders to gain a marked advantage over an opponent or contribute materially to achieving an operational objective". (Source: NATO Allied Joint Publication (AJP) 01 (D), 2010, page 5A-2).

social network media most effectively when the conflict is still latent or in its very early stages. In this time-frame many audiences are impressionable (see 'sense-making' in chapter two) and have not yet seriously started to question attribution and content in any major way. The higher the intensity of the fighting, and the more attention there is on the 'propaganda' part of the war, the lower the direct effect in the physical battle-space (on-ground) social network media will have in terms of influence and deception. They can, however, still play a significant role when it comes to "operations" and command and control. In terms of influence and deception, social network media will, however, have a very high worldwide impact, particularly on media agendas and political discourse. State actors will likely also in the future strategically plan on how social network media can be used, both directly and indirectly, to support diplomatic activity and political negotiations in connection with conflicts.

The fight – or war – does not end either! Mainstream media's attention fades away and is sometimes gone when a conflict comes to an end (or another conflict gets the news media's attention), but in the social network media sphere the conflict is likely to continue after the fighting ends and continues as a "social netwar" over the conflict's legacy,[177] or in other words the post-conflict narrative, that as discussed in chapter three will be open-ended and potentially impact future not yet conceived of or anticipated operations and conflicts.

INTERIM CONCLUSION

War is nothing if not a constant process of adaptation.[178] Social network media is a part of the information and communication technology development that, in turn, affects the character of contemporary conflicts. The way that contemporary conflicts are described (see chapter two) and the characteristics of them fit very well together with the opportunities that the characteristics of social network media afford. These two factors together make social network media a very powerful tool in contemporary conflicts – in concert with more traditional instruments of power, potentially employed in a "hybrid" way!

Over the course of more than 15 years, from Operation Allied Force in Serbia and Montenegro over the conflicts in Iraq, Afghanistan, Libya to present-day Syria and Ukraine, social network media has become ever more pervasive. One observable tendency is that the emergence of social network media has given all actors and stakeholders, as well as apparently irrelevant third

parties, a much more direct access to the target audiences, whose perception and behaviour they desire to influence. Actors are no longer dependent on traditional media-outlets to reach the target audiences. Social network media are, however, not just another media platform that can be used to disseminate information (messages and images)! They are also interactive, can facilitate dialogue, and content can be re-distributed. Content can also be altered by the users and new contexts can emerge through user generated content, which again can inform how a conflict is perceived by various actors and stakeholders leading to behavioural change. There is also a tendency for the traditional news media to lose access to conflict areas rendering social network media even more important as sources of information. Mechanisms that actors using social network media in contemporary conflicts seem to be very aware of and exploit strategically.

Changed conditions under which contemporary wars and conflicts are conducted; enhanced digital connectivity, democratisation of technology, urbanization and tech-savvy populations have also led to the emergence of "virtual theatres". Non-state actors can conduct "remote warfare", or "social netwar", creating effects that were not previously possible. All parties in the Syrian civil-war, for example, exploit cyber-space to further their goals.[179] As Pollock highlights, the ways in which social network media and online tools began to fulfil practical military functions in Libya, to include the use of, e.g., Twitter to crowd-source weapon-technical intelligence from international supporters, including from hacktivists, is a new way of creating effects. Effectively creating new notions of what symmetry and asymmetry is, social network media platforms can help even out the playing field.[180]

The tendency is that both cross-media communication planning and traditional media and online and offline activities are coordinated in time and space and what appears to be information from lots of different sources can very well be an orchestrated campaign. Primarily due to the possibilities that technology and media convergence afford, virtual networks of international support (Libya and Syria) represented a complete logistical, informational and command-and-control hinterland for the uprisings, providing instant strategic depth as the movements gathered momentum.[181] And each opposition "battalion" in Syria now has its own online presence on social network media.[182] The IDF and others would now not dream of planning an operation without integrating social network media and mobile technology, and most recently Russia's strategies and operations in Ukraine supports this tendency.

Social network media is therefore now not just a question of having new, technologically provided ways of communicating and excreting influence. They are weapon-systems in their own right, providing actors, state and non-state alike, new intelligence, targeting, influence, operations and command and control capabilities. These new capabilities, however, also comes with challenges; not least politically, legally and ethically!

CHAPTER 6

PERSPECTIVES

"You may be my creator, but I am your master"

Merry Shelly (Frankenstein)

Having examined which "military" effects can feasibly be created in and through social network media and how we and others have worked to create such effects in contemporary conflicts, it is also necessary to look at the broader political, cultural, ethical and legal effects of the weaponization of social media.

Although perspectives differ depending on whether a state or non-state actor or a liberal democracy or an authoritarian regime is in question, actors using social network media are faced with, at times hard, choices. Most of these choices are political and, in turn, also ethical. In the absence of a clear legal basis for using social network media for "military" purposes, one of these, inescapable, choices is linked to trying to mitigate opponents' use of social network media – should opponents have access cut off or be engaged?

THE DICTATOR'S DILEMMA

Oppressive regimes are often challenged by rebels and political activist's ability to use the internet, and particularly social network media, and therefore try to deny them access through various means. Regime reactions to this is nearly by default to either ban or close down internet access and or access to specific social network media platforms. This tendency has been seen in nearly all contemporary conflict areas and throughout the "Arab spring" with varying degrees of success. In Tunisia, after having failed to block Facebook and other social network media, due to online protests, the regime instead set up false "pinching sites" that mimicked Facebook and drew dissident users to reveal their logon details (user name and password) so they could be tracked and monitored.[183] Something that also have been used extensively in Syria.

Quickly though, when regimes try to censor or block information about uprisings from getting out to the outside world via social network media,

virtual activist groups (like Anonymous, WikiLeaks, The Open Net Initiative or anti-secrecy sites like Cryptome) will often provide support from abroad.[184] They do this either by providing connectivity or to find ways to enable or facilitate online collaboration amongst people on the ground in the affected area. Not unlike some government sponsored projects, like western "non-violent support" initiatives to support Syrian opposition groups with social network media enabled command and control capability.

The internet in Syria has been disabled several times during the civil war. The Syrian regime has claimed either that the opposition (or terrorists) did it or that the breakdown was caused by technical problems. Conversely, the opposition have continuously claimed that it is the regime that deliberately has shut down access to the internet. Why the regime would have done so is debatable, however. That the opposition should have been able to do it is highly unlikely taking into account the highly centralised way the internet is configured in Syria. To a degree, the regime itself is also dependent on the internet for command and control purposes and for intelligence gathering. This suggests that the regime either needed time to install detection and tracking software, or that there has been an attempt to prompt the opposition to use other communication means for specific periods of time, which have been easier for the regime to monitor. In other instances, it has been seen that the regime has disabled the internet in areas where attacks on opposition units have been imminent in order to prevent communication to the outside world and to coordinate actions between the opposition groups.[185]

In general, though, it remains a dilemma for regimes whether to block or ban internet access, even only to specific sites, as the regime provides people, who in other ways are not involved in the uprising, with a personal grievance and motivation for them to also protest. So actions designed to hamper protest organisation and coordination via social network media and mobile technology (e.g., SMS) can very well backfire.[186]

Oppressive regimes have therefore been looking for alternative approaches to dealing with these challenges. One such approach is to set up special entities, official or non-official, to "engage" with online opposition, such as the Egyptian "Electronic Army", which was set up as a counter to rebel or demonstrators' use of social network media in order to push out pro-regime messages and coordinate counter-demonstrations.[187] This approach was taken a step further in Syria, where Al-Assad, allegedly supported by Iranian

specialists, created the Syrian Electronic Army (SEA)[26] in order to collect intelligence but also to harass activists, hack opposition websites and social network media accounts and spread propaganda and misinformation.[188] The SEA's actions include trying to counter the dissemination of censorship circumvention tools by blocking Virtual Private Networks (PVNs), and the sites from where they can be downloaded, in order to prevent the opposition from using this technique to bypass censorship. This shows that the use of social network media represents a threat, at the very least a perceived one, to the regime.[189] Syrian awareness of this aspect of the conflict has led to an increase in their "cyber warfare" efforts, particularly efforts directed at social network media.[190]

It is, however, not only in actual crisis areas that social network media is being limited due to its political effect (e.g., the ability to create effects like exposing, influencing and mobilizing). In late March 2014, although not a conflict situation, some of the dynamics of "the dictators dilemma" became clear when Turkey, after several times having banned and or blocked access to social network media such as YouTube, and latest Twitter, on 20 March 2014 seemed to change tactics. A week later on 28 March, the Turkish government ordered that all mosques in their Friday sermons should "warn about the dangers of social media" in an attempt to justify and defend the decision.[191] On 3 April, however, the ban on Twitter was overturned by the Supreme Court.[192] This again was contested by the government. The companies behind YouTube and Twitter naturally contested it as well, for economic reasons among others. This case, among other things, shows just

(26) The Syrian Electronic Army (SEA) is just one of many groupings conducting "cyber-activities" on behalf of or in support of the regime or the different opposition groupings. SEA was created in early 2011 to fight a cyber-war on behalf of the regime. It does, however, claim to be independent. The SEA targets both websites and social network media accounts of opposition groups and interests and of Western and Arab news sources. The SEA has also engaged in Computer Network Attack (CNA) to include defacing and DDOS attacks and replacing content with centralized pro-regime messaging.
The SEAs stated mission is to "counter the media and information war against Syria". Another regime grouping is the "Electronic National Defence Force" (ENDF) associated with the regime-loyal para-militant group National Defence Force (NDF). ENDF´s declared mission is "dedicated to crushing the pages of the revolution and their NATO agents/clients".
(Source: SecDev Group (2013c): Flash Note Syria – Syrian Electronic Army Goes on the Offensive, Intensifies Targeting of Opposition Facebook Pages. Published online 4 June 2013. Page 3. www.secdev.com (Accessed 4 APR 14) and SecDev Group (2013f): Flash Note Syria - Syria´s National Defence Forces take the Battle to Cyberspace. Published online 30 September 2013. www.secdev.com (Accessed 4 APR 14)).

how effective social network media are perceived to be, also in countries at peace, at informing the political discourse, and how governments try to manage this challenge, even though it is practically unmanageable with traditional means. The case also shows how the psychological, the economic and the legal spheres merge and become one (hybrid) "battlefield" in, through and over social network media.

An overall structural problem or challenge that faces regimes and governments is that unless you can stop text from being uploaded in the first place and potentially going viral or just being further disseminated via, e.g., SMS or other social network media platforms, stopping it does not really matter. Short of taking steps to taking down an entire network (nation-wide), not just a website or social network media platform, once something is out, it is out, and alternative approaches are needed to address the challenges.[193] Approaches that require political choices.

POLITICAL CHOICES

As the discussion above in "the dictator's dilemma" shows, oppressive regimes and liberal democracies' governments alike are faced with some quite challenging political choices when it comes to handling the effects created in and through social network media. On the one side, they have to assess how much damage that comes from, or the effect of, the "opposition's" use of social network media. In the event that the threat is assessed as sufficiently potent, they need to come up with ways of mitigating the damaging effect(s). Now does this then become a question of closing down access to the internet or parts of it, what is the legal basis for this? And just as importantly, how does this impact the government's legitimacy? And also what are the operational losses? To which extent are the regime or government themselves dependent on the internet to keep civil society running or for maintaining security? If the consequences or negative effects are assessed as being too severe, how does a regime or government then deal with the challenges? Do they intensify monitoring and tracking of internet traffic and social network media use and content, with possible human rights or legal implications, or do they themselves actively engage in the online conversations in order to mitigate the effects and compete with the opposition and their narrative for the "hearts and minds" of the audiences in question, either overtly or covertly? If a covert approach is, at least partially, decided upon, how do they then deal with being exposed by, e.g., an interest group, internet activists or a corporate entity? Regardless of the legality of their actions, an exposure will impact their legitimacy and

reputation. In the end, it is about political choices, with no clear answers, where appreciations over the gains and losses and how it will position the regime or government in relation to other relevant actors, including how to maintain legitimacy, constantly has to be pivotal and constantly re-assessed. Regimes and governments are by far, however, the only entities online having a voice and an ability to create effects and thereby affecting the political choices. Non-state actors (activists, netizens and organisations alike), and to an increasingly high degree also corporate entities, influence regimes and governments choices and public policies in regard to social network media.

