ISBN 978-9934-8582-6-0

SOCIAL MEDIA AS A TOOL OF HYBRID WARFARE

PREPARED BY THE
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

ISBN 978-9934-8582-6-0

Project director
Sanda Svetoka

Editor
Anna Reynolds

Production & Copy Editor
Linda Curika

Riga, May 2016

NATO Strategic Communications
Centre of Excellence
Riga, Kalnciema iela 11b, Latvia LV1048
www.stratcomcoe.org
Ph.: 0037167335463
info@stratcomcoe.org

TABLE OF CONTENTS

FOREWORD

The development of information technology has changed the nature of conflicts by creating an additional layer of complexity to traditional battle spaces. Nearly global access to the virtual environment has created numerous opportunities to conduct battles online affecting events in both the physical domain, such as computer systems, and in the cognitive domain of people's attitudes and beliefs.

Recently we have witnessed how both states and non-state actors use hybrid approaches to pursue their political and military aims, skilfully combining military operations with cyber-attacks, diplomatic and/or economic pressure, and information (propaganda) campaigns. Over the past decade, social media has rapidly grown into one of the main channels of communication used today. Virtual communication platforms have become an integral part of warfare strategy. The recent conflicts in Libya, Syria, and Ukraine have demonstrated that social media is widely used to coordinate actions, collect information, and, most importantly, to influence the beliefs and attitudes of target audiences, even mobilise them for action.

Given this state of affairs, the NATO Strategic Communications Centre of Excellence (NATO StratCom COE) was tasked with looking into how state and non-state actors leverage social media as a tool for conflict and hybrid warfare strategies. The following topics will be addressed in the report:

- What is the role of social media in hybrid warfare? How is it 'weaponised'?
- What techniques and tactics do state and non-state actors employ to support their political and military aims using social media? What effects can they achieve?
- What can NATO and its member nations do to identify and counter the malicious use of social media?

We hope that this paper will serve as a comprehensive introduction and useful educational material for anyone interested in understanding the complexity of today's information environment, and specifically the techniques of influence used in the digital space.

The report summarises the conclusions of research commissioned by the StratCom COE—*Internet trolling as hybrid warfare tool: the case of Latvia* by the Latvian Institute of International Affairs (LIIA) in cooperation with Riga Stradiņš University,[1] *Social influence in Russia-Ukraine-conflict-related communication in social media* by a team of Polish researchers,[2] *Network of terror: how Daesh uses adaptive social networks to spread its message* by Joseph Shaheen, US State Department Fellow at the StratCom COE, as well as discussions from the seminars and conferences conducted by the COE over the course of 2015.

1 Authors: Prof Andris Sprūds (Latvian Institute of Foreign Affairs or LIFA), Ilvija Bruģe (LIFA), Mārtiņš Daugulis (LIFA), Dr Klāvs Sedlenieks (Riga Stradins University), Assoc prof Anda Rožukalne (Riga Stradins University), Diāna Potjomkina (LIFA), Beatrix Tölgyesi.

2 Authors: Dr Jan Zając (University of Warsaw, Faculty of Psychology), Julia Zając (Graduate School for Social Research, IFiS PAN), Dr Tomasz Grzyb (Opole University), Filip Cyprowski (Sotrender), Aleksander Zawalich (Sotrender).

The StratCom COE would like to thank Thomas Elkjer Nissen, Head of the StratCom Section of the Royal Danish Defence College, Dr Rebecca Goolsby, Project Officer at the US Office of Naval Research, Col (rtd) Ian Tunnicliffe, Director of Accordance Associates, Prof Aki-Mauri Huhtinen, Professor of Military Leadership and Management at the Finnish National Defence University, Prof Ben O'Loughlin, Professor of International Relations at the Royal Holloway University of London, Nik Gowing, Visiting Professor in War Studies at Kings College London, Assoc prof Cristina Archetti, Lecturer at the University of Oslo, as well as Mark Laity, Chief of Strategic Communications at NATO SHAPE, for valuable contributions to the social media related discussions organised by the StratCom COE.

1. THE NEW INFORMATION ENVIRONMENT AND THE ROLE OF SOCIAL MEDIA

The rapid development of technology has dramatically changed the information environment in which we live.[3] The opportunities provided by information technology allow anyone to film, edit, and share information, images, and videos in real time, whether or not traditional media outlets report on the events. This gives every individual the opportunity to become an information actor and potentially distribute messages to audiences of unlimited number and size around the world. The nature of mass communication has changed from being a 'single authority speaking and many listening' to a 'many speak to many' interaction, i.e. interactions between citizens who create the content themselves. Governments and traditional media are no longer the most important players in the information space; they now have to compete for their place amid all the other actors.

Certain features that characterise the new information environment should be mentioned:

- **Accessibility.** Aggregating and sharing information is easy with modern devices such as smartphones and

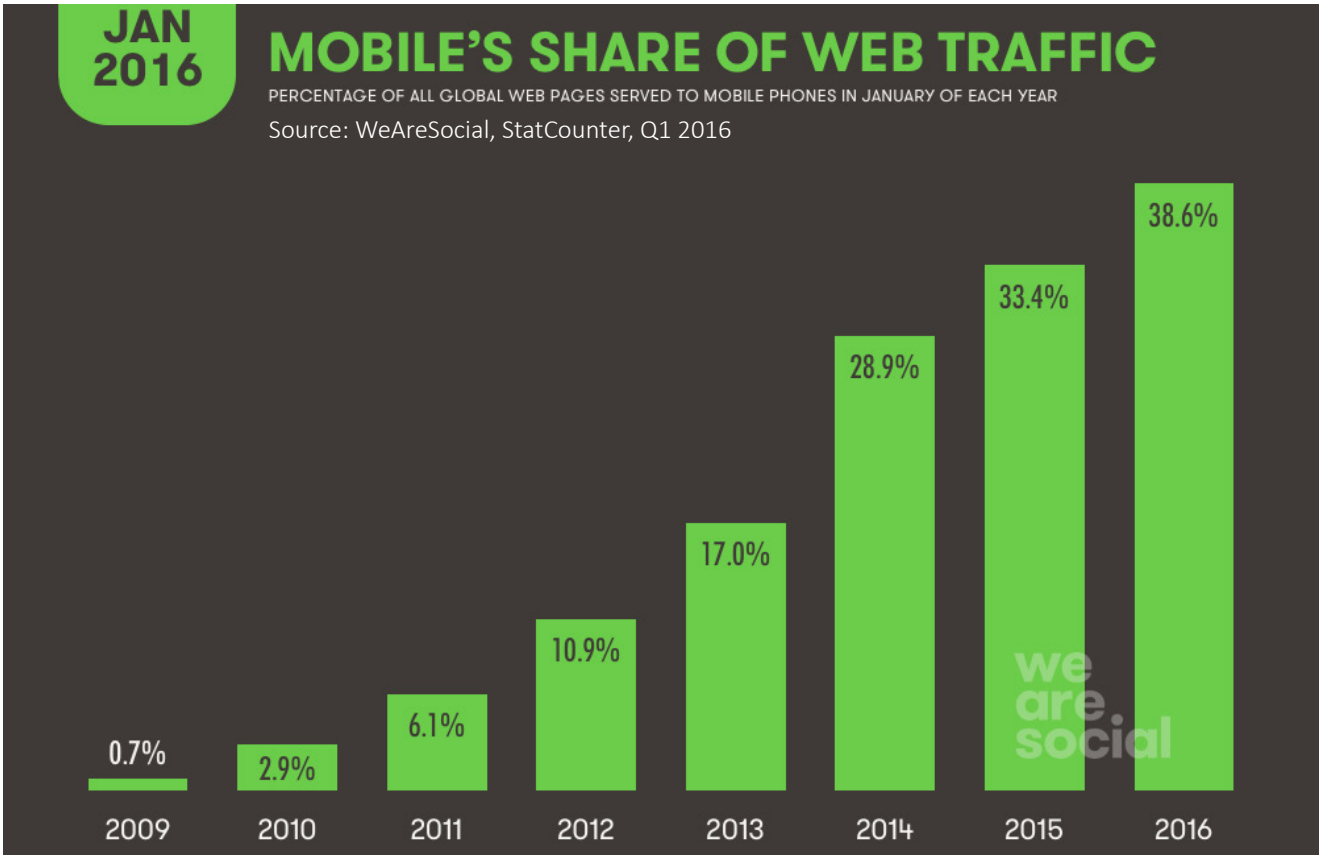
3 The NATO Military Policy for Information Operations, (MC 0422/5) 11 Feb 2015, defines the Information Environment as the environment that is comprised of the information itself, the individuals, organisations, and systems that receive, process, and convey information, and the cognitive, virtual, and physical space in which this occurs.

cameras that allow anyone to film, edit, and share information, almost in real time. Furthermore, these devices are relatively cheap and mobile networks are well developed, even in regions where income levels are low, so there are few barriers to using this technology to share information

- **Speed.** Social media provides the capability to spread information rapidly and in high volumes. Maximum impact can be achieved in a very short time. The new information environment is a contested environment in which all actors compete to be heard. Any hesitation results in others telling your story for you.
- **Anonymity.** Perceived Internet anonymity allows people to freely express opinions without taking responsibility. Anonymous users can manipulate audiences by fabricating visual and textual content, spreading fake information and rumours, or attack other participants of online discussions with impunity.
- **High volumes of information exchanged daily.** The amount of information that is exchanged worldwide on a daily basis can be compared to a wide river made up of many small tributaries. Some of this information is essential and may even be critically important for a wide audience (danger warnings, traffic information, etc.), while much of it may only be interesting for the closest friends and relatives of the social media user. The amount of information we face every day makes it difficult to track and differentiate between useful information and 'noise'.
- **No geographic or content-related borders.** Before the advent of social media one of the roles of the traditional media has always been to act as a 'gate keeper', advancing certain topics and shaping the discussion. This function is no longer exclusive to them; any post can reach the same number of people as a news article from a respected news organization. In this way, actors who would never get the chance to voice their opinions through traditional media outlets (e.g. minorities, radical groups, and extremists) can reach wide audiences through social media and thus magnify their capabilities.[4]

In January 2016 almost half (3, 4 billion) of the world's population was actively using the Internet, and 1/3 (or 2, 3 billion) of all people were using various social networking sites. Furthermore, the number of mobile social media users is growing by 12 users/second; the mobile phone is now the main way of accessing connected services, including the Internet, for the majority of individuals around the globe.[5] Social media increasingly shapes our perceptions and attitudes as more and more people are turning to social networking sites, such as Twitter and Facebook, to keep up with the news.[6]

4 NATO ACO Directive on Social Media, 16 September 2014.
5 Digital in 2016, special report by We are Social, http://wearesocial.com/uk/special-reports/digital-in-2016
6 Social Media Update 2014, http://www.pewinternet.org/2015/01/09/social-media-update-2014/; 'The Evolving Role of News on Twitter and Facebook' by Michael Barthel, Elisa Shearer, Jeffrey Gottfried, and Amy Mitchell, http://www.journalism.org/2015/07/14/the-evolving-role-of-news-on-twitter-and-facebook/



The Multinational Capability Development Campaign (MCDC) defines social media as 'internet based platforms and software used to collect, store, aggregate, share, process, discuss or deliver user-generated and general media content, that can influence awareness, perception, and acceptance and can promote behaviour indirectly as a means of interaction'.[7]

The NATO Allied Command Operations (ACO) Directive defines social media as 'web-based technologies used for social interaction and to transform and broadcast media monologues into interactives, social dialogues'.[8]

Some Types of Social Media:

Social networks – Facebook, Myspace, Linkedin

Visual social networks – Instagram, Snapchat, Periscope

Blogs – Wordpress, Blogspot, Livejournal

Microblogging – Twitter, Tumblr

Content communities – Youtube, Vimeo, Flickr

Instant messaging – Skype, Messenger, Whatsapp, Telegram

Location based services – Foursquare

Online gaming – World of Warcraft

Music sharing – Spotify

7 NATO ACO Directive on Social Media, 16 September 2014.

8 Multinational Capability Development Campaign (MCDC) Concept of Employment Social Media in Ssupport of Situation Awarness, 2014.