Non-state actors

Activist groups, like, e.g., Anonymous, that turn from targeting commercial and political interests to supporting "oppressed" populations and rebel movements against oppressive regimes, are more and more dominating actors in the global information environment, not least in social network media. They themselves might feel that they are on the 'right' side of the conflict, but this judgment is in flux as the perception of who is good and bad might change over time. Although their actions might be favourable to some outside states or other actors' objectives, it is often in no way equal with these activist groups supporting the state or actors' policies towards the specific crisis. The activist group might even actively work against this state or actor at the same time. This dynamic is likely to be even more common in the future and will represent a significant policy and strategic challenge for state actors and international organisations, as such groups are increasingly involved in a contested information battle-space.[194]

But it does not have to be a more or less structured activist group that has a supportive effect on state actors objectives. Self-organising systems and protest campaigns, such as the #NotInMyName campaign against Islamic State on social network media, may emerge, in support of or not, of one's own strategic objectives. With the democratisation of the technology, such "self-organising systems" are most likely also going to be a noticeable part of the future conflict environment as well. They operate (seemingly) spontaneously by using swarming-like tactics, affecting both on- and offline behaviour instigated by virtual leaderless activist groups or individuals. One thing is for sure, though; should they for some reason be in line with one's (i.e., as a government or organisation) strategic objectives, they should not be supported openly. Government (or military) support, or just endorsement, is likely to be the quickest way to kill a self-organising system. They may

not like your opponents and their actions but they do not necessarily like you either or may view endorsement as threating their legitimacy.

On the other hand, if these activist entities are hampering or directly working against your objectives they need to be addressed! What are, however, the political ramifications and secondary effects of taking action against such an entity? And should it be done directly or indirectly and overtly or covertly? This represents yet another challenging political choice for state actors and organisations to make. Non-state actors, however, also comprise corporate interests and entities. They also have their own interests and objectives that can be either in line with or working against regime or government objectives and interests for primarily economic or reputational reasons.

Corporate entities

For-profit-companies or entities and corporate interests are becoming more and more involved in contemporary conflicts, also when it comes to social network media. Either they do so because they are encouraged, being contracted by an actor, or because they do so because it is in their own interest, due to reputational or economic reasons. Just looking at Twitter, they were encouraged to delay an otherwise scheduled software update by the US government as described earlier in connection with the Iranian "Twitter-revolution". Twitter have also, apparently on the corporation's own initiative, facilitated access to their service, as in Egypt with the introduction of "speak2tweet" when the internet was closed down by the Egyptian authorities, and latest, Twitter's own arbitrary action against Islamic State after the Foley beheading videos. The latter with reference to Twitter's "Terms of Service".[195] The terms of service has also been exploited by different actors in order to get Twitter to close down specific accounts. Twitter has furthermore out of consideration for their reputation for, e.g., chosen not to comply with the Turkish government's demands and was subsequently banned from providing services in Turkey.

More broadly, however, corporations behind or operating / hosting social network media will increasingly find themselves in "policy-dilemmas" over their active involvement in conflict situations. Facebook, for instance, which in connection with the uprisings in Egypt, portrayed itself as having helped the demonstrators and facilitated much of the opposition's activities, had to make some hard choices in Syria in regard to having to close down opposition accounts and profiles due to their own terms of service. With their increased involvement, the corporations or companies behind social

network media services continually will have to make choices in order to protect their own business interests (economic, concern for market share, reputation and position or brand identity). It is, however, not only the companies providing the actual social network media service that have to make choices.

The rapid development within information and communication technology and particularly within social network media will likely force most notable state actors and international organisations to contract services in order to maintain monitoring and analysis capability in regard to social network media, as the demands for specific competencies and software will grow with the development. This will become more prevalent as state actors will not have the capacity themselves, and there is therefore also a tendency for state actors to outsource or contract services from "private military companies" or communication consultancies. Social network media is becoming an increasing area of revenue for these companies. They, however, also have to be aware of with whom they sign contracts. In a world where transparency is increasing, particularly due to social network media, they themselves must also think, not only about revenue but also about their reputation, as questionable activities and affiliations can have a blow-back effect not only on the contracting actor but also on the company itself.

Spillover to other conflict areas or issues

Blowback from online "military" activities on social network media is not only a question of political, legal or ethical ramifications for either state, non-state or corporate actors, there is also a serious risk of blowback in other ways. While some western countries and international organisations allegedly have provided "non-lethal assistance", in the form of circumvention and encryption tools, software and training, to the opposition in Syria in order to facilitate, e.g., command and control capability, the Syrian regime has constantly tried to find methods and techniques to thwart these efforts, leading to a new kind of "arms race". Such tools are being made with evermore sophisticated designs, making it near to impossible for even intelligence services to de-code them, but this also means that these tools spill over to Islamists and other groups, which may potentially use them in Europe; in turn, creating a serious challenge to counter-terrorism efforts.

The consequences of the use of social network media in contemporary conflicts are, however, not only a question of "policy" choices and the effect of such choices on political, military or economic issues. More broadly, there

are also some long-term consequences to consider - what is the effect on the post-war environment and society?

Affecting culture?

In the Syrian case, providing or facilitating communication technologies can be important for maintaining relations between people in civil society and communities that may prove vital to Syria's future once the fighting stops.[196] This means trying to maintain some of the fabric that constitutes civil society – if that is still possible! But also history-writing after the war can be heavily influenced by the chronicle of the conflict captured online, which can provide rich insight into the human experience of war, for, e.g., in Syria, despite the scarcity of traditional on-the-ground reporting from news-media.[197] Can future historians, however, trust the apparent "first-hand" sources to the events? Or are they writing a botnet's account of the war? Also, even though the physical war ends at some point, the struggle does not necessarily do so. Mainstream media's attention fades away and is maybe entirely gone when the conflict comes to an end, but in the social network media sphere the conflict continues after the fighting ends and continues as a "social netwar", perhaps maintaining and further deepening the gap between former warring factions.[198] Perhaps characterised as a 'contest of the post-war narratives', as discussed earlier the narrative has no fixed end when it comes to cross-media narratives.

It might be possible to reach strategic audiences in areas where regimes have restricted access to the internet or imposed restrictions or censorship measures through the delivery of circumvention tools and the like or technical solutions as for, e.g., "speak2twitter" are found, but what about where social network media are completely different? The may be based on different algorithms, basic scripting or cultural approach, such as uploading voice messages in clouds instead of text messages on server fixed platforms? Will the introduction of "our" communication approaches, tools and platforms affect the communication-culture in a conflict area after the war? And is that then good or bad? Also as the knowledge of how effective social network media functions in a contemporary battle-space increases, the more ineffective they might become, and at some point their effect for "military" purposes might be de facto neutralised. If people no longer trust the internet, social network media will no longer be able to mobilize people to the same extent or even act as a tool to connect socially! Social network media, although, will most likely retain some effect, as there is still value in the peer-to-peer endorsement of the content. At the end of the day, however,

when the war is over, it is more than likely that the culture of communication has been permanently affected by the way that social network media has been used by all actors during a war. This concerns the way people view and trust these media, the practises in regard to user culture and language, and also which platforms that are being used.

The relatively sterile political and military considerations and choices and the potential spillover on cultural aspects associated with the weaponization of social media, also creates some ethical aspects, which, in turn, can inform the political choices.

ETHICAL CONSIDERATIONS

The weaponization, or perhaps "securitization",[27] of social network media brought about by the way we address them and talk about their role in conflicts, e.g., the normative language used, can create some particular ethical issues. By labelling things as part of cyber war and thereby firmly nesting them within a security regime, instead of as terrorism or plain criminality, you frame the activity as being conducted in a state of emergency, effectively securitising them rendering all responses to be a security, intelligence or defence issues. This discourse can put human rights under pressure. This discourse can very well serve several national security interests but is that really *in* our interest from an ethical point of view?

The fact that security concerns set aside human rights is seen in both closed regimes and liberal democracies. E.g., in Turkey, security considerations are being used as the publicised reason for closing down access to social network media platforms such as Twitter. Other ethical questions also arise from the "military" use of social network media in conflicts. What about, e.g., asking people in conflict areas for information through crowd-sourcing for intelligence purposes? Does that raise ethical concerns? There might also be an ethical concern in regard to facilitating anonymity, e.g., in order

(27) "Securitization, developed by Ole Waever, is probably the most prominent concept of the Copenhagen School, and the one that has generated the most literature. It is argued that 'security' is a speech act with distinct consequences in the context over international politics. By talking security an actor tries to move a topic away from politics and into an area of security concerns, thereby legitimating extraordinary means against the socially constructed threat. The process of securitization is intersubjective, meaning that it is neither a question of an objective threat or a subjective perception of a threat. Instead securitization of a subject depends on an audience accepting the securitization speech act". (Source: http://en.wikipedia.org/wiki/Copenhagen_School_(international_relations) (accessed 26 SEP 14)).

to protect dissidents and other opposition figures versus at the same time promoting attribution of information to ensure transparency and validity.[199]

"Social Netwar" as a term for fighting in a domain using technology and software that is inherently intended for social purposes might also raise ethical questions. Being 'social' is not engaging in war with people, but yet social network media is still increasingly being used for war-fighting purposes, counter to their original purpose. Does this, for instance, make them "dual-purpose" objects and thereby lawful military targets?

Ethical considerations can also cover what non-state actors, e.g., NGOs, are to do with collected information from social network media about actors inside a conflict area. To include privacy issues. And conversely the collection of violent and inflammatory imagery, messaging and information gathered from an area in order to document events, e.g. crimes against humanity and human rights violations, to expose the wrongdoer, can also aggravate the conflict even more, in turn, creating yet another ethical issue.[200]

There are, in turn, of course, also initiatives and programs that look into how the internet can be used for more peaceful things. One of these is Stanford University's 'Peace Innovation Lab', which has a programme on Facebook and peace. As they describe it, "the Persuasive Technology Lab creates insight into how computing products - from websites to mobile phone software - can be designed to influence people in good ways".[201]

Finally, can the effects of several of the "military" activities, whether conducted by a state or non-state actor also have ethical implications? Trying to deny audiences the ability to speak freely on social network media sites and platforms can be ethically problematic, especially for western liberal democracies where the notion of keeping the moral high ground and defending freedom of speech are deeply rooted values. Already in 2011, the human rights organisation Amnesty International in its yearly report (no. 50) pointed out that the struggle of the future pertains to the right to access to information, and that the access to information in itself ought to be view as a human right. Denying people the right to information is also affecting the right to freedom of speech, which in their view is the precondition for other rights. In the report, Amnesty International also points to corporate entities as governments when they write:

> "Digital and communications companies are coming under greater scrutiny as they face governments' demands to comply with patently illegal laws that violate human rights, including the rights to freedom of expression, information and privacy. There is evidence that businesses ostensibly dedicated (and benefiting) from expression and sharing of opinion, including Facebook, Google, Microsoft, Twitter, Vodaphone and Yahoo, are collaborating in some of these violations. (…)
>
> Threats to freedom of expression on the internet being highlighted in the context of human rights revolutions is not new. Amnesty International has long documented the failures of governments, such as those of China, Cuba and Iran to respect freedom of expression and related rights on the internet. Recently introduced laws in the US Congress and in the European Union also threaten internet freedom.
>
> The failure of governments to demand any level of accountability of these corporations and institutions highlights yet again how governments work to support those in power rather than to empower those who are disempowered."[202]

However, besides the political and ethical, and for that matter cultural, perspectives on the weaponization of social media, there are the also legal issues or perspectives. They are also crucial to getting a coherent picture of the issues connected with the developments, although the legal basis for both state and non-state actors' activities in and through social network media is far from clear.

LEGAL ISSUES

There exists a global normative system (International Humanitarian Law - IHL) that divides physical space into a realm of war, where the laws and customs of war apply (Laws of Armed Conflict – LOAC), and a realm of peace, where norms of civil society, domestic law and civil protection apply.[203] Social network media used for "military" purposes challenges this system, as the activities are carried out in both spaces concurrently. This results in a blurring of traditional distinctions between war and peace, government, NGO, individual actors, and the traditional concepts of war and crime and the distinction between what is domestic and international. It has already undermined the spatial conception of war zones; e.g., virtual theatres. This has, in effect, created conflict spaces where actors do not

necessarily have a geographical connection to the physical conflict zone, and where the actors may be located anywhere on the globe.[204] This, for one, challenges the concepts of combatants and non-combatants (international armed conflicts - IAC) in regard to the law of armed conflicts and civilians who participate directly in hostilities (non-international armed conflicts - NIAC). This challenge is to a high degree identical to the challenge one will find in connection with "cyber-warfare", but due to the very low threshold for who can actually act and create effects in and through social network media, the challenge is very much broadened. This also has consequences for how state actors legally can respond to, e.g., third party actors that have an effect on their security or military operations. This includes the challenges in determining what or who is lawful military targets, virtually or physically, assuming that a clear attribution at all can be established in the first place, and that it is possible to discriminate between civilian and military actors. This, however, just highlights some of the most obvious international legal implications of the weaponization of social media. There are of course many more legal questions to appreciate.