Different social media platforms are used for different purposes. For example, *Facebook* (the most popular social networking site worldwide) is mainly used for networking with friends and relatives; the microblogging site Twitter provides a rapid exchange of short messages; and various chat platforms allow for the exchange of information, images, and videos within a closed network. A growing number of platforms provide opportunities for collaborative efforts where people share their knowledge and work such as *Prezi*, *Slideshare*, *Endomondo*, and others.

These social media platforms offer unprecedented opportunities for people to connect with their friends and others with similar interests or agendas, to share their experiences and opinions, to follow their friends' activities, and receive information (sports, culture, news, etc.), express themselves (report on their daily life activities, share photos/videos), and much more.[9]

This has brought a number of **positive effects**—we can now mobilize people to help one another and raise funds for social causes, investigate crimes, and provide greater assistance to humanitarian disaster relief efforts. It has also increased the level of transparency within governments as well as the ability of the people to engage in the decision-making process, uncover lies and false information, as well as find support for their ideas. Social media is a significant driver towards more open and direct dialogue among different social groups.

However, the same environment that offers so many great opportunities can also cause **negative effects**. The openness and engagement that form the basic principles of social networking can also expose the vulnerabilities of its users. Furthermore, the virtual environment is an unregulated environment in which anonymity provides more opportunities than ever to disseminate extreme views, deliberate misinformation, and create hoaxes without revealing the person or organisation behind the creation of the content. As David Stupples puts it, the great level of connectedness that populations have today is a strength, but being instantly connected means that misinformation and fear can also spread rapidly, resulting in panic.[10]

Therefore, social media, which is made up of a multitude of trust-based networks, provides fertile ground for the dissemination of propaganda and disinformation, and the manipulation of our perceptions and beliefs. Because of the potential effects social media activities can cause with little cost or effort, it has become an essential tool for warfighting used by both states and terrorist groups. Methods used to shape the opinions of populations are becoming even more sophisticated since the rapid advancement of this form of communication in the 2000s. These methods will be discussed in more detail in the next chapters.

9 'Social Networking Motivations', Global Web Index Insight Report 2015, http://www.globalwebindex.net/blog/top-10-reasons-for-using-social-media

10 David Stupples, 'The next big war will be digital and we are not ready for it', The Conversation, November 26, 2015, https://theconversation.com/the-next-war-will-be-an-information-war-and-were-not-ready-for-it-51218

2. THE CONCEPT OF HYBRID WARFARE

Concepts such as 'unconventional', 'asymmetric', 'irregular', 'hybrid', or 'new generation warfare' are often used in political and academic debates to describe the complexity and characteristics of modern conflicts in which both state and non-state actors combine conventional methods with methods that lie outside of our traditional understanding of military operation in their warfighting strategies.

The term 'hybrid warfare' first appeared in 2002 in a thesis by William J. Nemeth describing the way Chechen insurgents combined guerrilla warfare with modern military tactics and the use of mobile and Internet technology. In addition to their highly flexible operational tactics, the Chechens also used information activities and psychological operations against the Russian forces.[11]

The term 'hybrid warfare' was primarily used to refer to the strategies of non-state actors, such as the terrorist organisation Hezbollah, but it gained new momentum after the Russian operations in Crimea and Eastern Ukraine in 2014 that seemed to follow a script very much in line with General Valery Gerasimov's 2013 doctrine of 'non-linear war'.[12]

The doctrine outlined following activities:

- war is not declared at all, military action starts with the activities of militant groups during peacetime
- non-contact clashes between highly manoeuvrable fighting groups are used
- an enemy's military and economic resources are annihilated by means of precise strikes on strategic military and civilian infrastructure
- massive use of high-precision weapons and special operations, robotics, and weapons that use new physical principles (e.g. direct-energy weapons such as lasers, shortwave radiation, etc.) the use of armed civilians (4 civilians to 1 military)
- simultaneous strikes on enemy troops and facilities in an entire territory
- simultaneous battles on land, in the air, at sea, and in the information space
- the use of asymmetric and indirect methods
- troop management in a unified information sphere.[13]

Russia's hybrid warfare is not concentrated solely on the battlefield or in the theatre of operations; instead, the main emphasis has been on non-military methods that mitigate the necessity for armed confrontation.[14]

11 Andras Racz, 'Russia's Hybrid War in Ukraine: Breaking Enemy's Ability to Resist', FIIA Report 43, 2015, p.28, http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ukraine/

12 Nicu Popescu, 'Hybrid tactics: Russia and the West', EUISS, October 2015, http://www.iss.europa.eu/uploads/media/Alert_46_Hybrid_Russia.pdf

13 Jānis Bērziņš, 'Russia's new generation warfare in Ukraine: Implications for Latvian defense policy', Policy Paper No 2, 2014, p.4, http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx

14 Andras Racz, 'Russia's Hybrid War in Ukraine: Breaking Enemy's Ability to Resist', FIIA Report 43, 2015, p.43

The concept 'hybrid warfare' has been criticized as being neither new nor providing an additional explanation of modern warfare. As Damien Van Puyveld argues, 'any threat can be hybrid as long as it is not limited to a single form and dimension of warfare. When any threat or use of force is defined as hybrid, the term loses its value and causes confusion instead of clarifying the 'reality' of modern warfare'.[15]

Despite the lack of a unified definition, 'hybrid warfare' can be characterized as a form of warfare, which comprises a mix of methods—conventional and unconventional, military and non-military, overt and covert actions involving cyber and information warfare 'aimed at creating confusion and ambiguity on the nature, the origin and the objective of these actions'.[16]

One can argue that the non-military methods, including information operations, have always been used in times of war.

However, what makes modern warfare so different is the effects the information can cause to the development of the conflict, as audience perception of the outcome of the conflict matters more than the actual facts on the ground. The technological ability we now have to follow actions, almost without geographical limitations, makes the involvement of global audiences in the conflict even more significant. Domestic, diaspora, and foreign audiences now can interact with events in a real time as they follow online news sources and connect through social media.

Thereby the fight over control people's perceptions and behaviour has become an integral part of modern conflicts. As David Stupples predicts, 'information warfare that integrates electronic warfare, cyberwarfare, and psychological operations (PSYOPS) into a single fighting organisation will be central to all warfare in the future'.[17]

2.1. THE ROLE OF CYBERSPACE IN HYBRID WARFARE

Cyberspace (of which social media is a part) is often used in conflicts to take out the communications systems of the adversary. And discussions about cyber warfare are usually limited to the computerised systems that help run our daily lives and businesses, sustain critical infrastructure, financial transactions, supply electricity etc. As former White House advisor Richard Clarke writes, 'a cyber-attack can mean that these vital systems go down and we see exploding oil refineries, derailing trains, runaway satellites, food shortages, and much more'.[18] The disruption or breakdown of network and computer systems can have dramatic effects, however targeted narrative-driven operations can achieve results no less impressive than attacks on critical infrastructure.[19]

15 Daniel Van Puyveld, 'Hybrid war – does it even exist?', 2015, http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/

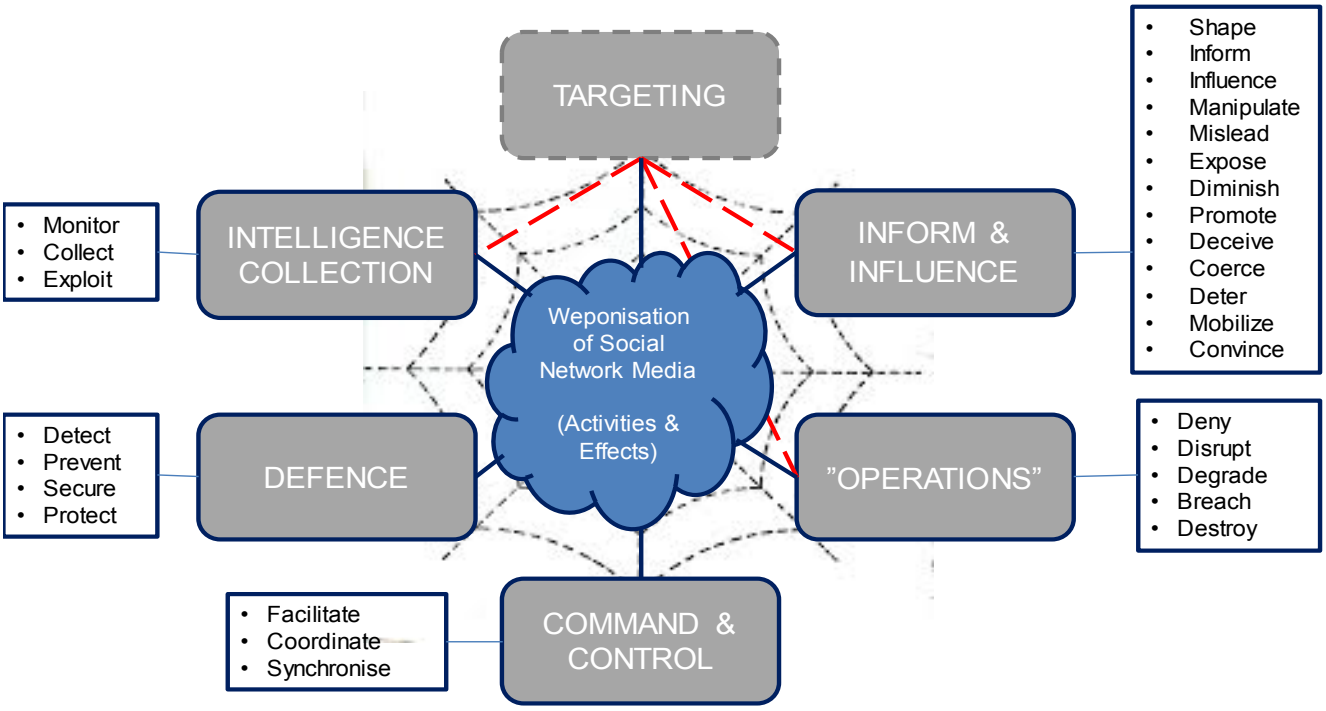
16 Jan Joel Andersson 'Hybrid operations: lessons from the past', EUISS, October 2015, http://www.iss.europa.eu/uploads/media/Brief_33_Hybrid_operations.pdf

17 David Stupples. 'The next big war'.

18 Richard A. Clarke & Robert Knake. Cyber War: The Next Threat to National Security and What to Do About It, New York: HarperCollins, 2011.

19 Elina Lange-Ionatamishvili and Sanda Svetoka, 'Strategic Communications and Social Media in the Russia-Ukraine Conflict' in Kenneth Geers (ed.) Cyber War in Perspective: Analysis from the Crisis in Ukraine, 2015, p. 94

Figure 1. Activities and effects framework by T. E. Nissen



Robert Brose discusses the developments of cyber war and the so-called 'netwar' foreseen more than 20 years ago as two emergent forms of warfare. Cyber war refers to the disruption of information and communication systems, whereas actors in a netwar overtly and covertly seek to 'disrupt, damage, or modify what a target population knows or thinks it knows about the world around it'.[20]

To conclude—the lines between cyber and information warfare are becoming increasingly blurred, and, especially with the rapid growth of social media platforms, cyberspace activities can be used not only to disrupt physical information systems, but also to influence the attitudes and behaviours to achieve certain political or military goals. By conducting activities that can have the effects on both physical and cognitive space even more impressive results can be achieved.

The Russian-Ukrainian conflict has demonstrated how cyber-attacks are used not only to disrupt technical systems, but also how they can psychologically influence audiences. Even minor, unsophisticated attacks supported by information activities can generate significant public and media attention, and highlight the weaknesses and insecurities of the adversary.

For example, the hacker group *b0ltai.org* leaked the hacked e-mail correspondence of the 'Internet Research Agency' in St. Petersburg to prove that the agency was, in fact, a 'troll farm' connected with the Kremlin. Another example is the leaked phone conversations between US and EU government officials regarding Ukraine that were later spread on social

20 Robert Brose, 'Cyberwar, Netwar and the Future of Cyberdefence', Office of Director of National Intelligence. United States of America, 11 June 2015, http://www.dni.gov/index.php/newsroom/ic-in-the-news/211-ic-n-the-news-2015/1205-cyber-war,-netwar,-and-the-future-of-cyberdefense

media.[21] This can be seen both as an attempt to make a point about the weak security systems safeguarding Western governmental communication lines, to discredit Western leaders and divide them, but also to influence and deceive the public by using social media.

Just few days before the Ukrainian parliamentary elections, electronic advertising billboards in the centre of Kyiv were hacked by the activist group 'Cyber Berkut'. The billboards displayed a video accusing Ukrainian government leaders and politicians of war crimes and showed graphic images of civilians killed in Eastern Ukraine. The announcement about the attack was posted on the activist group's *VKontakte* page.[22]

When discussing the role of social media it is often referred to as a part of cyberspace, however it is difficult to distinguish when one is talking about social media as a communication platform (technical tools/ information systems) and when one is referring to the interactions among information actors who are creating content (the information itself). We would suggest that the term 'social media' encompasses both aspects—social media content that is disseminated or shared by means of technological social media platforms. Due its enormous capabilities in replicating information at high speeds and low costs, as well as the challenges to separating fact from manipulated fiction because of the difficulties in tracking the authenticity and sources of this information, social media can be used to achieve specific military effects as will be discussed in the next chapter.

21 Two conversations were leaked—one between **State Department Official** Victoria Nuland and the US Ambassador to Ukraine, and the other between EU Foreign Affairs Chief Catherine Ashton and Estonian Foreign Minister Urmas Paet.

22 The English translation of the post reads: 'We, Cyber Berkut, are planning to use all means available to protect the interests of Ukrainian citizens against the tyranny of the nationalists-marginals and the oligarch elite. Today we used tens of advertising billboards in Kyiv in order to remind the people of Ukraine about the pointlessness of farce elections. […] Today everyone must realize that the solution depends on the future of our country and the sooner we deal with the Neo-Nazi Government and its Deputies who are profiting from the current war, the sooner there will be peace and order in the country.' The post and video can be found here: http://vk.com/wall-67432779_14678

3. THE "WEAPONIZATION" OF SOCIAL MEDIA

From the first 'Internet wars' in Kosovo in 1999, the conflict between the Hezbollah and Israel, and the 'Arab Spring' in Northern Africa and the Middle East to the current conflicts in Syria and Ukraine, we have been able to witness how social media is being used to shape public opinion, mobilize supporters, coordinate military activities, and collect information for targeting purposes. It has increasingly become the 'weapon of choice' both for state and non-state actors.

Thomas Elkjer Nissen proposes six ways social media can be used to support military operations — **Intelligence Collection, Targeting, Inform and Influence (Psychological Warfare), Cyber Operations, Defence,** and **Command and Control.** All of these activities, regardless of whether they have online or offline effects, can be conducted through social networking media. These activities are mutually supportive and often can be conducted in concert with physical activities on the ground.[23]

Targeting—Using social media to identify potential targets for military actions in the physical domain (based on geo-tagged pictures or on-going conversations in social media), as well as to attack social media accounts by hacking or defacing them. For example, *Google Maps* and cell phones were used in Libya to map regime positions that were then passed on to NATO, which used the information to identify targets and engage them using air power.[24] Another kexample is an attack on a Daesh headquarters building made by the US Air Force; only twenty-two hours elapsed between starting to track Daesh social media posts to the completion of the operation.[25]

Intelligence Collection—The focused search for and analysis of information from social media networks and profiles, including content and conversations; these activities can be done either overtly or covertly. There are several approaches to analysing social media for intelligence collection (e.g. trend, network, sentiment, geo-, content, behavioural, systemic, and information analysis). All of these forms of analysis can contribute to target audience analysis (TAA), and support psychological warfare or the selection of targets for operations both on- and offline. Basically, social media makes it possible to get detailed information about networks, actors, and related communication thus helping any group to get a better understanding of the information environment and the situation of any target group without being physically present. If consistently studied, social media can be a useful source for situational awareness and even for identifying the 'early warning signals' of a future crisis.[26]

Certain challenges and limitations in social media analysis exist. There are legal and ethical considerations, such as privacy

23 Nissen, The Weaponization of Social Media, p. 72.

24 Ibid., p. 82

25 Walbert Castillo, 'Air Force Intel Uses ISIS 'moron' Post to Track Fighters', 5 June 2015, http://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/

26 Nissen, The Weaponization of Social Media, p. 62-64.

violations, 'noise' in the data stream that is difficult to differentiate from valuable information using automated tools, as well as the challenge of measuring the effect of online discussions on offline events. For example, the role of *Twitter* in the Arab Spring revolutions is often overstated. *Twitter* was a game changer, but the scope of the effects of *Twitter* use should be considered with caution. *Twitter* was helpful for disseminating messages and coordinating actions, however these revolutions would never have happen without the actual conditions on the ground.[27]

Crowdsourcing is increasingly used by media employees and activists such as civic journalists for fact-checking, unmasking disinformation, and identifying developments in a conflict.[28] It can be used not only for intelligence collection and analysis, but also as a tool in the information war, revealing facts by sharing crowdsourced information with the public. For example, a joint project run by the Atlantic Council and Bellingcat was able to track and provide evidence of the presence of Russian troops in Ukrainian territory simply by collecting information from social media profiles used by Russian soldiers, Google maps, images in the media, as well as information crowd-sourced from eyewitnesses.[29] With the help of open source investigation, including social media, this approach makes it possible to counter disinformation and offer valuable support for strategic communications needs.

Cyber Operations—targeting social media platforms and accounts to breach password-protected spaces, alter the content of a profile, or render a website completely unusable. Cyber operations can be offensive or defensive, however most social media cyber-ops are offensive in nature. They can include actions like Distributed Denial of Service (DDoS) attacks on websites, password hacking to gain access and expose the content of chat rooms, e-mails, or cell phones, altering content in social media accounts, or intrusion into databases in order to collect information.

All such activities are aimed at preventing other actors from using social media platforms to communicate, coordinate actions, access information, or distribute messages, at least temporarily.[30]

For example, in the beginning of January 2015 a hacker using the name 'CyberCaliphate' and claiming to be connected to Daesh used the *Twitter* page of the Albuquerque Journal to post addresses, phone numbers, arrest records, and other sensitive personal information

27 '#gamechanger@MilitarySocialMedia', Dr Niel Verall (DSTL UK), IOsphere, 2014.

28 Crowdsourcing—the process of obtaining needed services, ideas, or content by soliciting contributions from a large group of people, and especially from an online community, rather than from traditional employees or suppliers; a portmanteau of 'crowd' and 'outsourcing,' its more specific definitions are yet heavily debated. By definition, crowdsourcing combines the efforts of numerous self-identified volunteers or part-time workers, where each contributor, acting on their own initiative, adds a small contribution that combines with those of others to achieve a greater result; hence, it is distinguished from outsourcing in that the work comes from an undefined public, rather than being commissioned from a specific, named group. https://en.wikipedia.org/wiki/Crowdsourcing

29 Maksymilan Czuperski, Eliot Higgins, et al., 'Hiding in Plain Sight: Putin's War in Ukraine, Atlantic Council', October 2015, http://www.atlanticcouncil.org/publications/reports/hiding-in-plain-sight-putin-s-war-in-ukraine-and-boris-nemtsov-s-putin-war

30 Nissen, The Weaponization of Social Media, p. 65-66

stolen from various databases.[31] Later the same month CyberCaliphate managed to attack the *Twitter* account of the US Central Command (CENTCOM) and send threatening messages to US soldiers. Some internal documents also appeared on CENTCOM's public *Twitter* feed. One *Twitter* message read: 'American soldiers, we are coming, watch your back.'[32] Although the attack did not reveal any classified documents, the effect was psychologically disturbing and served as a warning that terrorists will not hesitate to use poorly-guarded servers and other easy targets like social media for their informational attacks.

Cyber operations that take place through social media can also create tangible real life consequences. For example, the hacker group of the Syrian Electronic Army attacked the *Twitte*r account of the Associated Press news agency, publishing a false tweet claiming that the White House had been bombed and the US president was injured. This tweet resulted in a 1, 365 billion US$ dip in the S&P 500 index within three minutes.[33]

Command and Control—using social media for internal communication, information sharing, coordination, and synchronization of actions. The use of social media for Command and Control (C2) purposes is important for non-state actors such as insurgent groups, particularly if these groups lack formal structure or are dispersed over large geographical areas; social media can provide a means of communication and a way to coordinate their activities. However the use of social media exposes the activities of insurgent groups to intelligence services.[34]

Such 'open', social media based, command and control arrangements makes it difficult for conventional armed forces to attack the C2 networks of non-state actors; there are no centralized networks, nodes, or physical targets to attack. Any attack would be associated with a variety of legal issues, since the infrastructure and platforms are not military.