Among these are the classical questions of "conflict status" (IAC or NIAC or something else), combatant status (in respect to the individuals conducting the actual activities, e.g. controlling personas online or hacking social network media accounts), classification of the activities (is it use of force or "armed" attack), and is it a "one-off" incident or something that continues (evoking possible right to self-defence)? Also the attribution of these activities and subsequent response options (e.g., is it possible to identify an "agent of state"). And against whom or what can a response be directed, is an interesting question. In such cases, principle questions of what is to be considered "military targets" (in and through social media); to which degree these can fall under "military necessity"; how to ensure "discrimination" and "proportionality" of activities (particularly when it comes to PsyWar and CNA), not to mention avoiding "unnecessary suffering", are important questions as well. Moreover, to what extent is this at all relevant when dealing with social network media? Nevertheless, they are all central legal questions to be appreciated by actors using social network media for "military" purposes.

To these central legal questions, also come more specific questions, such as the "legality of cyber deception" (what are legal ruses, and what is to be considered perfidy in and through social network media?). The international legal issues discussed or listed above are, due to the novelty of the use of

social network media for military purposes, most likely to be discussed or appreciated in connection with each individual case or activity and desired effect that is planned for in and through social network media.

For state actors, however, also a series of additional legal considerations exist in respect to the "military" use of social network media. These include further restraints and constraints to be found in the Rules of Engagement (RoE), national and international (e.g., for NATO) policy and military doctrine, and potentially also in Memoranda of Understanding (MOU), Status of Forces Agreements (SOFA) and Military Technical Agreements (MTA) agreed upon in specific operations.

However, also other legal questions, which are not directly related to either Jus ad Bello or Jus in Bello arise. "Weapons law", such as the "weaponization" of social media as described earlier, involves the use of particular technology for war-fighting purposes. States are required to assess the lawfulness of new weapons before fielding them.[205] States thereby have an obligation to consider whether weapons they plan on developing or acquiring and using are in breach of international humanitarian law. With social network media, this is of course challenging, as there are no provisions in international humanitarian law specifically addressing them. However, as William Boothby writes, "a weapon is an offensive capability that is applied, or that is intended or designed to be applied, to a military object or enemy combatant. A destructive, damaging or injurious effect of the weapon need not result from physical impact as the offensive capability need not be kinetic".[206] With this definition Boothby also implies, although in connection with a broader debate on "cyber-weapons", that social network media, in a "weaponized" form, also can be regarded as weapons and therefore need to be assessed as such under the rules and provisions of international humanitarian law.

As mentioned in the introduction to the legal aspects, much of the use of social network media for "military" purposes are extremely hard to classify in terms of peace and war, civil and military, and criminal activity "boxes". Civil legal aspects in situations where international humanitarian law does not apply therefore also become very relevant. This is the case in instances where a crisis situation exist, but which has not been classified as war or other form of armed conflict, but where activities conducted by multiple actors, in and through social media, clearly have offensive intent, and where individual and likely non-attributable activities remain under the threshold of what can be codified as use of force or attacks. The accumulated effect,

however, of these activities amounts to cohesion. In such cases, besides domestic legislation, different Human Rights conventions, like the European Convention on Human Rights and its article 10 on freedom of expression, would most likely be relevant to consider; e.g., in connection with "the dictators dilemma" and a state's ability to mitigate effects of both foreign states, non-state actors and own citizens activities in and through social media within the country in question. In these cases, also a whole host of civil and criminal law issues arise. These can be tied to media-legislation, marketing-laws, laws on copyright and protection of intellectual property, to mention a few. The discussion of the civil-law aspects of the use of social network media can come across as somewhat of an academic debate, but with the growing tendency for "remote warfare" and "civilian participation" in activities in and through social network media that have effect(s) on the cause of a conflict, they become increasingly relevant. Not least their relevance in connection with "hybrid warfare".

At the end of the day, however, what can be penalized? Close to no legal rulings exists that can answer the questions and without precedence legal appreciations of the legality of the use of social network media must be contextual and made on a case-by-case basis. Some rulings, however, can give some indications. Firstly, the Rwanda case where an editor and two journalists were convicted by the International Criminal Tribunal for Rwanda (ICTR) for incitement to commit genocide through their radio broadcasts. This case can be transferred to social network media and the content publicised on them. Secondly, the International Criminal Tribunal for Yugoslavia (ICTY) and its assessment of the lawfulness of NATO bombing of the Serbian Television tower in Belgrade, and the targeting of information dissemination means, i.e., in this respect social network media platforms and accounts. The two cases are relevant as far as Psychological Warfare content and Computer Network Attack on networks, platforms and accounts is concerned, but at the end of the day, they can only be indications as the circumstances and the technology are very different.

One thing, however, is the above, very briefly discussed "black-letter law" considerations about the weaponization of social media, another is how social media fit into the concept of Legal Warfare or "Lawfare".

Legal warfare

"Lawfare" is a term accredited to the former US Air Force Major General Charles Dunlap. Lawfare according to Dunlap is "the strategy of using, or

misusing, law as a substitute for traditional military means to achieve a war-fighting objective".[207] By this is meant that actors can achieve operational effects, e.g., stopping an offensive or the use of a specific weapons platform, by claiming its illegality and thereby creating international normative pressure that, in turn, will force the opponent to stop this specific behavior. In other instances, it can involve affecting public opinion about an opponent, causing him to lose public support and thereby forcing him to halt operations. To this end, social network media, and the many options for exposing, e.g., wrongdoings or just insinuating them can be used to create effects in the normative sphere.

There is also the question of Lawfare "light", so to speak, when it comes to social network media. Many actors try to exploit corporate policies such as "terms of use" for platforms and sites to achieve operational effects. The SEA, for example, has conducted a concerted "complaint campaign" by regime supporters that aimed at flooding Facebook with complaints about pages requesting them to be taken down.[208] YouTube, for one, will remove content that is in violation of their "Community Guidelines" if flagged to their attention.[209] Facebook will do the same, but ironically enough, as discussed earlier, Facebook used to be proud of its supporting role in the Arab Spring in North Africa, but now repeatedly finds itself in a situation where it has to block opposition Facebook accounts for "terms of use" violations in Syria.[210] It is still an open domain as you can write, comment and share whatever, but within the site's or service's terms of use, drawing the "civil" legal aspects of social network media into the war-fighting effort. Also, the companies themselves behind the social network media platforms, as we have seen in the case study on Islamic State in Iraq and Syria, have arbitrarily begun closing down accounts with reference to their "terms of use".

To mention another aspect of Lawfare, the IDF have started using imagery and video on social network media to document and show how they try to minimise harm to civilians in an area of operation.[211] A sort of online legal defence in advance, effectively shaping public opinion on issues where they expect their opponents will accuse them of breaching international humanitarian law. Conversely, it is also repeatedly seen that various groups (terror groups etc.) actually document their own "war-crimes" on social network media as a part of their propaganda efforts. This has been the case in Syria in general and in particular in connection with Islamic State.

Other legal issues, such as to which extent, e.g., botnets and sock puppets are criminal impersonations,[212] or which rules within intellectual property rights, copyright law, data protection and privacy actually apply when actors generate UGC also exist? In a virtual theatre, where non-state actors are situated in countries in deep peace, other legal issues in regard to social network media's use in conflicts are in need of being addressed. But in these instances, it becomes a matter of exploiting national legislation and not international law to wage Lawfare in, over and through social network media.

The issues above discussed are, however, just some of the political, ethical and legal issues that can be associated with the weaponization of social media. One thing is, however, for sure, and that is that it is a development which will continue as the technology, and the use of it for "military" purposes, develops.

What about the future then? What will that bring? This question is in no way trivial, and as a consequence also very hard to answer. Based on just the last two or three year's developments within the use of social network media for "military" purposes it is nearly an impossible task to predict what the future, virtual social battle-space and its tactics, tools and techniques (TTP) will look like!

PROJECTIONS INTO THE FUTURE

This monograph has predominantly dealt with current operational use of social network media within an "effects framework". Future use, however hard it may be to project, may involve elements such as the integration of "artificial intelligence" (IA), robotics and other technology that we do not currently employ, but whose application, in operational terms, we are only exploring. Also the integration of technologies as facial recognition and voice identification technology, in different ways interlinked with CCTV in urban areas can have future utility in respect to intelligence collection and targeting, perhaps even outside the physical conflict area. For-profit companies, on their own or government encouraged, and other public-private initiatives will most likely be more prominent in future information warfare, particularly when it comes to social network media and broader cyber-operations, alone due to the technology involved (both off-the-shelf and highly customised for specific contexts or tasks). The technology will also to a much higher degree facilitate "remote warfare" and more connectivity will enhance non-state actor's ability to wage social netwar. But

also state actors will most likely be using 'Citizen Global'-like programmes more to generate, through crowd-sourcing or by other future methods, real authentic content prompting further responses and desired behaviour via botnets run by artificial intelligence. Along this comes more developed ways of mining big data, analysing it and exploiting it for intelligence, singling out targets and designing behavioural change.

The mere fact, however, that we talk about these "future" approaches to using social network media for "military" purposes means that the technology is already here; it just has not been employed in large-scale war-fighting yet. What will the future really bring? One thing appears to be sure: social network media will be an integral part of the characteristics of future conflicts. They will not be "stand alone" tools but, due to their pervasiveness, affect outcomes across all the three domains (physical, informational, cognitive) simultaneously. Welcome to "multi-dimensional maneuverers" facilitated by social network media.

INTERIM CONCLUSION

One of the characteristics of contemporary conflicts is the increase in numbers of actors that are willing and able to create effects both on- and offline through cyber-activities, and social network media is an integral part of this. The technological development will also result in new types of actors, besides traditional state and perhaps even non-state actors (understood as, e.g., rebel movements and terror-organisations) such as virtual activist groups and corporate entities that will be direct participants in the conflicts, as we also see it today. This participation in conflicts of multiple actors, along with the possibilities which are created by the information and communication technology development and the democratisation of technology, results in a series of political, ethical and legal challenges, considerations and choices.

Politically, especially state actors are increasingly faced with policy choices that reach into their own nations and not only into "theatres of operations", as some of the "opposing" actors may be their own citizens. This presents governments and organisations alike with ethical dilemmas, including having to balance between creating a discourse facilitating or supporting security agendas (through speech-acts highlighting danger) and on the other side retaining the moral high-ground and upholding normative standards (civil and human rights). These issues are predominantly domestic, though. Looking at the "military" use of social media internationally in conflicts very

little governs this use in terms of international humanitarian law neither in regard to Jus ad Bello nor in regard to Jus in Bello. Nonetheless, social network media are used for war-fighting purposes, which present states and organisations with legal challenges. And not only in a black-letter law sense, but also in a Lawfare sense. Conversely, it seems that non-state actors can completely avoid legal issues over their use of social network media as long as they stay clear of liberal democracies' civil law jurisdiction (sometimes even enjoying its protection) and the social network media provider's terms of use.

And what will the future bring? This is an important question, but also a question that is nearly impossible to answer. The speed in which the technology develops, and the speed in which in particularly non-state actors adapt to it, challenge traditional state military organisations immensely. One thing is sure, though, social network media will be a part of any future conflict environment, and affect it to an even higher degree than it affects the characteristics of the contemporary conflicts.