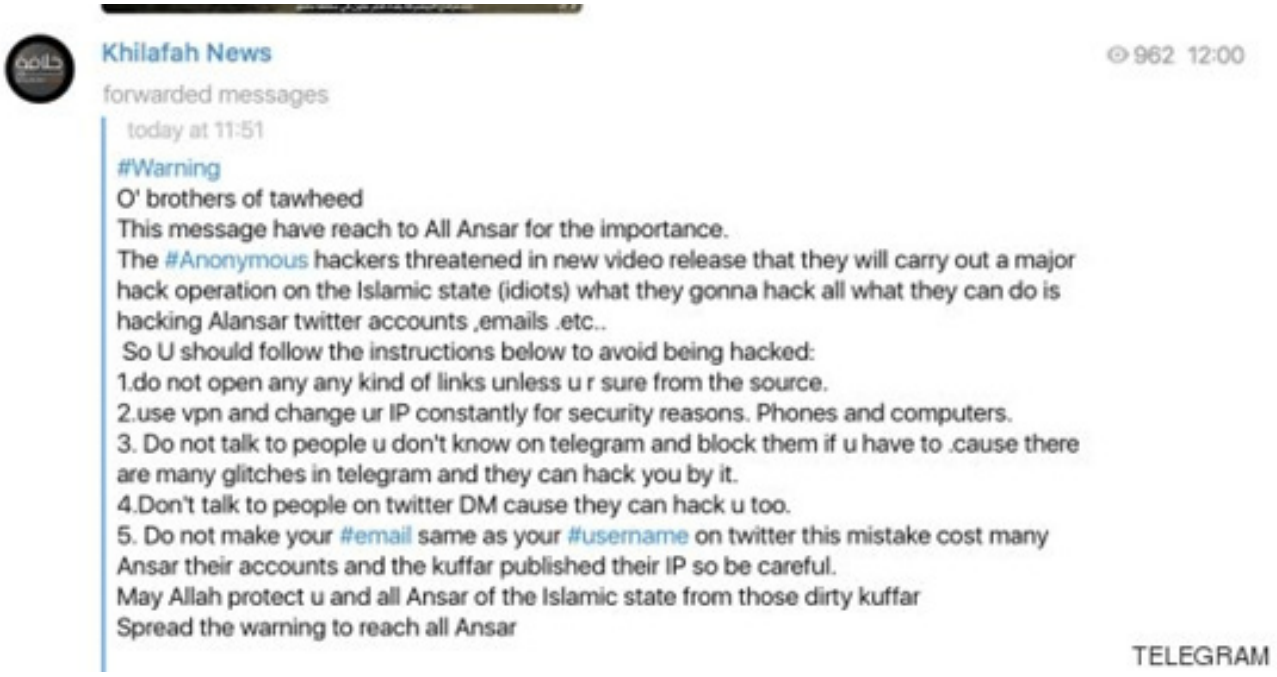
Social media can be used also for 'swarming' tactics—the distribution of information to mobilize and coordinate non-state actors with a common interest to engage with a specific target. By using social media, actors are able to gather quickly for protests giving security

31 Armin Rosen, 'A self-proclaimed ISIS fan is hacking local news outlets', 6 January 2015, http://www.businessinsider.com/a-self-proclaimed-isis-fan-is-hacking-local-news-outlets-2015-1

32 'US Centcom Twitter account hacked by pro-IS group', 12 January 2015, http://www.bbc.com/news/world-us-canada-30785232

33 Peter Foster, ''Bogus' AP tweet about explosion at the White House wipes billions off US markets', 23 April 2013, http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html

34 Nissen, The Weaponization of Social Media, p. 71



institutions little or no time for to respond. This approach was used during the Arab Spring revolutions. The Iranian authorities have also allegedly used this technique as a counter-measure; a protest demonstration was organised through social media, but when the demonstrators showed up they were met by riot police and security agents.[35]

Due to the above-mentioned security issues, the terrorist organization Daesh conducts most of its C2 activities in 'closed' chat apps and through gaming networks,[36] however recent analysis by the NATO StratCom COE identified that some coordination is also taking place via more open platforms such as *Twitter*. According to the report, Daesh is adding geo-locations to its hashtags (e.g. 'State of Homs' or 'State of Raqqa'), which allows members to 'disseminate target information to specific regions and any independent actor to share information within their region using a combination of Islamic State hashtags as well as geographic keyword tagging'. At the same time the hashtag 'State of Twitter' is used to widely share *Twitter*-specific operations and tactical needs and events. Numerous examples of this hashtag being used to enlist sharing, tweeting, following, and spamming operations by Daesh members have been identified.[37]

Defence—the protection of social media platforms, sites, profiles and accounts at the technical or system level. Defensive activities can include the use of encryption, anti-tracking, and/or IP-concealing software in connection with social network media. A lack of appreciation of operational security (OPSEC) and lack of awareness about basic cyber-security have cost many rebels their lives, in particularly in Syria.[38] Given these conditions, it is no surprise that terrorist organisations are mainly using encrypted

35 Ibid., p. 94.
36 For example, Telegram, SnapChat, WhatsApp, etc.
37 Joseph Shaheen 'Network of Terror: How DAESH Uses Adaptive Social Networks to Spread its Message', 2015, p. 9-10, http://stratcomcoe.org/network-terror-how-daesh-uses-adaptive-social-networks-spread-its-message
38 Nissen, The Weaponization of Social Media, p. 90

chat platforms for communication and the further radicalization of their supporters. For example, *PlayStation* has been found to be one of the most challenging game platforms for law enforcement services to track.[39] Furthermore, Daesh has warned their members of the dangers of ignoring cyber-security and in December of 2014 issued an edict that forbade its fighters from turning on *Twitter's* geo-tagging function.[40] Daesh has also established an online help-desk and privacy manual that gives suggestions on how to ensure operational security in the virtual environment.[41]

Another example of defence in social media is related to the activities of the hacker group Anonymous to hack Daesh social media accounts as a response to the terrorist attacks in Paris. In order to protect their supporters, a message was distributed in the chat app Telegram, widely used by Daesh to communicate with supporters, providing five tips for precautionary measures to take to avoid being hacked.[42]

Inform and Influence (also 'Psychological Warfare' in Nissen)—refers to the dissemination of information to influence a target audience's values, belief system, perceptions, emotions, motivation, reasoning, and behaviour. The use of social media in this case would seek to achieve certain military effects in the cognitive domain—shape, inform, influence, manipulate, expose, diminish, promote, deceive, coerce, deter, mobilize, convince.[43]

The methods of influence used on social media can be **overt,** such as the creation of official accounts, channels, websites, comments by opinion leaders etc., or **covert**, such as fake identities, botnets, and trolling. They can be used in any combination for information operations in social media.

The understanding about use of different information and influence techniques varies among the different actors in a conflict. The NATO doctrine does not foresee the use of covert or clandestine operations to influence attitudes and behaviour of the audiences; furthermore, PSYOPS can be used only in military operation declared by the highest strategic decision making body, the North Atlantic Council.[44]. On the other hand, terrorist groups and undemocratic regimes often have different standards and impose no ethical or legal limitations on the use of influence activities, even covert ones; they do not always officially declare war, and the line between 'peacetime' and 'wartime' is blurred. Such covert operations have been demonstrated by Russian forces in recent operations against Ukraine when massive amounts of information, including

39 Lily Hay Newman, 'Intelligence Officials Have Named One More Enemy in the Paris Attacks: Encryption', http://www.slate.com/blogs/future_tense/2015/11/16/officials_say_digital_encryption_makes_anti_terrorism_efforts_more_difficult.html

40 Shaheen 'Network of Terror', p. 16.

41 'ISIS has a 'Jihadi Help Desk' and an Online Privacy Manual, Because Terrorists Need Tech Support Too', http://www.slate.com/blogs/future_tense/2015/11/19/terrorist_tech_support_isis_has_a_jihadi_help_desk_online_privacy_manual.html

42 'Islamic State issues anti-hacking guidelines after Anonymous threats', 17 November, 2015, http://www.telegraph.co.uk/technology/internet-security/12001420/Islamic-State-issues-anti-hacking-guidelines-after-Anonymous-threats.html

43 Nissen, The Weaponization of Social Media, p. 67

44 NATO defines Psychological Operations (PSYOPS) as 'planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives', AJP – 3.10.1, Allied Joint Doctrine for Psychological Operations, 2014.

propaganda, deception, and rumours, were disseminated online using 'fake profiles', 'social bots', and 'troll armies', or what Russian information warfare theorist Igor Panarin calls 'information special forces' ('infospecnaz').[45]

When discussing the different intentions of social media engagement, Dr Rebecca Goolsby talks about **'social cyber-attacks'**—deliberate and organised actions to spread rumours, hoaxes, and manipulative messages in the virtual environment aimed at raising the fear and panic. Since tracking the organisers and perpetrators of social cyber-attacks is complicated, they remain anonymous, hiding both real people and automated bot networks. Dr Goolsby describes the case in Assam, India in July 2012 when the distribution of fake images and text messages about attacks against the Muslim population resulted in a panicked mass exodus.[46]

The recent conflict in Ukraine is rife with examples of social cyber-attacks used to incite panic. For example, one day in June 2014 Pavel Astakhov, the Children's Ombudsman under the President of the Russian Federation, used his Instagram account to announce that more than 7,000 Ukrainian refugees had fled Ukraine and arrived in the Rostov Oblast in the previous 24 hours. According to him, the number had risen to 8,386 by the next day. Russian mass media reported these numbers, but the Rostov Governor's office contradicted them, reporting that the number of refugees did not exceed 712.[47]

Some other techniques that can be used for psychological influence and manipulation on social media include:

1) Increasing the visibility of the message:

- The use of **automatically generated content**, by **spamming** (e.g. '*Twitter*-bombs'—sending out thousands of similar messages at once) or **fake identities** (e.g. trolls, sock puppets, bots) in order to spread a message and minimize alternative voices.
- **Saturating the information environment**—the coordinated use of blogs, posts, articles etc. that are posted and reposted by opinion leaders, activists and fake personas.
- **Hijacking of trending hashtags[48]** on *Twitter* in order to increase the reach of a message or misdirect audiences. For example, Daesh has used hashtags with high national or international focus such as *#napaquake* (posts about the recent earthquake in Northern California) to post threatening images and messages against US[49] or *#WorldCup2014* to share pro-Daesh content in addition to using various

45 Jolanta Darczewska, 'The anatomy of Russian information warfare the Crimean operation, a case study', Point of View, Centre for Eastern Studies, Warsaw, May 2014., http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

46 Rebecca Goolsby. 'On Cybersecurity, Crowdsourcing and Social Cyber-Attack.' Washington: Wilson Center. U.S. Office of Naval Research, 2013., https://www.wilsoncenter.org/sites/default/files/127219170-On-Cybersecurity-Crowdsourcing-Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf

47 'Rostov officials refuted information about thousands of Ukrainian refugees', 6 June 2014, StopFake.org, accessed 27 June 2015, http://www.stopfake.org/en/rostov-officials-refuted-information-about-thousands-of-ukrainian-refugees/

48 A hashtag is a type of label or metadata tag used on social network and microblogging services, which makes it easier for users to find messages with a specific theme or content. Hashtags can be used to collect public opinion on events and ideas at the local, corporate, or world level. They are often used for social activism as well. https://en.wikipedia.org/wiki/Hashtag

49 Alexander Towbridge, 'ISIS swiping hashtags as part of propaganda efforts', CBS News, 26 August, 2014, http://www.cbsnews.com/news/isis-hijacks-unrelated-hashtags-in-attempt-to-spread-message

Daesh-specific hashtags as well.[50] The Russian Ministry of Foreign Affairs has also used this technique in its '*Twitter* war' with the US State Department over the Ukrainian crisis. On 27 March 2014 the US State Department announced a social media campaign *#UnitedforUkraine* in order to raise awareness about events in Ukraine. The Russian MFA used *#UnitedforUkraine* to post tweets with comments by Foreign Minister Sergey Lavrov. According to Radio Free Europe/Radio Liberty, no fewer than nine such tweets in two days were posted.[51]

2) Targeting and distracting the opponent:

- **Distribution of misinformation and rumours—**to publicise an opponent's alleged wrongdoing. Many examples of such actions can be taken from the conflict in Ukraine, when pro-Russian voices have systemically cultivated fear, anxiety, and hate among the ethnically Russian (and other non-Ukrainian populations) of Ukraine. They have manipulated and distributed images of purported atrocities by the Ukrainian army, including mass graves of tortured people, civilians used for organ trafficking, crop-burning to create famine, recruiting child soldiers, the use of heavy weapons against civilians, and acts of cannibalism.[52] On one occasion, terrified locals called the Donbas Water Company after social media informed them that the regional water supply had been poisoned.[53]
- **Attacking the target—**blocking adversary content or asking social media platforms to remove the content of specific profiles by complaining about inappropriate content to security. For example, *Facebook* administrators removed the picture of girl commemorating her father, a Ukrainian soldier who had fallen in Eastern Ukraine, after several pro-Russian social media users reported the post for containing graphic content.[54]

50 'How Isis used Twitter and the World Cup to spread its terror', 24 June 2014, http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/10923046/How-Isis-used-Twitter-and-the-World-Cup-to-spread-its-terror.html

51 Luke Johnson, 'Hashtag Hijacked: Russia Trolls U.S. Twitter Campaign In Ukraine Crisis', 25 April, 2014. Radio Free Europe, Radio Liberty, http://www.rferl.org/content/ukraine-us-russia-twitter-trolling/25362157.html

52 More can be found at StopFake.org, accessed 27 June 2015, http://www.stopfake.org/en/russia-s-top-100-lies-about-ukraine

53 Lily Hyde, 'Rumors and disinformation push Donetsk residents into wartime siege mentality,' 3 May, 2014, Kyiv Post, accessed 27 June 2014, http://www.kyivpost.com/content/ukraine-abroad/rumors-and-disinformation-push-donetsk-residents-into-wartime-siege-mentality-346131.html

54 'Ukrainians petition Facebook against 'Russian trolls'', 13 May 2015. BBC http://www.bbc.com/news/world-europe-32720965

- Targeting an opponent also involves any sort of personal attack, and can go so far as to **acquire personal information and use it to defame, ridicule, threaten** etc. as has been reported by opposition activists in Russia and social media users of other countries who have expressed their dislike of Kremlin policies. For example, Finnish journalist Jessikka Aro who has personally experienced and written extensively about Russia's troll attacks, described how trolls harassed her online, ironizing and jeering about her professional and personal life.[55]
- **Social engineering—**in the cyber context this refers to the psychological manipulation of people into performing actions or divulging confidential information.[56] Cyber criminals often use social engineering to discover information necessary for system access, fraud, or other attacks. However, these techniques can be also used for military purposes such as espionage and information gathering. Such attacks can be automated, i.e. conducted by bots, or carried out by humans with fake identities. An example of social engineering is the 'catfishing' of soldiers— the Taliban has used fake profiles of attractive women to make friends on *Facebook* with Australian soldiers and draw out information that can be later used for their operations.[57] Most of the soldiers did not recognise that people using fake profiles, perhaps masquerading as school friends, could capture their personal information and movements.[58]
- **Deception—**creating 'noise' or 'informational fog' around a topic in order to distract attention from more strategically important events. A significant example of this has been the case of the downing of Malaysian air flight MH17. Russian media channels and social media distributed a large volume of messages offering numerous explanations for why the plane crashed. Another bot campaign was used to distract the public by offering an 'alternative explanation' of the murder of Russian politician Boris Nemtsov, saying that he was killed by jealous Ukrainians. This 'news' was published just a few hours after the attack had happened.[59]

55 Jessikka Aro, Kioski Yle, 'My Year as a Pro-Russia Troll Magnet: International Shaming Campaign and an SMS from Dead Father', 9 October 2015, http://kioski.yle.fi/omat/my-year-as-a-pro-russia-troll-magnet

56 For more information see: https://en.wikipedia.org/wiki/Social_engineering_%28security%29 https://en.wikipedia.org/wiki/Social_engineering_(security)

57 'Taliban pose as women to friend soldiers on Facebook', 11 September 2012, http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/9535862/Taliban-pose-as-women-to-friend-soldiers-on-Facebook.html

58 Review of Social Media and Defence, Australian Department of Defence, 2011, http://www.defence.gov.au/pathwaytochange/docs/socialmedia/Review%20of%20Social%20Media%20and%20Defence%20Full%20report.pdf

59 Lawrence Alexander, 'Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign', 2 April 2015, https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/

4. CASE STUDIES

4.1. THE ROLE OF SOCIAL MEDIA IN RUSSIA'S INFORMATION ACTIVITIES

The Russian military operation against Ukraine, which resulted in the annexation of Crimea in March 2014 and the continuous warfare in Eastern Ukraine, provide a demonstration of Russia's new generation warfare approach in which traditional military tools were used alongside a well-orchestrated mix of information warfare, cyber-attacks, and diplomacy. The use of cyberspace, both in its technical and content-related aspects, show how Russian leaders have adapted to the new networked environment, putting strong emphasis on information and information control.[60]

Russia's ability to fight information warfare was well developed during the Soviet Era, when methods like 'active measures' and 'reflexive control' were used widely to undermine and intimidate its opponents in the West. These old methods have now been adjusted to the requirements of the new information environment. However, as Jolanta Darczewska puts it, these innovations primarily concern the organisation of activity within the network; since there is no civil society in Russia, this information 'spetsnaz' is formed by 'political technologists'[61] and internal 'opinion leaders'.[62] We can conclude that the methods currently in use are an imitation of grass-root actions and public opinion, however they are organised by and conducted under the control of government operatives.

INFORMATION AND CYBERSPACE IN STRATEGIC DOCUMENTS

There is a strongly held perception in Russian academic and political circles that their country is the target of an on-going information warfare campaign, significantly waged in cyberspace. Therefore, it seems a logical desire to define and safeguard the borders of Russian information space.[63] This is also well reflected in Russian strategic policy documents.

The role of the virtual environment has been acknowledged in several Russian policy documents. The *Russian Military Doctrine* from December 2014 highlights the extensive geopolitical threats that Russia is currently facing, as well as the new methods that the West is using against Russia. According to the document, these threats have forced Russia to react and create a new response strategy that consists of military and non-military measures and incorporates new,

60 Margarita Jaitner, Dr Peter A. Mattsson, 'Russian Information Warfare of 2014', 7th International Conference on Cyber Conflict: Architectures in Cyberspace, NATO CCD COE Publication, 2015, p. 48. https://ccdcoe.org/cycon/2015/proceedings/03_jaitner_mattsson.pdf

61 Political technology—a term mostly used in former Eastern bloc countries to describe highly developed political manipulation techniques. A more detailed explanation can be found here: https://www.opendemocracy.net/od-russia/andrew-wilson/political-technology-why-is-it-alive-and-flourishing-in-former-ussr

62 Jolanta Darczewska, 'The anatomy of Russian information warfare'p. 28.

63 Jaitner, Mattsson, 'Russian Information Warfare of 2014', p. 41.

non-traditional method.[64] The importance of information operations in contemporary conflicts is emphasised as one of the state's primary defence tools,[65] serving to protect the country from both external threats (e.g. actions contravening international law and regional stability, actions aimed at ousting legitimate regimes adjacent to Russia's borders, etc.) and internal threats (e.g. activities aimed at destabilising the ruling regime, informational activities targeting the general population with the intent to undermine patriotic and historic traditions or provoke inter-ethnic and social tensions, etc.).[66] The Doctrine concludes that the only efficient way to ensure information security is a 'joint [counter] effort by all Internet users, journalists, local authorities, civil society organisations etc.'[67]

An underpinning policy document prescribing Russia's approach to managing information space is the *Russian Information Security Doctrine,* last published in 2000.[68] The Russian Security Council has started work on the development of a new doctrine that would take into consideration the current situation. Russia will develop its means of information resistance and perform strategic deterrence in order to defend against current threats—secret services and NGOs controlled by Western countries, which use information and communication technologies to destabilize the political and social situation in the country. The newspaper *Kommersant* reported that Russian authorities will counter exploitation of the Internet, whether it be to disseminate ideas of national exclusiveness, undermine social and political stability, or call for the forced change of the constitutional system of the Russian Federation.[69]

Conceptual Insights into the Activities of the Russian Armed Forces in the Information Space, the 2011 Russian Cyber-Warfare Strategy, discusses a more active response to threats in the virtual environment.[70] According to the strategy, 'Upon escalation of a conflict in informational space and its entering a critical phase [the state] should use its rights to individual and collective defence and use any chosen methods and means that do not contradict universally recognized norms and principles of the international law.'[71] Most importantly, this document specifies that, in the interests of security, the state can deploy its forces and means of information security in the territory of other states.[72]

64 Jolanta Darczewska, 'The Devil is in the Details. Information Warfare in the Light of Russia's Military Doctrine', Point of View, Centre for Eastern Studies, Warsaw, May 2015, p. 9, http://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf

65 Darczewska, 'The Devil is in the Details', p. 10.

66 Военная доктрина Российской Федерации (утверждена Президентом Российской Федерации 25 декабря 2014 г., № Пр-2976), 25 December 2014, http://www.scrf.gov.ru/documents/18/129.html; .

67 Darczewska, 'The Devil is in the Details', p. 31.

68 Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895), 9 September 2000, http://www.scrf.gov.ru/documents/6/5.html

69 'Russian authorities feel threat from foreign media and the Internet', 10 October 2015. http://112.international/russia/russia-developed-the-new-doctrine-of-information-security-1099.html

70 'В России создана стратегия кибервойны', 11 March 2012, http://www.cnews.ru/news/top/?2012/03/11/480954

71 'Концептуальные взгляды на деятельность вооруженных сил российской федерации в нформационном пространстве', Ministry of Defence of the Russian Federation, 2011, http://www.km.ru/tekhnologii/2012/03/14/ministerstvo-oborony-rf/ministerstvo-oborony-rf-opublikovalo-strategiyu-kiber; 'МинОбороны РФ разработало стратегию кибервойны', 10 February 2012, http://lukatsky.blogspot.com/2012/02/blog-post_10.html

72 'Концептуальные взгляды на деятельность вооруженных сил российской федерации в нформационном пространстве', Ministry of Defence of the Russian Federation, 2011, http://www.km.ru/tekhnologii/2012/03/14/ministerstvo-oborony-rf/ministerstvo-oborony-rf-opublikovalo-strategiyu-kiber

As described above, official Russian policy documents take a strictly defensive position by constantly referring to threats to the Russian information environment coming from the US, NATO, and other Western powers. This defensive approach justifies the Kremlin's actions against perceived threats, both external and internal, by imposing more stringent control over the Internet and social media in the Russian Internet environment (*RuNet*)[73] and by simultaneously working to ensure Russian information superiority and spread the Kremlin's narrative worldwide by creating multi-language web news platforms and maintaining armies of 'cyber mercenaries'.