CHAPTER 7

CONCLUSION

The character of contemporary conflicts is marked by, not being inter-state war, but for most liberal democracies, being "wars of choice", for other actors' uprisings and civil-wars that might even cross state borders. This is the case with the Islamic State in Syria and Iraq. These conflicts are fought amongst people in predominantly urban areas for multiple reasons, by multiple actors and with many strategic audiences or actors, from both inside and outside the geographical conflict area, having an ability to influence the agendas and outcomes. These outcomes are to a high degree informed by the actor's perceptions of what is taking place in a complex and globalised security and conflict environment, which is shaping their behaviour. Furthermore, the ever-developing technology and the use of particularly social network media as an integral part of it have affected the character of war through affording new ways of constructing realities for the actors, audiences and media, which again affect the way actors behave and fight in this reality. To this end, social network media have played a large role, beyond just being another "horse to tank moment". They have also affected the distribution of power in contemporary conflicts due to the effect(s) possible to create in and through social network media, recognising that the struggle for public opinion is of central importance, and at the heart of strategies in contemporary conflicts due to the vitality of legitimacy.

The global information environment, of which social network media is a part, continues to change at an ever-accelerating pace, faster than most could imagine just a few years ago, due to the developments within Information and Communication Technology. Media content produced for one purpose can easily and rapidly be edited and repackaged in near real-time just to be re-transmitted across many, predominantly social network media, platforms. This challenges the traditional news media's function as gatekeepers and agenda-setters, in turn, empowering a whole host of actors effectively changing the distribution of power in the media environment and therefore also in the political sphere. While traditional media still play a vital role, this role has changed. Traditional media, pressured by economy and security issues, rely to a higher and higher extent on social network media

for both information gathering and news distribution. At the same time, the convergence between traditional and new media forms is increasing, a tendency that multiple actors constantly try to exploit. Social network media have also started to act as a form of "gatekeepers" themselves with the evolving legal role of "terms of use" and the platform administrator's arbitrary decisions about which posts, videos and imagery to host on their sites and which to erase or which accounts should be entirely closed.

Collectively, these developments have prompted several actors, state and non-state alike, to strategically use social network media. In this context "social network media refers to internet connected platforms and software used to collect, store, aggregate, share, process, discuss or deliver user-generated and general media content, that can influence knowledge, perception and thereby directly or indirectly prompt behaviour as a result of interaction", for Targeting, Intelligence collection, Psychological Warfare, Operations (offensive and defensive) and command and control purposes in order to achieve effects both on- and offline, effectively weaponizing them.

Social network media are, based on the effects resulting from the changing conflict environment and the development within information and communication technology, therefore affecting the character of contemporary conflicts in significant ways. The extent is not yet fully understood, however. What can be determined as of now is that social network media challenge and are used by all actors in contemporary conflicts. All actors have little choice but to engage in the social network media domain. Failure to do so will create a vacuum in which the opposition or third party's version of realities will become the pre-dominant narrative and, in turn, inform behaviours.

The changed conflict environment has also changed the traditional notion of the "battle-space" creating new forms of asymmetry, facilitating an increased power to, or effect of, social network media in contemporary conflicts. The traditional notions of geographical "theatres of operations" are no longer sufficient. We now have to look at "virtual theatres" as well. This results in new concepts as "remote warfare" empowering actors not previously able to create effects in the traditional battlespace. Thereby social network media effectively re-distributes power in the international system. But it also draws the conflict from remote theatres of operations and into the domestic domain of the troop contribution nations to international operations.

The bottom line is, however, that social network media has been weaponised through the systematic and strategic use for "military" (writ large – i.e., by all actors) purposes (in and through social network media - from intelligence collection and targeting to all aspects of operation) in order to create effects on- and offline. Social network media therefore have an equation-changing effect on the scale and speed of how information and information-systems affect the global information environment, in turn, altering decision-making and behaviours in the physical domain in new ways.

This has many real, but not yet fully understood, implications, including political, ethical and a variety of legal issues. With this realization, new questions arise. New questions that easily can form the basis for several new research agendas. Such agendas can include, but are not limited to, further theorisation over the basic international relations theories in order to explain the role and effect of social network media, besides from a social constructivist point of view, such as securitisation (Copenhagen school), realism and systems theory. New research agendas could also look further at case studies of conflicts more closely related to traditional inter-state wars in order to discover to which degree, if at all, that these change the findings of this monograph. A third research agenda could be more closely associated with military science and look at how social network media, due to how they affect contemporary conflicts, creates new requirements for military policy and doctrine, materiel and organisation. Lastly, it is also relevant to further explore the ethical and perhaps new legal (international humanitarian law, law of armed conflicts and Lawfare) challenges of the weaponization of social media. One thing is for certain, though – more interdisciplinary work is needed in order to understand more comprehensively how social network media affects contemporary and future conflicts and warfare.

Copenhagen, February 2015.

--- # ---

BIBLIOGRAPHY

Ackerman, Spencer: Voice of America Uses Social Media to Aid Foreign Dissent. February 15, 2011. http://www.wired.com/2011/02/voice-of-america-uses-social-media-to-aid-foreign-dissent/ (Accessed 15 APR14).

Ackerman, Spencer: Taliban Texts Terror to Afghan Phones. March 17, 2011. http://www.wired.com/2011/03/taliban-texts-terror-to-afghan-phones/ (Accessed 15 APR 14).

Alberts, David S. and Hayes, Richard E.: Understanding Command and Control. The Command and Control Research Program (CCRP). www.dodccrp.org

Alexander, Bryan and Levine, Alan: Web 2.0 Storytelling – Emergence of a New Genre. In Educause review, November/December 2008 (page 40 – 56)

Al-Jazeera: Syria's war moves to electronic battlefield. http://www.aljazeera.com/video/middleeast/2013/08/201387101132386957.html (Accessed 12 SEP13)

Altman, Howard: Post-modern warfare – Tweets attempt to influence Centcom airstrikes. Tampa Bay Online. http://tbo.com/list/military-news/post-modern-warfare-tweets-attempt-to-influence-centcom-airstrikes-20140926/ (Accessed 13 JAN 15).

Andress, Jason and Winterfeld, Steve: Cyber Warfare – Techniques, Tactics and Tools for Security Practitioners. Elsevier, Syngress, USA, 2011.

Apps, Peter: From Syria to Ukraine, social media opens up warfare. http://in.reuters.com/article/2014/08/06/us-security-socialmedia-idINKBN0G61MU20140806 (Accessed 17 SEP 14)

Arquilla, John and Ronfeldt, David: Swarming and the Future of Conflict. RAND.

Bartlett, Jamie: ISIS and their so-called social media genius: http://blogs.telegraph.co.uk/technology/jamiebartlett/100013899/isis-and-their-so-called-social-media-genius/ (Accessed 30 JUN 14)

Baylis, John; Smith, Steve and Owens, Patricia (Eds.): The Globalization of World Politics – An Introduction to International Relations. Oxford University Press, 5th edition, 2011.

Baylis, John; Wirtz, James J. and Grey, Colin S. (Eds.): Strategy in the Contemporary World – An Introduction to Strategic Studies. Oxford University Press, 4th Edition, 2013.

Betz, David: Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. In Journal of Strategic Studies. Volume 35, no. 5, October 2012, pp 689 – 711.

Borkowski, Mark: ISIS and the propaganda war: How the social-savvy extremists are dominating the headlines. http://www.thedrum.com/opinion/2014/06/25/isis-and-propaganda-war-how-social-savvy-extremists-are-dominating-headlines (Accessed 27 JUN 14)

Boothby, William: Conflict law – The Influence of New Weapons Technology, Human Rights and Emerging Actors. Asser Press, Springer, The Hague, the Netherlands, 2014.

Brownlee, Billie Jeanne: Media and the Syrian Revolution – a war of truths and lies. (15 AUG 12) www.yourmiddleeast.com

Buch, David: Ondsindet hackerangreb på New York Times. http://nyhederne.tv2.dk/article.php/id-71010671:ondsindet-hackerangreb-på-new-york-times.html (Accessed 12 SEP 13)

Burchill, Scott (et al): Theories of International Relations. Palgrave Macmillan, 4th edition, 2009.

Buzan, Barry: Peoples, States and Fear – An agenda for International Security Studies in the post-Cold War Era. 2nd Edition, Harvester Wheatsheaf, UK, 1991.

Caldwell, William B.; Murphy, Dennis M. and Menning, Anton: Learning to Leverage New Media – The Israeli Defense Forces in Recent Conflicts. In Military Review, May – June 2009. (Page 2 – 10).

Castells, Manuel: Communication power, 2009, Oxford University Press.

Clayton, Mark: Syrian's cyberwars: using social media against dissent (25 JUL 12) http://www.csmonitor.com/USA/2012/0725/Syria-s-cyberwars-using-social-media-against-dissent

Collings, Deirdre and Rohozinski, Rafal: Bullets and Blogs – New Media and the Warfighter. US Army War College, Carlisle Barracks, Pennsylvania, USA, 2009.

Comninos, A: "E-revolutions and cyber crackdowns: User-generated content and social networking in protests in MENA and beyond," GSI Watch – Internet rights and democratisation, 2011. http://www.giswatch.org/sites/default/files/gisw_-_e-revolutions_and_cyber_crackdowns_0.pdf.

Coombs, Timothy W. and Holladay, Sherry J. (Eds.): The Handbook of Crisis Communication, Wiley-Blackwell, Malden, MA, 2009.

Creveld, Martin Van: The Transformation of War. The Free Press, New York, USA, 1991.

Cunningham, Timothy: Strategic Communication in the New Media Sphere. In Joint Force Quarterly (JFQ), issue 59, 4th quarter 2010, pp 110 - 114. National Defence University Press (NDUPress).

Dauber, Cori E.: YouTube War – Fighting In A World of Cameras in Every Cell Phone and Photoshop on Every Computer. US Army Strategic Studies Institute, November 2009. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=951 (Accessed 15 APR 14).

Dinniss, Heather Harrison: Cyber Warfare and the Laws of War: Cambridge, Cambridge University Press, 2012.

Dunlap, Charles J., Jr., Lawfare Today…and Tomorrow. In International Law and the Changing Character of War. (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger, eds.), US Naval War College International Law Studies, Vol. 87, 2011. Page 315-325.

Efaw, James: Social Networking Services – The New Influence Frontier. In: IOSphere, Winter 2009. http://home.iosphere.org/?page_id=234 (Accessed 13 APR 14).

European Commission: Communicating with the outside world – Guidelines for All Staff on the Use of Social Media, 2013. Http://ec.europa.eu/ipg/docs/guidelines_social_media_en.pdf (Accessed 24 FEB 14)

Farrell, Henry: Five key questions – and answers – about Iran's social media influence. In The Washington Post. December 17, 2013. http://www.washingtonpost.com/blogs/monkey-cage/wp/2013/12/17/five-key-questions-and-answers-about-irans-social-media-influence/ (Accessed 14 APR 14).

Farwell, James and Arakelian, Darby: A Better Syria Option: Cyber War. (Accessed 18 NOV 13): http://nationalinterest.org/commentary/better-syria-option-cyber-war-9003.

Farwell, James and Arakelian, Darby: What to do Next About Syria. December 26, 2013. http://www.huffingtonpost.com/james-p-farwell/what-to-do-next-about-syria_b_4494532.html (Accessed 14 APR 14).

Feldman, Rachel: "'Fried' request from Al-Qaeda", University of Haifa, 8 January 2012: http://newmedia-eng.haifa.ac.il/?p=5680 (Accessed 12 MAR 14)

Fielding, Nick and Cobain, Ian: Revealed – US spy operation that manipulates social media. In: The Guardian (UK), March 17, 2011 http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks (Accessed 14 APR 14).

Fitzpatrick, Alex: Social Media Becoming Online Battlefield in Syria. (9 AUG 12) http://mashable.com/2012/08/09/social-media-syria/

Franco, Chiara De: Media Power and the Transformation of War, New York, NY: Palgrave Macmillan, 2012.

Franke, Ulrik: Information Operations on the Internet – A Catalog of Modi Operandi. Swedish Defence Research Agency. Report no.: FOI-R-3658-SE, March 2013.

Fulghum, David A.: Israel shows electronic prowess. In Aviation Week and Space Technology. 25 November 2007. https://warsclerotic.wordpress.com/2010/09/28/israel-shows-electronic-prowess/ (Accessed 10 FEB 14)

Goldman, Lisa: In Syria's Civil War, Cyber Attacks are the 'New Modern Warfare'. (8 AUG 12) www.techpresident.com

Gomez, Jeff: Storyworlds – The New Transmedia Business Paradigm, 2011. http://www.transmediaproducer.org/portfolio/toc-2010-jeff-gomez-storyworlds-the-new-transmedia-business-paradigm/#/toc-2010-jeff-gomez-storyworlds-the-new-transmedia-business-paradigm (Accessed 27 AUG 14)

Gowing, Nik: 'Skyful of Lies' and Black Swans. The new tyranny of shifting information power in crises. RISJ CHALLENGES, 2009.