CONTROL OVER THE VIRTUAL ENVIRONMENT

The Internet has been widely exploited by bloggers and opponents of the Kremlin to communicate views that differ from the official narrative that dominates most Russian TV channels, radio, and printed media. However, since the Russian presidential elections of 2012 and the unrest in Ukraine, Russia has put considerable effort into putting restrictions on the virtual environment to silence the Kremlin's critics and limit their ability to express opinions differing from those offered by the state-controlled media.

A number of restrictive laws were adopted during 2014. For example, the *Blogger Registration Law* specifies that bloggers who have more than 3000 followers should register as a media outlet; it also specifies that the authorities have the right to access a user's information and that online information must be stored in Russian servers so that the government can access it. Another law adopted in early 2014 allows the government to block any website without explanation. The law was used to block the websites of opposition activists Alexey Navalny and Garry Kasparov.[74] The law on personal data storage that went into effect in September 2015 specifies that Internet service providers who handle Russian customer data are required to physically keep their servers on Russian soil, which allows security institutions to monitor their activities. This law also affects the operation of foreign social network sites such as *Facebook* and *Twitter.*[75]

These restrictions have real implications. According to a recent report by the Association of Internet Users, a Russian digital rights organization, the number of cases where Russian citizens' Internet freedom was limited increased 1.5-fold in 2014 (from 1832 instances in 2013 to 2951 in 2014). While the number of criminal cases filed concerning Internet activity actually dropped, more extra-legal administrative pressure on users was reported (e.g. unofficial threats, dismissal from work) and more restrictions on accessing certain kinds of content online.

The report also notes that punishment for extremism-related

73 RuNet (a portmanteau of 'Russian' and 'network')—refers to the sphere of Internet sites predominantly visited by Russian-speaking users. The term is used in different meanings though. It can refer both to the Internet in the territory of Russia, i.e. for Internet infrastructure which is subject of Russian law (mainly used by Government officials), as well as the one which is used by the Russian-speaking online community also outside Russia (in Ukraine, Belarus, Kazakhstan, Latvia, Israel, etc.).

74 'Russia enacts 'draconian' law for bloggers and online media', http://www.bbc.com/news/technology-28583669

75 'Law on Russian Personal Data Storage Goes Into Effect Today; Status of Social Media Uncertain', http://www.interpretermag.com/russia-update-september-1-2015/

crimes has become more severe. Charges of 'incitement to extremism', coupled with increasingly restrictive public assembly and unsanctioned protest regulations, considerably limit freedom of expression. Even retweeted image or republished post might cost a Russian citizen access to the Internet or even their freedom.[76] For example, in February 2013 police charged a member of one of Russia's smaller political parties with hate crime for republishing a satirical *LiveJournal* post by Lev Sharansky, an Internet personality notorious for his parodies and exaggerated political speech. In 2014 federal law enforcement officers arrested a philosophy professor at Moscow State University for reposting an article that discussed the possible overthrow of the Kremlin in an online forum. In 2014 a trial began in the Siberian city of Barnaul in which state prosecutors accused a political activist of 'liking' a photograph deemed extremist on a social network site.[77]

Apart from these legal restrictions, the Kremlin has engaged in a number of activities aimed at controlling the information environment, such as replacing the leadership the of largest Russian social network, *Vkontakte*,[78] blocking pro-Ukrainian groups in social media,[79] and requesting foreign social media platforms to block specific kinds of content. For example, *Twitter* has received multiple requests from Russian governmental agencies to remove content and close accounts. 1735 such requests were submitted in the second half of 2015—a twenty-five-fold increase compared with other periods.[80] These occurrences are representative of the Kremlin's fear that it is losing control of the information environment.

A MULTI-PLATFORM APPROACH TO ENSURE INFORMATION DOMINANCE

The report on Russia's information campaign against Ukraine published by the StratCom COE in 2014 identified strong coordination between the ideological base, traditional media, and a well-developed network of *Twitter* users.[81] The report analysed how the Kremlin effectively uses a cross-media communication approach, in which information is created by a social media user claiming to be an eye-witness of some significant event, that story is later taken over by Kremlin-controlled TV channels and pro-Kremlin webpages. And vice versa—the media stories created by news channels are distributed via social media are later on amplified by different social media accounts, many of them holding fake identities.

Other studies have also analysed coordination between several media channels that disseminate pro-Kremlin

76 'In Putin's Russia a Retweet can Lead to a Jail Term', 12 February 2015, Global Voices, https://globalvoices.org/2015/02/12/russia-repost-extremism-social-media-jail/

77 'Russia's bureaucracy's Race to Police the Web', Global Voices, 23 June 2014, https://globalvoices.org/2014/06/23/russia-bureaucracy-police-internet-censorship-law/

78 'Russia's VKontakte COE says he was fired, flees Russia', Reuters, 22 April, 2014. http://www.reuters.com/article/russia-vkontakte-ceo-idUSL6N0NE1HS20140422

79 'Russia blocks pro-Ukraine groups on social media', Mahsable, 3 March 2014. http://mashable.com/2014/03/03/russia-ukraine-internet/#svcJ3NB0q5qc

80 'Twitter reports massive increase in Russian Government's content removal requests', Global Voices, 6 March 2016. https://globalvoices.org/2016/03/06/twitter-reports-massive-increase-in-russian-governments-content-removal-requests/

81 Analysis of Russia's Information Campaign Against Ukraine, NATO StratCom COE, Riga, 2015, p. 25, http://stratcomcoe.org/analysis-russias-information-campaign-against-ukraine-1

content, including Russian news agencies, blogs, webpages (supportive experts, think tanks, NGO's, interest groups), and social media accounts. For example, social network analyst Lawrence Alexander has identified connections between several pro-Kremlin information channels, where the activities of Kremlin-sponsored bloggers and commentators are combined with the activities of social media bots.[82] He found that an extensive network of more than 17 000 *Twitter* users, previously identified as bots by other *Twitter* users, and are closely interconnected. Furthermore, he documented an increase in bot registration coinciding with the start of the Euromaidan protests in Ukraine in the fall and winter of 2013/2014 and subsequent armed uprisings by pro-Russian militants in Eastern Ukraine in early spring of 2014.[83]

Another study by L. Alexander reveals the interconnections between a number of webpages dedicated either to posting compromising material about Ukraine (such as whoswho.com.ua), discrediting Russian opposition activists (such as yapatriot.ru), or expressing an anti-US stance on the Syrian conflict (syriainform.com).[84]

Other efforts to create 'official' and semi-official information agencies concerned with the Ukrainian conflict also demonstrate how seriously Russia is taking the need to provide information leadership in the online environment. For example, as of March 2014 numerous webpages including novorus.info and novorossia.ru were registered to promote the idea of 'Novorossiya'. Similarly the 'official' websites of the People's Republics of Donetsk and Lugansk were registered even before these entities declared themselves.[85]

The Kremlin has also devoted a great deal of energy to ensure information dominance among non-Russian-speaking audiences. As technology advances, any actor's ability to reach international audiences grows dramatically. The international TV channel *RT* (previously *Russia Today*) and *Sputnik*, Russia's latest international media project, are both deeply integrated with social media.[86]

From 2005 to 2013 the Kremlin spent almost 2 billion USD on RT, which calls itself 'essentially an internet media company'. *RT* claims that its presence on *YouTube* is even higher than on TV, although this statistic may be overestimated due to RT's wish to present itself as one of the leading channels globally, as leaked documents reveal.[87]

Analysis by L. Alexander reveals how bots artificially inflate the retweet and favourite counts of tweets by means of links to articles from the Russian news agencies *RT, RIA Novosti*, and *LifeNews*, thus affecting *Twitter* search and trending topics results. Some of the bots are simply retweeting posts by news agencies; others are posting links to news stories.

82 A bot is a software program coded to spread information on all kinds of social media platforms and are often organised in the interconnected networks called 'botnets'.

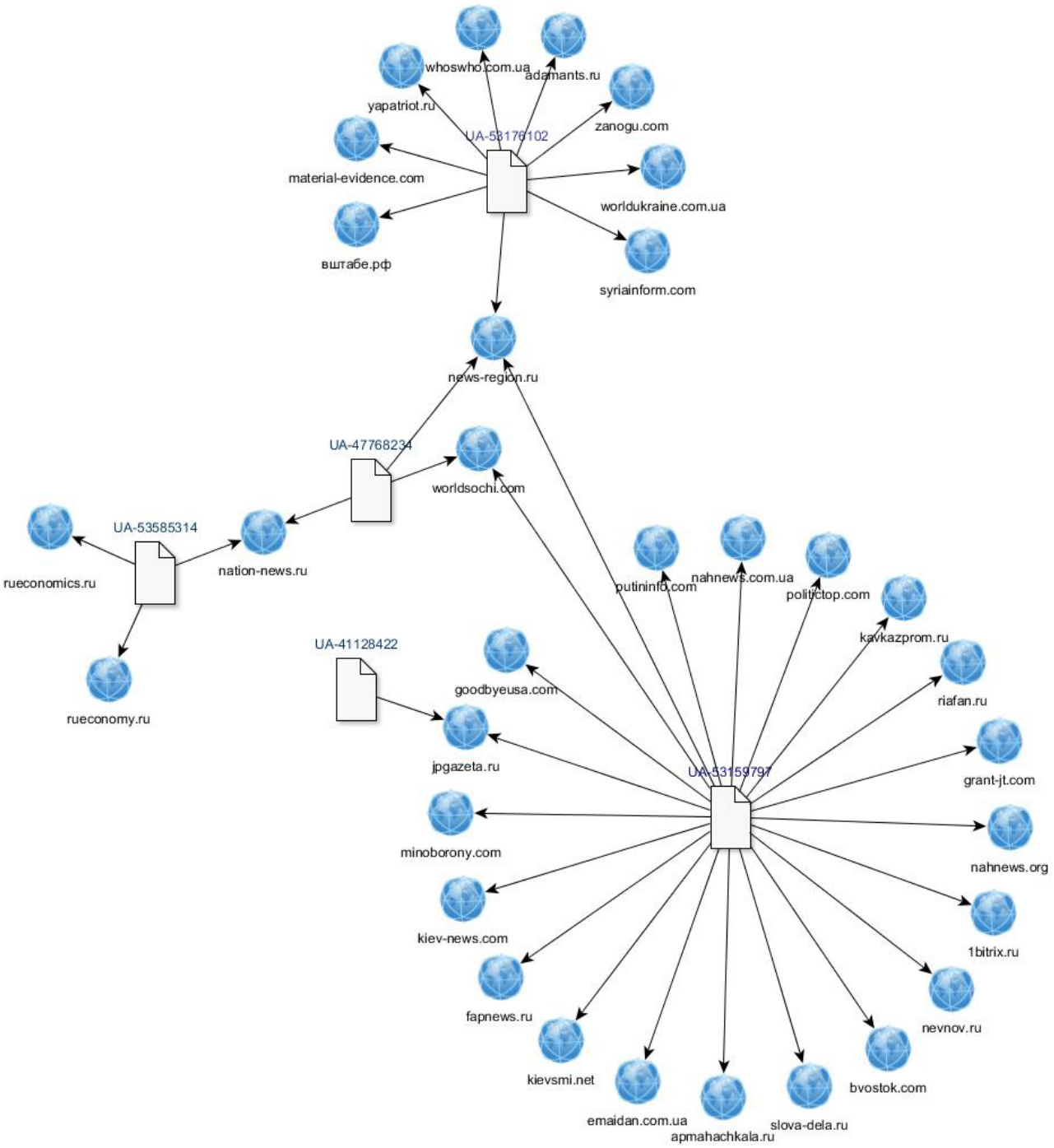
83 Lawrence Alexander, 'Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign', Global Voices, 2 April 2015. https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/

84 Lawrence Alexander, 'Open source information reveals pro-Kremlin web campaign', Global Voices, 13 July 2015, https://globalvoices.org/2015/07/13/open-source-information-reveals-pro-kremlin-web-campaign/

85 Jaitner, Mattsson, 'Russian Information Warfare of 2014', p. 46.

86 Ibid., p. 42

87 'Putin's propaganda TV lies about its popularity', The Daily Beast, 17 September 2015, http://www.thedailybeast.com/articles/2015/09/17/putin-s-propaganda-tv-lies-about-ratings.html



Relationships between the websites and their Google Analytics account numbers. Image by Lawrence Alexander. Source: https://globalvoices.org/2015/07/13/open-source-information-reveals-pro-kremlin-web-campaign/

The same fake accounts have mass-posted links to scores of pro-Kremlin *LiveJournal* blogs. Several thousand such blogs were identified.[88]

INTERNET TROLLING

Organizing activities by using fake identities in Internet and social media in order to achieve certain effects is not new. The phenomenon of imitating grass-roots actions using social media is known as 'astroturfing' and has been in use for some time. However, the Russian-Ukrainian conflict triggered the intensification of the discussion on how trolling can be used as a tool of influence in the conflict to manipulate people by spreading propaganda and rumours and distorting the online discussion by attacking commenters with alternative views.

Trolling has been recognised since late 1980s and early 1990s when USENET groups, forums, and bulletin boards suffered from 'flame wars' instigated through what was dubbed 'trolling', which was a new social behaviour at the time. Trolls commonly attempted to reveal hidden disagreements among community members by posing provocative question or posting extreme viewpoints on controversial topics. Sometimes trolls manipulate others into attacking them or encouraged community leaders to attack each other.[89] So, most researchers define trolling as deliberately provocative behaviour that aims to disrupt online discussions and cause conflict among participants. Trolls enjoy the attention and excitement of the conflict, and use deceptive, disruptive, and destructive behaviour for their own entertainment and with 'no apparent instrumental purpose'.[90]

However, research conducted by the NATO StratCom COE suggests a differentiation between the 'classic troll' as described above and the 'hybrid troll', who engages in the same patterns of behaviour as the traditional troll, but operates in the context of a particular political or military agenda.[91] The classic troll acts with no apparent instrumental purpose, whereas the hybrid troll, as the authors of the study have labelled paid pro-Russian trolls, communicates a particular ideology and, most importantly, operates under the direction and orders of a particular state or organisation.

Messages with pro-Russian content appeared in comment sections and social media exchanges in Russia and Ukraine and increasingly in the West as the crisis in Ukraine developed in 2014. The comments repeated the official Russian narrative, which was already widely disseminated in the

88 For more information see: 'Are Russian news media getting the boost from retweet bots on Twitter?', Global Voices, 27 November 2015, https://globalvoices.org/2015/11/27/are-russian-news-media-getting-a-boost-from-retweet-bots-on-twitter/ and 'Massive LiveJournal troll network pushes pro-Kremlin narratives', Global Voices, 22 December 2015, https://globalvoices.org/2015/12/22/massive-livejournal-troll-network-pushes-pro-kremlin-narratives/

89 Goolsby, 'On Cybersecurity, Crowdsourcing and Social Cyber-Attack'

90 Erin E. Buckels, Pauld D. Trapnell, Delroy L. Paulhus, 'Trolls just want to have fun', Elsevier, 2014, p. 97.

91 'Internet Trolling as Hybrid Warfare Tool: the case of Latvia', NATO StratCom Centre of Excellence, 2015, http://stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

Kremlin-controlled media—TV, radio, news outlets—supporting Russia's actions and aggressive posture against Ukraine, the USA, and the EU, as well as anybody else who offered an alternative interpretation of events.

The comments had a certain pattern—there were massive attack on the news articles, blog posts, and opinions each time events in Ukraine were mentioned. The unprecedented number of pro-Kremlin comments led researchers to believe that these activities were somehow synchronized. Reports on similarly unprecedented numbers of comments came from many countries (including Finland, Poland, Germany, the USA, the UK, and others). Information from previous employees of the Kremlin-sponsored 'Internet Research Agency' in St. Petersburg provided additional confirmation of these assumptions.[92]

The objectives and messages of these 'information warriors' can vary from country to country, depending on the vulnerabilities of specific target audiences. For example, according to Polish researchers (T. Grzyb et al.) who analysed social influence techniques related to the conflict in Ukraine on Ukrainian, Russian, and Polish social media sites, found that the communication strategies of suspected trolls vary:

- Trolls writing in Russian engage in discussions to calm participants, hide the truth about the state of the Russian economy, and to extol the virtues of the President and the government of Russia.
- Trolls writing in Ukrainian use their comments to disqualify and humiliate the President and the government of Ukraine by depicting their actions as hostile and neglectful, and by comparing them to fascists.
- Trolls writing in Polish strive to convince Internet users that the war in Ukraine is not the business of Poles. Some arguments concerning common history of Ukraine and Poland are raised in discussions so as to present Ukrainians in the worst possible light.[93]

The choice of influence techniques depends on the objectives the trolls want to achieve. However, when analysing discussions in Ukrainian, Polish, and Russian social media in the context of the Ukraine-Russia conflict, certain similar patterns were identified that were used to influence the participants of the discussion:

- **Aggression** against other participants (offensive slurs, attacks, including calling names, vulgarisms)
- **Labelling** (use of particular names and terms to evoke specific associations. For example, the same people can

92 For more information see: 'My life as a pro – Putin propagandist' in Russia's secret 'troll factory", The Telegraph, 25 June, 2015, http://www.telegraph.co.uk/news/worldnews/europe/russia/11656043/My-life-as-a-pro-Putin-propagandist-in-Russias-secret-troll-factory.html; Woman who sued pro-Russian "troll factory" gets one ruble in damages', August 18, 2015, The Guardian, http://www.theguardian.com/world/2015/aug/18/woman-who-sued-pro-putin-russian-troll-factory-gets-one-rouble-in-damages

93 The study 'Social influence in the Russia-Ukraine conflict related communication in social media' analysed social media (Facebook, Twitter, Youtube) profiles of the most popular news websites from Poland, Russia, and Ukraine (five news sites from each country). Nearly 4000 comments were analysed in the period of 1-30 April 2015. A quantitative analysis was conducted by using the social analysis tool Sotrender, whereas the qualitative analysis focused on the content of the most commented posts related to the conflict in Ukraine.

be defined as 'separatist groups', 'terrorists' and 'people's militia', but each of these terms leads to entirely different cognitive consequences)

- **Use of historical references** (for example, WW II).
- **Demonstrating civilization or moral superiority** (use of messages that demonstrate greater cultural and civilizational development – frequently associated with depreciation of the achievements of other nations)
- **Use of irony and sarcasm** (ironic phrases designed to mock behaviours, people or events, for example, 'of course, Ukrainians always want peace, just like they wanted to fight alongside Hitler'.)
- **Conspiracy theories**
- **Blaming others** (other countries) for creating conflict: suggesting that third parties (NATO, the EU, the US) generate conflicts to strengthen their international position.
- **Diverting discourse** to other problems: agreeing that the Ukraine-Russia conflict is not good, but that there are more important problems to solve, such as dealing with refugees, the budget, etc.
- **Slavic brotherhood:** emphasizing the commonalities of the Slavic people (Poles, Russians, and Ukrainians), rather than with EU/NATO cultures
- **Social Proof:** saying that 'everybody does it', 'many have already decided', etc. to highlight a particular solution or support for an idea (e.g. joining Crimea to Russia or support for separatist forces in the Donetsk and Lugansk regions)
- **'The biggest jerk in the neighbourhood':** depicting Russia with 'brutal honesty' as a country that can use its military might to break international law with impunity. (e.g. the *YouTube* video 'I'm the Russian occupant')
- **Dehumanization:** Ukrainians are shown as lacking in humanity (participating in brutal executions, particularly of children), violating all human norms and customs.
- **Data attacks:** presenting indigestible amounts of data—percentages, facts, and numbers—mostly without sources or verification saying that is confidential information from a trusted source, 'secret data', etc. (E.g. 'My friend works in the General Staff and said that 85% of the people drafted into the army run away and never show up.')[94]

For more details on the social influence techniques used, please **see Annex 2.**

The StratCom COE study *Internet trolling as a tool of warfare: the case of Latvia* suggests distinction between five main message templates used for creating comments. Although each type of trolling message targets a different audience, the styles overlap and can be used in combination.

94 'Social influence in the Russia-Ukraine conflict related communication in social media', 2015

- ***Blame the US conspiracy trolls*** disseminate information based on conspiracy theories and blaming the US for creating international turmoil. 'Conspiracy trolls' write long texts presenting logical arguments and unveiling the truth for readers. However, the logic of the messages inevitably breaks down and the end result is always the same—it is the fault of the US. Comment length is the first sign that this is a conspiracy troll.
- ***Bikini trolls*** post naïve, mostly anti-US comments typically accompanied by a profile picture of an attractive young girl. The content is simple, containing a question or/and a suggestion—'Could it be that only Russia is bad? The world doesn't work like that – maybe we should look…' which is then followed by a 'blame the US' motive. Despite the primitive message, the 'bikini troll' in fact significantly affects the Internet community as is often not recognised as a troll.
- ***Aggressive trolls*****,** similarly to classic trolls, post emotional and highly opinionated comments intended to stir up emotional responses from general users. Classic trolls are usually highly responsive, as they are interested in prolonging verbal conflict, whereas the responsiveness of the 'aggressive troll' is very low.
- ***Wikipedia trolls*** tend to post factual information from *Wikipedia* (or other authoritative information sources such as history blogs). The information posted is true *per se*, however it is used in a context that leads the audience to false conclusions and is unlikely to be discredited, even by more experienced users.
- ***Attachment trolls*** post very short messages with links to other news articles or videos containing value-laden information (for example, from Russian news platforms, TV news, eye-witness videos in *YouTube*, etc.). It is difficult to identify this troll, since its message is less human.[95]

The identification of a hybrid-troll is challenging though since, to some extent, it depends on the subjective judgment of the analyst.

It is much easier to identify information coming from automatically generated content that is spread by bot than it is to identify posts created by humans.[96] It is always possible to accuse someone of being a hybrid-troll, even if the account in question is not mobilized by any state or organization, but merely exhibiting classic attention-seeking troll behaviour.