Grdovic, Mark: Developing a Common Understanding of Unconventional Warfare. In Joint force Quarterly (JFQ), issue 57, 2d quarter 2010 (pp. 136 – 138). Published by National Defence University, NDU Press, USA.

Grossman, Lev: Iran Protests: Twitter, the Medium of the Movement. http://content.time.com/time/world/article/0,8599,1905125,00.html (Accessed 20 MAR 14)

Harding, Luke and Arthur, Charles: Syrian Electronic Army: Assad's cyber warriors. http://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background (Accessed 12 SEP 13)

Hopkins, Nick and Harding, Luke: Pro-Assad Syrian hackers launching cyber-attacks on western media http://www.theguardian.com/world/2013/apr/29/assad-syrian-hackers-cyber-attacks (Accessed 12 SEP13)

Hoskins, A., & O'Loughlin, B.: War and media - The emergence of diffused war. Malden, MA: Polity Press, 2010.

Howard, Philip N: The Digital Origins of Dictatorship and Democracy – Information Technology and Political Islam. Oxford University Press, New York, 2010.

Howe, Jeff, The Rise of Crowdsourcing, The wired Magazine, June 2006. Available under http://www.wired.com/wired/archive/14.06/crowds.html (Accessed 26 MAR 14)

Howe, Jeff, Crowdsourcing: A Definition, June 2006. Available under http://crowdsourcing.typepad.com/cs/2006/06/crowdsourcing_a.html (Accessed 26 MAR 14)

Hunker, Jeffrey: Cyber war and cyber power – Issues for NATO doctrine. Research Paper, NATO Defence College, Rome, No. 62, November 2010.

Hunter, Elizabeth: The Arab Revolution and Social Media, 2011. (Accessed 16 FEB 14) http://flipthemedia.com/2011/02/the-arab-revolution-and-social-media/

Ibish, Hussein: http://ibishblog.com/2014/08/09/isis-and-its-success-narrative-must-be-broken (Accessed 27 AUG 14)

Jackson, Robert and Sørensen, Georg: Introduction to International Relations – Theories and Approached. Oxford University Press, 3ed edition, 2007.

Jaitner, Margarita: Exercising Power in Social Media. In: The Fog of Cyber Defence (Eds. Jari Rantapelkonen & Mirva Salminen). National Defence University Department of Leadership and Military Pedagogy. Publication Series 2. Article Collection no. 10. Helsinki, Finland, 2013.

Jenkins, Henry: Transmedia Storytelling. In Technology Review (MIT), 2003. http://www.technologyreview.com/news/401760/transmedia-storytelling/ (Accessed 24 MAR 14)

Jenkins, Henry with Purushotma, Ravi, Weigel, Margaret, Clinton, Katie and Robison, Alice J.: Confronting the Challenges of Participatory Culture – Media Education for the 21st Century, The MIT Press, Cambridge, Massachusetts, London, England, 2009, www.macfound.org.

Jessen, Catarina Nedertoft and Kaarsholm, Lotte Folke: Diplomatiets digitale overmand. http://www.information.dk/493514 (Accessed 06 APR 14)

Jones, Nigel and Baines, Paul: Losing Control – Social Media and Military Influence. In The RUSI Journal, February / March 2013, volume 158, number 1, pp. 72 – 78.

Kaldor, Mary: New and Old Wars – Organized Violence in a Global Era. 2nd Edition, 2011, Polity Press, Cambridge, UK.

Kaldor, Mary: In Defence of New Wars. In Stability, article no. 4, 2013, pp. 1 – 16. http://www.stabilityjournal.org/article/view/sta.at (Accessed 14 APR 14).

Kaplan, Andreas. M. and Haenlein, Michael: Users of the world, unite – The challenges and opportunities of social media, Business Horizons, no. 53, Kelly School of Business, Indiana University, 2009, pp. 59 – 68. http://www.slideshare.net/escpexchange/kaplan-haenlein-users-of-the-world-unite-the-challenges-and-opportunities-of-social-media# (Accessed 24 FEB 14).

Katerji, Oz: The Syrian Electronic Army Talks About Hacking the 'Guardian' and Their Obama Bomb Hoax http://www.vice.com/read/the-syrian-electronic-army-almost-crashed-the-dow-jones (Accessed 12 SEP 13)

Keene, Shima D.: Threat Finance - Disconnecting the Lifeline of Organised Crime and Terrorism, Gower, September 2012.

Kerr, Dara: How Israel and Hamas Weaponized Social Media. www.cnet.com , 13 January 2014. (Accessed 03 APR 14)

Kilcullen, David: Out of the Mountains – The Coming Age of the Urban Guerrilla. Oxford University Press, 2013.

Kingsley, Patrick: Who is behind ISIS's terrifying online propaganda operation? http://www.theguardian.com/world/2014/jun/23/who-behind-isis-propaganda-operation-iraq (Accessed 26 JUN 14)

Lawson, Sean: The US military's social media civil war: technology and antagonism in discourses of information-age conflict. In Cambridge Review of International Affairs, 07 MAR 2013. http://dx.doi.org/10.1080/09557571.2012.734787

Liff, Adam P.: Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. In: The Journal of Strategic Studies. Vol. 35, No. 3, June 2012, page 401 – 428.

Lonsdale, David J.: The Nature of War in the Information Age – Clausewitzian Future. Frank Cass, London, 2004.

Mackey, Robert: Crisis in Syria looks very different on satellite channels owned by Russia and Iran. http://thelede.blogs.nytimes.com/2012/02/10/crisis-in-syria-looks-very-different-on-satellite-channels-owned-by-russia-and-iran/?_php=true&_type=blogs&_r=0 (Accessed 04 APR 14).

MacKay, Andrew and Tatham, Steve: Behavioural Conflict – Why understanding people and their behaviour will prove decisive in future conflicts, Military Studies Press, UK, 2011.

Matejic, Nicole: How ISIL have weaponized Social Media in Iraq. http://www.infoopshq.com/case-study-isil-weaponized-social-media-iraq/ (Accessed 10 JUL 14)

Matthews, Dylan: The surreal infographics ISIS is producing, translated. http://www.vox.com/2014/6/24/5834068/the-iraqi-rebels-make-annual-reports-with-infographics-we-translated (Accessed 27 JUN 14)

Michael, Alex: Cyber Probing – The Politicisation of Virtual Attack. Special Series 10/12. Defence Academy of the United Kingdom, September 2012.

Miller, Carol Handler: Digital Storytelling – A creator's Guide to Interactive Entertainment. Elsevier, Amsterdam, 2008. 2nd edition.

Mitchell, William: Project Kitae - Battlespace Agility in Helmand - Network vs. Hierarchy C2. 2012. http://forsvaret.dk/FAK/PUBLIKATIONER/RESEARCH%20PAPERS/Pages/Forsvarsakedemiet%20Working%20Papers.aspx#publication_b1399452-e6dd-4abb-b2e0-98633d9c089f (Accessed 03 APR 14)

Multinational Capability Development Campaign (MCDC): Applied concept for Social Media for Situational Awareness, September 2014.

Murphy, Dennis: Fighting Back - New Media and Military Operations, Center for Strategic Leadership, United States Army War College, November 2008.

Münkler, Herfried: The New Wars. Cambridge, Polity Press, 2005.

Møller, Hans Henrik: Effects-Based Thinking in NATO. Page 173 – 189. In "Preparing for the Imperfect World: Strategy in NATO". (Ed. Liselotte Odgaard) Palgrave MacMillan, London, 2014.

NATO - MC Position on the use of effects in operations (MCM-0041-2010), 20 July 2010, NATO UNCLASSIFIED.

NATO Allied Joint Publication (AJP) 01 (D) Operations Doctrine, 2010, NATO UNCLASSIFIED.

NATO Allied Joint Publication (AJP) 03 (B) Operations Doctrine, NATO UNCLASSIFIED.

NATO Allied Joint Publication (AJP) 3.10 Information Operations Doctrine, Study Draft, Version 1.1., 2013, NATO UNCLASSIFIED.

NATO - ACO Directive 95-3: Social Media. SHAPE, Mons, Belgium, December 2009. http://www.aco.nato.int/page300303028.aspx (Accessed 24 FEB 14).

NATO System Analysis and Studies (SAS) research project 050: Exploring New Command and Control Capabilities. Final Report, January 2006

Nissen, Thomas Elkjer: Tactical Information Operations in Contemporary COIN Campaigns. RDDC Research Paper, September 2011. (Accessed 27 MAR 14) http://forsvaret.dk/FAK/ENG/PUBLICATIONS/Pages/default.aspx

Nissen, Thomas Elkjer: Black and White and 256 Shades of Grey in Between – Reflections on the question of Attribution of Psychological Operations. RDDC Brief, March 2012. http://forsvaret.dk/FAK/ENG/PUBLICATIONS/Pages/default.aspx (Accessed 26 MAR 14).

Nissen, Thomas Elkjer (2013a): Narrative Led Operations. In Militært Tidsskrift (Danish Military Journal), Volume 141, no. 4 - January 2013, pp. 67 – 77.

Nissen, Thomas Elkjer (2013b): The Ever Changing Narrative of Conflict – How the Role of War Narratives Changes from Mobilizing for the Battle of Perceptions to Influencing History. Pp. 73 – 83, in Democracy Managers. (Ed. Carsten Jensen) Published by the Royal Danish Defence College, June 2013.

Nissen, Thomas Elkjer (2014a): Strategizing NATOs Narratives. Page 157 – 171. In "Preparing for the Imperfect World: Strategy in NATO". (Ed. Liselotte Odgaard) Palgrave MacMillan, London, 2014.

Nissen, Thomas Elkjer (2014b): Terror.com - IS's Social Media Warfare in Syria and Iraq. In Contemporary Conflicts (RDDC Web Military Studies Magazine) September 2014, 2nd volume. http://forsvaret.dk/FAK/eng/news/magazine/Pages/default.aspx

O'Reilly, Tim: What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software. http://oreilly.com/web2/archive/what-is-web-20.html (Accessed 23 MAR 13)

Peled, Ariel: "The first social media war between Israel and Gaza," The Guardian online, 6 December 2012, http://www.guardian.co.uk/media-network/media-network-blog/2012/dec/06/first-social-media-war-israel-gaza (Accessed 12 MAR 14)

Petersen, Anja Bechmann: Internet and Cross Media Productions: Case Studies in Two Major Danish Media Organizations. In Australian Journal of Emerging Technologies and Society AJETS Vol. 4, No. 2, 2006, pp: 94-107. http://www.swin.edu.au/ajets (Accessed 24 MAR 14).

Pftit, Brian: Social Media and Unconventional Warfare. In Special Warfare, April-June 2012, page 21 – 28.

Pizzi, Michael: The Syrian Opposition Is Disappearing From Facebook. In The Atlantic.com, February 4, 2014. http://www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-Facebook/283562/ (Accessed 15 APR 14).

Pollock, John: People Power 2.0. – How Civilians Helped Win the Libyan Information War. In MIT Technology Review, April 20, 2012.

Powell, Rose: Cats and Kalashnikovs: Behind the ISIL social media strategy. http://www.smh.com.au/world/cats-and-kalashnikovs-behind-the-isil-social-media-strategy-20140625-zsk50.html (Accessed 26 JUN 14)

Reilly, Richard Byrne: Iraq cracks down further on social media – but leaves ISIS-affiliated web sites alone. http://venturebeat.com/2014/06/23/iraq-cracks-down-further-on-social-media-but-leaves-isis-affiliated-web-sites-alone/ (Accessed 26 JUN 14)

Rid, Thomas and Hecker, Marc: War 2.0 – Irregular Warfare in the Information Age. Praeger Security International, London, 2009.

Rid, Thomas: Cyber War Will Not Take Place. In Journal of Strategic Studies. Volume 35, no. 1, February 2012. Page 5 – 32.

Ringsmose, Jens: Den medie-militære relation mellem kontinuitet og nybrud. In International Politikk, volume 71, no. 2, 2013, page 149 – 173.

Robertson, Katie: Taliban using Facebook to lure Aussie soldier. In The Sunday Telegraph, September 9, 2012. http://www.news.com.au/national/nsw-act/taliban-using-Facebook-to-lure-aussie-soldier/story-fndo4bst-1226468094586 (Accessed 14 APR 14).

Seaboyer, Anthony: The Evolution of Russian Cyber Influence Activity – A Comparison of Russian Cyber Ops in Georgia (2008) and Ukraine (2014). Contract Report No. DRDC-RDDC-2014-C119. Royal Military College of Canada, Department of Political Science.

SecDev Group: Syria Cyber Watch. Published online 25 November 2012. www.secdev.com (Accessed 4 APR 14).

SecDev Group (2013a): Flash Note Syria – Syrian Regime Tightens Access to Secure Online Communications. Published online 23 April 2013. www.secdev.com (Accessed 4 APR 14).

SecDev Group (2013b): Flash Note Syria – The Internet in Syria – Down, but not out. Published online 8 May 2013. www.secdec.com (Accessed 4 APR 14).

SecDev Group (2013c): Flash Note Syria – Syrian Electronic Army Goes on the Offensive, Intensifies Targeting of Opposition Facebook Pages. Published online 4 June 2013. www.secdev.com (Accessed 4 APR 14).

SecDev Group (2013d): Backgrounder – The Hard Realities of Soft Power – Keeping Syrians Safe in a Wired War. Published online 25 June 2013. www.secdev.com (Accessed 4 APR 14).

SecDev Group (2013e): Flash Note Syria – Find, Fix and Finish – Syrian Activist Targeted for Online Activities. Published online 6 September 2013. www.secdev.com (Accessed 4 APR 14).

SecDev Group (2013f): Flash Note Syria – Syria's National Defence Forces take the Battle to Cyberspace. Published online 30 September 2013. www.secdev.com (Accessed 4 APR 14).

SecDev Group (2013g): Flash Note Syria – Syria's Hacker Wars. Published online 8 October 2013. www.secdev.com (Accessed 4 APR 14).

Simpson, Emile: War from the ground up – Twenty-First-Century Combat as Politics. Oxford University Press, New York, 2013.

Sloan, Elinor, C.: Modern Military Strategy – An Introduction. Routledge, 2012.

Smith, Rupert: The Utility of Force – The art of war in the modern world. Penguin, Allan Lane. London, England, 2005.

Snyderwine, William B.: The Dictator's Dilemma - The Role of Social Media in Revolutions. https://econ.duke.edu/uploads/media_items/snyderwine-dictator-s-dilemma-final.original.pdf. (Accessed 28 MAR 14)

Terrazas, Michael: Four Telltale Signs of Propaganda on Twitter. May 31, 2012. http://www.scs.gatech.edu/content/four-telltale-signs-propaganda-twitter (Accessed 14 APR 14).

Thomas, W. I.: The Unadjusted Girl. Boston: Little, Brown and Co., 1923.

Townsend, Mark: Jihad in a social media age: how can the west win an online war? http://www.theguardian.com/world/2014/aug/23/jihad-social-media-age-west-win-online-war (Accessed 24 AUG 14)

Tucker, Patrick: Social Media's Very Arab Future. http://www.defenseone.com/technology/2014/09/social-medias-very-arab-future/93488/print/ (Accessed 17 SEP 14)

UK ministry of Defence (UK MoD): Cyber Primer. Published by: Development, Concepts and Doctrine Centre (DCDC), December 2013. www.gov.uk/development-concepts-and-doctrine-centre (Accessed 14 APR 14)

US Department of Defense (US DoD): Joint Publication: JP 3-13: Information Operations, November 2012, page vii – viii. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (Accessed 12 MAR 14).

US Department of Defense (US DoD): Military Community and Family Policy Social Media Guide, http://www.militaryonesource.mil/12038/MOS/ResourceGuides/Social_Media_Guide.pdf. (Accessed 16 FEB 14)

Verrall, Neil: #gamechanger @MilitarySocialMedia. IOsphere, 2014. (home.iosphere.org)

Waxmann, Matthew C.: Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). In Yale Journal of International Law. Hein Online – 36 Yale J. Int'l 2011.

Weimann, Gabriel: New Terrorism and New Media.(2014) www.wilsoncenter.org/publications/new-terrorism-and-new-media

Wendt, Alexander: Anarchy is what states make of it – the social construction of power politics. In International Organizations, volume 46, no. 2 (Spring 1992), pp. 391 – 425.

Zambelis, Chris: Information Wars: Assessing the Social Media Battlefield in Syria (22 AUG 12). https://www.ctc.usma.edu/posts/information-wars-assessing-the-social-media-battlefield-in-syria

Other sources:

Curriculum for the Master's program in International Security and Law at the University of Southern Denmark. (Accessed 6 FEB 14): http://www.sdu.dk/en/Information_til/Studerende_ved_SDU/Din_uddannelse/Kandidat/IntSecureLaw/Uddannelsens_opbygning/Studieordninger

http://www.darpa.mil/Our_Work/I2O/Programs/Social_Media_in_Strategic_Communication_(SMISC).aspx (Accessed 14 APR 14).

http://www.oxforddictionaries.com

http://whatis.techtarget.com

http://www.thefreedictionary.com

http://peace.stanford.edu/ & http://captology.stanford.edu/ (Accessed 13 APR 14)

http://nyhederne.tv2.dk/udland/2014-04-03-tyrkiet-oph%C3%A6ver-twitter-forbud?nidk (Accessed 4 APR 14)

http://www.todayszaman.com/news-343325-politicized-friday-prayer-sermon-supports-blocking-of-social-media-platforms.html (Accessed 31 MAR 14)

www.twitter.com/speak2tweet (Accessed 15 APR 14).

END NOTES

CHAPTER 1:

1 See Thomas Rid: Cyber war will not take place.
2 http://www.dunproject.org/ (Accessed 13 AUG14)
3 Herfried Münkler: The New Wars. Cambridge, Polity Press, 2005, p. 1.
4 Simpson, Emile: War from the ground up – Twenty-First-Century Combat as Politics. Oxford University Press, New York, 2013, p. 41.
5 Simpson, 2013, p. 3.
6 Carl von Clausewitz: On War, book 1, chapter 1.
7 One must remember that this is a Western European conception of classical war brought about by the peace of 1648 and the birth of the Westphalian state system.
8 Mary Kaldor: In Defence of New Wars. In Stability, Article no. 4, 2013, p. 1 – 16. p. 1
9 Mary Kaldor: New and Old Wars – Organized Violence in a Global Era. 2nd Edition, 2011, Polity Press, Cambridge, UK, pp. 1 – 2.
10 Kaldor, 2013, p. 2.
11 Kaldor, 2013, p. 3.
12 Münkler, 2005, chapter 4.
13 Martin van Creveld: The Transformation of War. The Free Press, New York, USA, 1991, p. xi.
14 Creveld, 1991, pp. 10 – 11.
15 Creveld, 1991, pp. 18 – 25.
16 Kilcullen, 2013.
17 Simpson, 2013, p. 10.
18 Simpson, 2013, p. 12.
19 Thomas Elkjer Nissen: Thomas Elkjer Nissen (2013): The Ever Changing Narrative of Conflict – How the Role of War Narratives Changes from Mobilizing for the Battle of Perceptions to Influencing History. Pp. 73 – 83, in Democracy Managers. (Ed. Carsten Jensen) Published by the Royal Danish Defence College, June 2013. Pp. 80 – 83.
20 Simpson, 2013, pp. 1 - 2.
21 Simpson, 2013, p. 6.
22 Rupert Smith: The Utility of Force – The art of war in the modern world. Penguin, Allan Lane. London, England, 2005, p. 289.
23 David Kilcullen: Out of the Mountains – The Coming Age of the Urban Guerrilla. Oxford University Press, 2013.P. 171.

CHAPTER 2:

24 Fra W. I. Thomas, The Unadjusted Girl. Boston: Little, Brown and Co., 1923.
25 Jackson, Robert and Sørensen, Georg: Introduction to International Relations – Theories and Approached. Oxford University Press, 3rd edition, 2007, p. 162.
26 Wendt, 1992, p. 397.
27 Michael Barnett: Social constructivism. In Baylis, John; Smith, Steve and Owens, Patricia: The Globalization of World Politics – An Introduction to International Relations. Oxford University Press, 5th edition, 2011, pp. 149 – 150.
28 Barry Buzan: Peoples, States and Fear – An agenda for International Security Studies in the post-Cold War Era. 2nd Edition, Harvester Wheatsheaf, UK, 1991, pp. 269 – 271.
29 Wendt, 1992, p. 397.
30 Simpson, 2013, pp. 35 – 36.
31 Simpson, 2013, p. 37.
32 See Simpson, 2013, pp. 38 – 39.
33 Manuel Castells: Communication power, 2009, Oxford University Press, p. 10.
34 Thomas Elkjer Nissen: Narrative Led Operations. In Militært Tidsskrift (Danish Military Journal), Volume 141, no. 4 - January 2013, pp. 67 – 77; p. 69
35 US Department of Defense: Joint Publication: JP 3-13: Information Operations, November 2012, pp. vii – viii. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf. (Accessed 12 MAR 14).
36 NATO – AJP 3.10 Information Operations, paragraph 0102.
37 Simpson, 2013, pp. 6 – 7.
38 Rid, Thomas and Hecker, Marc: War 2.0 – Irregular Warfare in the Information Age. Praeger Security International, London, 2009, p. 6.
39 Ariel Peled: "The first social media war between Israel and Gaza," The Guardian online, 6 December 2012, http://www.guardian.co.uk/media-network/media-network-blog/2012/dec/06/first-social-media-war-israel-gaza (Accessed 12 MAR 14)
40 Rachel Feldman: "'Fried' request from Al-Qaeda", University of Haifa, 8 January 2012: http://newmedia-eng.haifa.ac.il/?p=5680. (Accessed 12 MAR 14)
41 A. Comninos, "E-revolutions and cyber crackdowns: User-generated content and social networking in protests in MENA and beyond," GSI Watch – Internet rights and democratisation, 2011, p. 34. http://www.giswatch.org/sites/default/files/gisw_-_e-revolutions_and_cyber_crackdowns_0.pdf.
42 Simpson, 2013, p. 12.
43 Simpson, 2013, p. 9.
44 Thomas Rid: Cyber War Will Not Take Place. In Journal of Strategic Studies. Volume 35, no. 1, February 2012. Pp. 5 – 32; p. 7.

45 Adam P. Liff: Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. In: The Journal of Strategic Studies. Vol. 35, No. 3, June 2012, pp. 401 – 428. p. 408.
46 Liff, 2012, pp. 415-416.
47 Based on Matthew C. Waxmann: Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). In Yale Journal of International Law. Hein Online – 36 Yale J. Int`l 2011. P. 422.
48 See NATO CoE for StratCom "Analysis of Russia´s Information Campaign": http://www.stratcomcoe.org/~/media/SCCE/Ukraine_report_StratComCOE_Public_Fin2.ashx (Accessed 9 FEB 15), and Pomerantsev (OpCit).
49 Thomas Rid: Cyber War Will Not Take Place. In Journal of Strategic Studies. Volume 35, no. 1, February 2012. Page 5 – 32.
50 Jeffrey Hunker: Cyber war and cyber power – Issues for NATO doctrine. Research Paper, NATO Defence College, Rome, No. 62, November 2010; p. 6.
51 Waxmann, 2011, p. 426.
52 Rid, 2011, p. 16.
53 Alex Michael: Cyber Probing – The Politicisation of Virtual Attack. Special Series 10/12. Defence Academy of the United Kingdom, September 2012, pp. 1 – 2.
54 Liff, 2012, p. 408.
55 Liff, 2012, p. 422.
56 Rid, 2012, p. 9.
57 See Betz, 2012, p. 690.

CHAPTER 3:

58 See Tim O'Reilly: What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software. http://oreilly.com/web2/archive/what-is-web-20.html (Accessed 23 MAR 13) and FMV Swedish Defence Materiel Administration (FMV): Rapport on Social Media No. 58482/2009.
59 Huges et.al: "Site-seeing" in disaster – An Examination of On-line Social Convergence. In Conference proceedings of the 5th International ISCRAM Conference, Washington D.C., 2008, p. 8
60 Coombs, Timothy W. and Holladay, Sherry J. (Eds.): The Handbook of Crisis Communication, Wiley-Blackwell, Malden, MA, 2009. P. 381
61 Deirdre Collings and Rafal Rohozinski: Bullets and Blogs – New Media and the Warfighter. US Army War College, Carlisle Barracks, Pennsylvania, USA, 2009. Pp. 9 – 10.
62 Kaplan, Andreas. M. and Haenlein, Michael: Users of the world, unite – The challenges and opportunities of social media, Business Horizons, no. 53, Kelly School of Business, Indiana University, 2009, pp. 59 – 68, p. 61. http://www.

slideshare.net/escpexchange/kaplan-haenlein-users-of-the-world-unite-the-challenges-and-opportunities-of-social-media# (Accessed 24 FEB 14)

63 European Commission: Communicating with the outside world – Guidelines for All Staff on the Use of Social Media, 2013. http://ec.europa.eu/ipg/docs/guidelines_social_media_en.pdf (Accessed 24 FEB 14)

64 Kaplan and Haenlein (2009), p. 62.

65 NATO - ACO Directive 95-3: Social Media. SHAPE, Mons, Belgium, December 2009, p. 3. http://www.aco.nato.int/page300303028.aspx (Accessed 24 FEB 14).

66 Collings and Rohozinski, 2009, p. 7.

67 Petersen, Anja Bechmann: Internet and Cross Media Productions: Case Studies in Two Major Danish Media Organizations. In Australian Journal of Emerging Technologies and Society AJETS Vol. 4, No. 2, 2006, pp. 94-107. http://www.swin.edu.au/ajets (Accessed 24 MAR 14). P. 95.

68 See Nissen, 2013a.

69 http://en.wikipedia.org/wiki/Crossmedia (Accessed 24 MAR 14)

70 Jenkins, Henry: Transmedia Storytelling. In Technology Review (MIT), 2003. http://www.technologyreview.com/news/401760/transmedia-storytelling/ (Accessed 24 MAR 14). P. 3.

71 Carol Handler Miller: Digital Storytelling – A creator's Guide to Interactive Entertainment. Elsevier, Amsterdam, 2008. 2nd edition.

72 Based on Thomas Elkjer Nissen: Strategizing NATOs Narratives. (pp. 157 – 162) In Strategy in NATO – Preparing for an Imperfect World. Ed. Liselotte Odgaard. Palgrave Macmillan, 2014.

73 Alister Miskimmon, Ben O`Loughlin and Laura Roselle: Forging the World: Strategic Narratives and International Relations. October 2011. P. 3. http://newpolcom.rhul.ac.uk/npcu-blog/2012/1/17/strategic-narratives-working-paper-published.html (accessed August 20, 2013)

74 Jeffry R. Halverson, H. L. Goodall and Steven R. Corman: Master Narratives of Islamist Extremism. New York: Palgrave MacMillan, 2011.

75 Ibid.

76 UK MoD: Joint Doctrine Note 12/1: Defence Contribution to Strategic Communication. Pp. 2-10.

77 Based on Alister Miskimmon, Ben O`Loughlin and Laura Roselle: Forging the World: Strategic Narratives and International Relations. October 2011. P. 3. http://newpolcom.rhul.ac.uk/npcu-blog/2012/1/17/strategic-narratives-working-paper-published.html (accessed August 20, 2013)

78 Laura Roselle: Strategic Narratives of War – Fear of Entrapment and Abandonment During Protracted Conflict. SGI, Stockholm, September 2010. P. 6.

79 Bryan Alexander and Alan Levine: Web 2.0 Storytelling – Emergence of a New Genre. In Educause review, November/December 2008 (pp. 40 – 56), p. 40.

80 Jeff Gomez: Storyworlds – The New Transmedia Business Paradigm. http://www.transmediaproducer.org/portfolio/toc-2010-jeff-gomez-storyworlds-the-new-transmedia-business-paradigm/#/toc-2010-jeff-gomez-storyworlds-the-new-transmedia-business-paradigm

81 Alexander and Levine (2008), p. 51.

82 Henry Jenkins, Ravi Purushotma, Margaret Weigel, Katie Clinton and Alice J. Robison: Confronting the Challenges of Participatory Culture – Media Education for the 21st Century, The MIT Press, Cambridge, Massachusetts, London, England, 2009, www.macfound.org. Pp. 87 – 88.

83 Based on: (An earlier version of this case study have been published in September 2014 in the Royal Danish Defence College's online military studies magazine "Contemporary Conflict".

Jamie Bartlett: ISIS and their so-called social media genius. http://blogs.telegraph.co.uk/technology/jamiebartlett/100013899/isis-and-their-so-called-social-media-genius/ (Accessed 30 JUN 14)

Patrick Kingsley: Who is behind ISIS's terrifying online propaganda operation? http://www.theguardian.com/world/2014/jun/23/who-behind-isis-propaganda-operation-iraq (Accessed 26 JUN 14)

Richard Byrne Reilly: Iraq cracks down further on social media – but leaves ISIS-affiliated web sites alone. http://venturebeat.com/2014/06/23/iraq-cracks-down-further-on-social-media-but-leaves-isis-affiliated-web-sites-alone/ (Accessed 26 JUN 14)

Mark Borkowski: ISIS and the propaganda war: How the social-savvy extremists are dominating the headlines. http://www.thedrum.com/opinion/2014/06/25/isis-and-propaganda-war-how-social-savvy-extremists-are-dominating-headlines (Accessed 27 JUN 14)

Rose Powell: Cats and Kalashnikovs: Behind the ISIL social media strategy. http://www.smh.com.au/world/cats-and-kalashnikovs-behind-the-isil-social-media-strategy-20140625-zsk50.html (Accessed 26 JUN 14)

Dylan Matthews: The surreal infographics ISIS is producing, translated. http://www.vox.com/2014/6/24/5834068/the-iraqi-rebels-make-annual-reports-with-infographics-we-translated (Accessed 27 JUN 14)

84 Mark Borkowski: ISIS and the propaganda war: How the social-savvy extremists are dominating the headlines. http://www.thedrum.com/opinion/2014/06/25/isis-and-propaganda-war-how-social-savvy-extremists-are-dominating-headlines (Accessed 27 JUN 14)

85 Mark Townsend: Jihad in a social media age: how can the west win an online war? http://www.theguardian.com/world/2014/aug/23/jihad-social-media-age-west-win-online-war (Accessed 24 AUG 14)

86 Dan Bloom: ISIS use US journalist hostage as focus of latest terror campaign on social media by hijacking discussions using #StenensHeadInObamas Hands hsahtag. http://www.dailymail.co.uk/news/article-2734534/ISIS-use-US-journalist-hostage-focus-latest-terror-campaign-social-media-hijacking-discussions-using-StevensHeadInObamasHands-hashtag.html (Accessed 13 FEB 15)

87 Hussein Ibish: http://ibishblog.com/2014/08/09/isis-and-its-success-narrative-must-be-broken/ (Accessed 27 AUG 14)

88 Nicole Matejic: How ISIL have weaponized Social Media in Iraq. http://www.infoopshq.com/case-study-isil-weaponized-social-media-iraq/ (Accessed 10 JUL 14)

89 Alice Speri: ISIS Fighters and Their Friends Are Total Social Media Pros. https://news.vice.com/article/isis-fighters-and-their-friends-are-total-social-media-pros (Accessed 30 JUN 14)

90 J. M. Berger: How ISIS Games Twitter. In The Atlantic. (Accessed16 JUN 14). http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

91 Townsend (2014)

92 https://citizenlab.org. (Accessed 27 JUN 14)

93 The Intelligence "gain – loss" analysis is pivotal to counter-propaganda activities online.

CHAPTER 4:

94 Hans Henrik Møller: Effects-Based Thinking in NATO. Pp. 173 – 189. In "Preparing for the Imperfect World: Strategy in NATO". (Ed. Liselotte Odgaard) Palgrave MacMillan, London, 2014, p. 180.

95 Shima D. Keene: Threat Finance - Disconnecting the Lifeline of Organised Crime and Terrorism, Gower, September 2012.

96 NATO - MC Position on the use of effects in operations (MCM-0041-2010), 20 July 2010, NATO UNCLASSIFIED.

97 NATO - Allied Joint Publication (AJP) 3.10 Information Operations Doctrine, Study Draft, Version 1.1., 2013, NATO UNCLASSIFIED

98 NATO Allied Joint Publication (AJP) 3.10 Information Operations Doctrine, Study Draft, Version 1.1., 2013, NATO UNCLASSIFIED: Ulrik Franke: Information Operations on the Internet – A Catalog of Modi Operandi. Swedish Defence Research Agency. Report no.: FOI-R-3658-SE, March 2013, and http://www.oxforddictionaries.com/definition/english/ (Accessed 30 APR 14).

99 For more on computer network attack and social media, see, e.g., Jaitner, Margarita: Exercising Power in Social Media. In: The Fog of Cyber Defence (Eds. Jari Rantapelkonen & Mirva Salminen). National Defence University

Department of Leadership and Military Pedagogy. Publication Series 2. Article Collection no. 10. Helsinki, Finland, 2013.

100 For more on attribution of messaging, see: Thomas Elkjer Nissen (2012): Black and White and 256 Shades of Grey in Between – Reflections on the question of Attribution of Psychological Operations. RDDC Brief , March 2012. http://forsvaret.dk/FAK/ENG/PUBLICATIONS/Pages/default.aspx (Accessed 26 MAR 14).

101 http://en.wikipedia.org/wiki/Psychological_warfare (Accessed 25 MAR 14).

102 See also Sean Lawson: The US military's social media civil war: technology and antagonism in discourses of information-age conflict. In Cambridge Review of International Affairs, 07 MAR 2013. http://dx.doi.org/10.1080/09557571.2012.734787 and Thomas Elkjer Nissen (2011): Tactical Information Operations in Contemporary COIN Campaigns. RDDC Research Paper, September 2011. http://forsvaret.dk/FAK/ENG/PUBLICATIONS/Pages/default.aspx for more on the debate on Influence versus Inform and the separation of Public Affairs and Information Operations (PsyWar).

103 David S. Alberts and Richard E. Hayes: Understanding Command and Control. The Command and Control Research Program (CCRP). www.dodccrp.org

104 NATO System Analysis and Studies (SAS) research project 050: Exploring New Command and Control Capabilities. Final Report, January 2006, pp. 5 – 7.

105 Ibid.

CHAPTER 5:

106 James Farwell and Darby Arakelian: A Better Syria Option: Cyber War. (Accessed 18 DEC 13): http://nationalinterest.org/commentary/better-syria-option-cyber-war-9003

107 Farwell and Arakelian.

108 Digital Native refers to the generation born into the digital era that therefore has a greater understanding of its concepts.

109 SecDev Group (2013g): Flash Note Syria – Syria's Hacker Wars, p. 1. Published online 8 October 2013. www.secdev.com (Accessed 4 APR 14).

110 "The Internet War", BBC News 16 April 1999, in Andrew Mackay and Steve Tatham, Behavioural Conflict – Why understanding people and their motivations will provide decisive in future conflict. Military Studies Press, Essex, United Kingdom, 2011, p. 32.

111 Christopher Burnett, 2000, quoted in: Kilcullen, David: Out of the Mountains – The Coming Age of the Urban Guerrilla. Oxford University Press, 2013. P. 169.

112 Jens Ringsmose, Den medie-militære relation mellem kontinuitet og nybrud. In International Politik, volume 71, no. 2, 2013, (pp. 149 – 173). P. 158.

113 See Dennis Murphy: Fighting Back: New Media and Military Operations, Center for Strategic Leadership, United States Army War College, November 2008.
114 Niel Verrall: #gamechanger @MilitarySocialMedia, summer 2014 edition of IO Sphere http://home.iosphere.org/?page_id=11466, pp. 1 – 2. (Accessed 13 JAN 15)
115 William B. Caldwell, Dennis M. Murphy and Anton Menning: Learning to Leverage New Media – The Israeli Defense Forces in Recent Conflicts. In Military Review, May – June 2009. (Pp. 2 – 10). P. 4.
116 The case study is based on Deirdre Collings and Rafal Rohozinski: Bullets and Blogs – New Media and the Warfighter. US Army War College, Carlisle Barracks, Pennsylvania, USA, 2009. Pp. ix and 1 – 15. And Thomas Elkjer Nissen (2013b): The Ever Changing Narrative of Conflict – How the Role of War Narratives Changes from Mobilizing for the Battle of Perceptions to Influencing History. Pp. 73 – 83, in Democracy Managers. (Ed. Carsten Jensen) Published by the Royal Danish Defence College, June 2013, pp. 80 – 81.
117 Dara Kerr: How Israel and Hamas Weaponized Social Media. www.cnet.com, 13 January 2014. (Accessed 03 APR 14)
118 Caldwell, Murphy and Menning, 2009, p. 6.
119 Lev Grossman: Iran Protests: Twitter, the Medium of the Movement http://content.time.com/time/world/article/0,8599,1905125,00.html (Accessed 20 MAR 14)
120 Kilcullan, 2013, pp. 170 – 171.
121 Kilcullen, 2013, p. 192.
122 Philip Howard: The Digital Origins of Dictatorship and Democracy – Information Technology and Political Islam. Oxford University Press, New York, 2010.
123 John Pollock: People Power 2.0. – How Civilians Helped Win the Libyan Information War. In MIT Technology Review, April 20, 2012. Pp. 1 – 2.
124 http://www.guardian.co.uk/world/2011/jun/13/syrian-lesbian-blogger-tom-macmaster (Accessed 6 FEB 13):
125 Kilcullen, 2013, p. 218.
126 Howard Altman: Post-modern warfare – Tweets attempt to influence Centcom airstrikes. Tampa Bay Online. http://tbo.com/list/military-news/post-modern-warfare-tweets-attempt-to-influence-centcom-airstrikes-20140926/ (Accessed 13 JAN 15).
127 Sky News: US Centcom Twitter Account Hacked By IS. http://news.sky.com/story/1406621/us-centcom-twitter-account-hacked-by-is (Accessed 13 JAN 15).
128 SecDev Group (2013d): Backgrounder – The Hard Realities of Soft Power – Keeping Syrians Safe in a Wired War. Published on-line 25 June 2013. Pp. 1 – 2. www.secdev.com (Accessed 4 APR 14)

129 Farrell, Henry: Five key questions – and answers – about Iran's social media influence. In The Washington Post. December 17, 2013. http://www.washingtonpost.com/blogs/monkey-cage/wp/2013/12/17/five-key-questions-and-answers-about-irans-social-media-influence/ (Accessed 14 APR 14).

130 Spencer Ackerman: Voice of America Uses Social Media to Aid Foreign Dissent. February 15, 2011. http://www.wired.com/2011/02/voice-of-america-uses-social-media-to-aid-foreign-dissent/ (Accessed 15 APR14).

131 Citizen Global is a cloud-based multimedia platform that provides easy tools for citizens around the world to contribute to and engage with Voice of America's (VOA's) journalistic mission. (Source: http://www.bbg.gov/blog/2011/04/28/voa-and-citizen-global-elevating-voices-in-the-congo-around-the-world/ (Accessed 20 APR 14)).

132 Kerr, 2014, p. 7.

133 Kerr, 2014, p. 7.

134 SecDev Group (2013c): Flash Note Syria – Syrian Electronic Army Goes on the Offensive, Intensifies Targeting of Opposition Facebook Pages. P. 1. Published online 4 June 2013. www.secdev.com (Accessed 4 APR 14)

135 Caldwell, Murphy and Menning, 2009, p. 5.

136 Kilcullen, 2013, p. 180.

137 Doina Chiacu and Arshad Mohammed: Leaked audio reveals embarrassing U.S. exchange on Ukraine, EU. http://www.reuters.com/article/2014/02/07/us-usa-ukraine-tape-idUSBREA1601G20140207 (Accessed 13 JAN 15)

138 Ewen MacAskill: Ukraine crisis: bugged call reveals conspiracy theory about Kiev snipers. http://www.theguardian.com/world/2014/mar/05/ukraine-bugged-call-catherine-ashton-urmas-paet (Accessed 13 JAN 15).

139 Kilcullen, 2013, p. 220.

140 James Efaw: Social Networking Services – The New Influence Frontier. In: IOSphere, Winter 2009. P. 5. http://home.iosphere.org/?page_id=234 (Accessed 13 APR 14).

141 Catarina Nedertoft Jessen & Lotte Folke Kaarsholm: Diplomatiets digitale overmand. http://www.information.dk/493514 (Accessed 06 APR 14)

142 James Efaw, 2009, p. 4.

143 Quoted in: Caldwell, Murphy and Menning, 2009, p. 3.

144 Kerr, 2014, p. 6.

145 Kerr, 2014, p. 6.

146 Kerr, 2014, p. 6.

147 NATO Center of Excellence (CoE) for Strategic Communication (StratCom): http://www.stratcomcoe.org/~/media/SCCE/NATO_PETIJUMS_PUBLISKS_29_10.ashx (Accessed 13 JAN 15), p. 27.

148 SecDev Group: Syria Cyber Watch, p. 1. Published on-line 25 November 2012. www.secdev.com (Accessed 4 APR 14)
149 SecDev Group, 2012, p. 1.
150 Nick Fielding and Ian Cobain: Revealed – US spy operation that manipulates social media. In: The Guardian (UK), March 17, 2011 http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks (Accessed 14 APR 14).
151 ISAF = the NATO led "International Security Assistance Force" in Afghanistan (2002 – 2014).
152 Katie Robertson: Taliban using Facebook to lure Aussie soldier. In The Sunday Telegraph, September 9, 2012. http://www.news.com.au/national/nsw-act/taliban-using-Facebook-to-lure-aussie-soldier/story-fndo4bst-1226468094586 (Accessed 14 APR 14).
153 SecDev Group, 2013g, p. 4.
154 SecDev Group, 2013g, p. 2.
155 Mark Grdovic: Developing a Common Understanding of Unconventional Warfare. In Joint force Quarterly (JFQ), issue 57, 2d quarter 2010 (pp. 136 – 138). Published by National Defence University, NDU Press, USA. P. 136.
156 Ackerman, 2011.
157 SecDev Group, 2013c, p. 2.
158 SecDev Group, 2013e, p. 1.
159 Michael Terrazas: Four Telltale Signs of Propaganda on Twitter. May 31, 2012. http://www.scs.gatech.edu/content/four-telltale-signs-propaganda-twitter (Accessed 14 APR 14).
160 SecDev Group, 2012, p. 2.
161 DARPA http://www.darpa.mil/Our_Work/I2O/Programs/Social_Media_in_Strategic_Communication_(SMISC).aspx (Accessed 14 APR 14).
162 Kilcullen, 2013, p. 202.
163 William Mitchell: Project Kitae - Battlespace Agility in Helmand - Network vs. Hierarchy C2. 2012. http://forsvaret.dk/FAK/PUBLIKATIONER/RESEARCH%20PAPERS/Pages/Forsvarsakedemiet%20Working%20Papers.aspx#publication_b1399452-e6dd-4abb-b2e0-98633d9c089f (Accessed 03 APR 14)
164 See John Arquilla and David Ronfeldt: Swarming and the Future of Conflict. RAND,
165 The ICP contains the specific questions (Request for Information – RFI) or an organisation would like to have answered in order to conduct planning or revile an opponent or third parties intentions and capabilities.
166 http://www.thefreedictionary.com/weaponization (Accessed 18 MAR 14)
167 Quoted in: Kilcullen, 2013, pp. 206 – 207.

168 SecDev Group, 2013d, pp. 1 – 2.
169 Ibid
170 Ibid
171 Ibid + SecDev Group, 2013e, p. 1.
172 Kilcullen, 2013.
173 Kerr, 2014, p. 7.
174 Betz, 2012, p. 706.
175 Liff, 2012, p. 426.
176 Betz, 2012, p. 697.
177 Kerr, 2014, p. 7.
178 Collings & Rohozinski, 2009, p. ix.
179 SecDev Group, 2013d, p. 1.
180 Kerr, 2014, p. 8.
181 Kilcullen, 2013, p. 204.
182 SecDev Group (2013f): Flash Note Syria – Syria's National Defence Forces take the Battle to Cyberspace. Published on-line 30 September 2013. P. 1. www.secdev.com (Accessed 4 APR 14).
183 Kilcullen, 2013, p. 185.
184 Kilcullen, 2013, p. 188.
185 SecDev Group (2013b): Flash Note Syria – The Internet in Syria – Down, but not out. Published on-line 8 May 2013. Pp. 1 – 3. www.secdec.com (Accessed 4 APR 14).
186 Kilcullen, 2013, p. 190.
187 Kilcullen, 2013, p. 196.
188 Kilcullen, 2013, pp.220 – 221.
189 SecDev Group, 2012, p. 1.
190 SecDev Group (2013a): Flash Note Syria – Syrian Regime Tightens Access to Secure Online Communications. P. 2. Published on-line 23 April 2013. www.secdev.com (Accessed 4 APR 14).
191 http://www.todayszaman.com/news-343325-politicized-friday-prayer-sermon-supports-blocking-of-social-media-platforms.html (Accessed 31 MAR 14)
192 http://nyhederne.tv2.dk/udland/2014-04-03-tyrkiet-oph%C3%A6ver-twitter-forbud?nidk (Accessed 4 APR 14)
193 Spencer Ackerman: Taliban Texts Terror to Afghan Phones. March 17, 2011. http://www.wired.com/2011/03/taliban-texts-terror-to-afghan-phones/ (Accessed 15 APR 14).

CHAPTER 6:

194 Kilcullen, 2013, p. 187.

195 See http://twitter.com/tos
196 SecDev Group (2013a): Flash Note Syria – Syrian Regime Tightens Access to Secure Online Communications. P. 2. Published 23 April 2013. www.secdev.com (Accessed 4 APR 14).
197 SecDev Group, 2013d, p. 1.
198 Kerr, 2014, p. 7.
199 Spencer Ackerman Voice of America Uses Social Media to Aid Foreign Dissent. February 15, 2011. http://www.wired.com/2011/02/voice-of-america-uses-social-media-to-aid-foreign-dissent/ (Accessed 15 APR14).
200 See SecDev Group, 2013d, p. 2.
201 http://captology.stanford.edu/ (Accessed 13 APR 14)
202 http://www.amnesty.org/en/annual-report/2012/foreword (Accessed 20 JAN 15)
203 Kilcullen, 2013, p. 171.
204 Kilcullen, 2013, p. 172.
205 William Boothby: Conflict law – The Influence of New Weapons Technology, Human Rights and Emerging Actors. Asser Press, Springer, The Hauge, the Netherlands, 2014, p. 157.
206 Boothby, 2014, p. 176.
207 Charles J. Dunlap, Jr., Lawfare Today…and Tomorrow. In International Law and the Changing Character of War 315-325 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds.), US Naval War College International Law Studies, Vol. 87, 2011. P. 315)
208 SecDev Group (2013c): Flash Note Syria – Syrian Electronic Army Goes on the Offensive, Intensifies Targeting of Opposition Facebook Pages. Published on-line 4 June 2013. P. 1. www.secdev.com (Accessed 4 APR 14)
209 Kerr, 2014, p. 3.
210 Michael Pizzi: The Syrian Opposition Is Disappearing From Facebook. In The Atlantic.com, February 4, 2014. http://www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562/ (Accessed 15 APR 14).
211 Kerr, 2014, p. 3.
212 Nick Fielding and Ian Cobain: Revealed – US spy operation that manipulates social media. In: The Guardian (UK), March 17, 2011 http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks (Accessed 14 APR 14).

About the book:
In today's conflict environment, transformed by information technology and of who can communicate and how, states, non-state actors, ad hoc activist networks and individuals create effect(s) in and through social network media. #TheWeaponizationOfSocialMedia develops a framework to understand how social network media shapes global politics and contemporary conflicts by examining their role as a platform for conduction intelligence collection, targeting, cyber-operations, psychological warfare and command and control activities. Through these, the weaponization of social media shows both the possibilities and the limitations of social network media in contemporary conflicts and makes a contribution to theorizing and studying contemporary conflicts.

About the author:
Thomas Elkjer Nissen, MA, M.sc., has from 2001 worked at the Royal Danish Defence College (RDDC) as a Military Analyst responsible for Strategic Communication (StratCom), Cyber-Warfare, Information Operations (Info Ops) and Psychological Operations (PsyOps). In that capacity he conducts research, teaches and advises in the above fields of work. He has acted as course director and developer of courses and seminars at the RDDC as well as acted as high level advisor both nationally and within NATO. He has previously published a series of journal articles, book chapters and research papers on the topics. Resent works include writings on "Strategy and Strategic Communication", "Narrative Led Operations", "Islamic State´s Media Warfare" and "The Weaponization of Social Media"