It has been especially challenging to separate organised trolls from those who share their personal views in the Russian language commentary forums and web portals, where general discussion atmosphere is supportive to Kremlin's narrative. As Veronika Solovian, the administrator of the popular Finnish Russian website *russia.fi***,** admits that 'the trolls in this particular forum are commenting on political topics very

95 For more detailed description see: 'Internet Trolling as Tool of Hybrid Warfare: the case of Latvia'.

96 Some of its mains features are: very high number of tweets/comments/texts (which would not be possible by a human), account name usually consists of random numbers and letters or some known naming, it does not have many followers or several bots follow each other.

actively and always solely defending Putin and his policy. They are able to draw other participants into arguments, and others don't necessarily immediately identify them as trolls. It's extremely problematic that nobody can unambiguously identify or point out conversationalists distributing pro-Russia propaganda as paid writers. Some of them may be ordinary private citizens'.[97]

The criteria for identifying trolls in social media and web comments varies, however certain indicators could serve as the signals for the trolling:

1) The troll must have posted a large amount of comments.
2) The content of the comments must be consistently pro-Russian.
3) It must either post links to pro-Russian web-pages or large chunks of copy-pasted information from such pages.
4) It must be repetitive; reposting the same message multiple times rather than writing purpose-made comments that are content-specific (i.e., related to what other users are saying or making an original argument).
5) It generally does not engage in conversation with other users.
6) It does not comment on mundane and non-political topics unless the comments are political and pro-Russian.
7) When operating in languages other than Russian, it tends to be illiterate or having spelling mistakes.

These indicators alone do not confirm that the entity is in fact a troll. Extensive analysis of the troll's behaviour is necessary in order to acquire provable results. The simple trolling identification manual developed by the StratCom COE study could help Internet users with preliminary identification **(see Annex 1).**

THE USE OF TROLLING FOR CYBER ESPIONAGE

Trolling is used for psychological influence, but can also be used for conducting cyber operations with the purpose of intelligence collection. Recent findings by the Latvian **Information Technology Security Incident Response Institution** (CERT) show that pro-Russian trolls are using the comments sections of Latvian web portals to distribute propaganda and trick other participants into opening web links containing spying malware.[98]

A troll seemingly comments with an alternative opinion, saying 'it is nothing if compared with this…' or 'for more information, see here' together with a link to a Russian propaganda webpage infected by malware programmed to collect the data of its readers. CERT was able to confirm that these activities originated from the Russian hacker group 'TURLA', known to have connections to Russian intelligence services.

The case studies analysed by CERT showed certain common features of this trolling tactic—quick reaction time (no more than

97 'Yle Kioski Investigated: This is how pro-Russia trolls manipulate Finns online—check the list of forums favoured by propagandists', 24 June 2015, http://kioski.yle.fi/omat/troll-piece-2-english

98 The research findings were presented during the CERT.LV and ISACA Latvia annual IT security conference 'Cyberchess: strategy and tactics in the virtual environment', 1 October 2015.

30-60 minutes after the publication of an article), comments on topics related to Ukraine and Russia, and some particularly active accounts (the link to a specific infected webpage were included in half of the 3000 comments posted by one troll).

Although so far this technique has not been widely used in Latvia, it demonstrates a dangerous trend—trolling is used for psychological influence, as well as to distribute malware to gather information for intelligence purposes.

CONCLUSIONS ON THE EFFECTS OF RUSSIA'S INFORMATION ACTIVITIES ON SOCIAL MEDIA

As can be seen from the case study, social media can be a favourable environment for achieving desirable effects as described by T. E. Nissen, starting with defensive measures to the execution of techniques of psychological influence in order to shape the public opinion. However, are these effects achieved? Is it worth putting resources and effort into distributing thousands of messages through social media, even if they are shared only among other trolls/bots and do not reach out to wider audiences? Can they shape the opinions of intended target audiences?

One of the negative effects is the saturation of information space—the information distributed by botnet can affect social media trends and search engines results. This means that if a bot campaign is successful, every time somebody searches for information about Ukraine the first search results would include the comments or links that support Kremlin's narrative distributed by bots.

One of the most significant effects of the activities of trolls is the potential to **discourage people from participating in open debate on the Internet, leaving space for propaganda messages.** Catherine Fitzpatrick, who has documented Kremlin disinformation for *InterpreterMag.com*, argues that trolls inhibit informed debate by using crude dialogue to change the climate of discussion. 'You don't participate. It's a way of just driving discussion away completely. Those kinds of tactics are meant to stop democratic debate, and they work.'[99]

Trolling can also facilitate preventing the organization of alternative voices. When news organisations and social media sites face trolling activity they tend to block all commentary instead of trying to deal with the trolls. With no place to comment and discuss, people who share common sentiments have no idea whether they are alone or could connect up with others, and so the trolls achieve their aim. Their activity blocks the possibility for political opposition to develop before it can even productively form.[100]

An analysis conducted by the Finnish public broadcasting company web portal *yle.kioski* concluded that many Finns were forced to give up debating because of trolling, as they **did not see the use of fighting with masses of aggressive comments or threatening messages**.

99 'The Kremlin's Troll Army, Moscow is financing legions of pro-Russia Internet commenters. But how much do they matter?', The Atlantic, 12 August 2014, http://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/

100 Rebecca Goolsby. 'Information tactics and manoeuvres in the new information environment', NATO Science and Technology Organisation, p. 10.

Another effect found by the Finnish study was the **increasing confusion** about the events in Ukraine and **the diminishing the value of the truth.** Furthermore, the analysis showed a certain **emotional vulnerability**; Finnish people are not psychologically prepared for aggressive and cynical attacks that use extremely strong words, such as 'Nazi' and 'fascist', usually avoided in the West.[101]

The study conducted by the NATO StratCom COE analysed the comments of the three largest Latvian web portals, both in Latvian and Russian to learn about the effects of trolling on public opinion.[102]

Findings from the study did not provide proof of an extensive trolling presence in Latvian web portal comments; around 4% of all commented articles by trolls. Furthermore, the media consumption habits of the web portal users indicate that trolling should not be perceived as the most influential tool shaping opinion in Latvian society.

However, the study identified certain features about the vulnerability of the public to trolling messages:

- **The inability of certain segments of respondents to identify trolls**—seniors are the most vulnerable to trolling and have the lowest awareness of Internet security. In Latvia, 42% of 55- to 74-year-olds use the Internet, which makes them highly susceptible to the more aggressive cases of trolling. Another major risk group is the so-called homebodies (family men in their forties). This group is susceptible to conspiracy theories and is highly likely to respond to 'bikini troll' comments; they are also the most likely group to engage in commenting activities per se. Homebodies themselves typically comprise a large percentage of anonymous online commentators. Therefore the most efficient mechanism in this case would be decreasing the anonymity of Internet media. The other social groups studied were found to be highly resistant to hybrid-trolling attempts, albeit to different extents. The reasons for such resistance ranged from users having a highly critical approach to publicly available information and high Internet literacy, to disinterest in the political process.
- **Aggression online leads to aggression offline**—real life consequences of online discussions are a significant threat. In the Latvian case, the activities of trolls can be misperceived as coming from real Russians or Russian-speakers living in Latvia. This encourages mistrust and leads to tension among members of different ethnic groups. Given the experience gained from the Russian information campaign against Ukraine, where the political insecurity of Russian-speakers living in Ukraine was used as one of

101 'This is What Pro-Russia Internet Propaganda Feels Like—Finns Have Been Tricked into Believing in Lies', 24 June 2015. http://kioski.yle.fi/omat/this-is-what-pro-russia-internet-propaganda-feels-like

102 During the research more than 200 000 comments were analysed. The web comments were collected and analysed, focus groups and in-depth interviews were organized to analyse the respondents' ability to identify trolls and to understand their attitudes and reactions to trolling messages. Respondents were asked to discuss the content of troll messages, and to define the feelings that the content and form of expression evoked in them. For more detailed results please see 'Internet trolling as hybrid warfare tool: case of Latvia', NATO StratCom Centre of Excellence, 2016, http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

the main reasons for interference, online aggression resulting in changes in real life relationships would serve Russia's cause to become more actively involved in safeguarding Russian-speaking people in the Baltic States.

- **Long-term effects—**trolling can also cause specific effects over the long run. The strength of long-term effects does not lie in manipulating the limited group of people who read web comments and actively post in social media, but rather in reinforcing the Russian narrative that is already being communicated via other information channels, such as TV, blogs, propaganda webpages owned by pro-Kremlin activists, and others. Trolling is a small, but important part of a larger influence machine aimed at expanding information dominance and influencing the public in NATO member and partner countries.

4.2. DAESH'S USE OF SOCIAL MEDIA FOR INFORMATION ACTIVITIES

The conflict in Syria has been recognised as the most 'socially mediated' war in history.[103] Here, the exploitation of the virtual space for warfare is taking place at unprecedented levels of sophistication with Daesh being one of the most visible actors in this regard. As the terrorist organisation advanced into Iraq and Syria in the summer of 2014, they also 'invaded social media', particularly *Twitter.*

By understanding that public perception is more important that the actual success of combat on the ground, Daesh established a digital propaganda network to disseminate their narrative to global audiences. As Charles Lister, visiting fellow at the Brookings Doha Centre, admitted 'Daesh appears to be fusing both quantity and quality increasingly effectively [...] The constant flow of material and its high quality provides followers with the image of a highly organised, well-equipped organisation seemingly [worthy] of joining.'[104]

Daesh is not the first militant group to use social media for information activities and gaining support, but they do it more effectively than their counterparts with similar ideologies. However Daesh's ability to build its social media-based propaganda network has surprised many policy makers and experts.

As Brendan Koerner from *Wired* writes, 'Unlike al Qaeda, which has generally been fanatical about controlling its terror cells, the more opportunistic Islamic State is content to crowdsource its social media activities out to individuals with whom it has no concrete ties. And they are doing it openly in the West's beloved Internet, co-opting the digital services that have become woven into our daily lives.'[105]

When so many actors are against Daesh and so many efforts are made to limit their propaganda efforts in social media, how it

103 Marc Lynch, Deen Freelon, and Sean Aday, 'Syria's socially mediated civil war', United States Institute for Peace, 91.1 (2014)

104 'How ISIS used Twitter and the World Cup to spread its terror', http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/10923046/How-Isis-used-Twitter-and-the-World-Cup-to-spread-its-terror.html

105 Brendan I. Koerner, 'Why ISIS is winning the social media war', Wired, http://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/

is possible that they still manage to survive and even enlarge their presence there? Although there have been many attempts to counter them, and *Twitter* and other social media platforms are shutting down Daesh accounts on a daily basis, tens of thousands Daesh supporters are still active and keep distributing pro-Daesh content.

DAESH'S TWITTER NETWORK

The analysis conducted by NATO StratCom COE identifies the tactics and methods Daesh uses to make the most of *Twitter* opportunities to disseminate propaganda and recruit new members. It also considers why the DAESH propaganda network on *Twitter* is so resistant to anti-Daesh propaganda efforts.[106]

The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter conducted by the Brookings Institute in 2014 estimated that no fewer than 46 000 *Twitter* accounts have been established supporting Daesh. This number does not include the use of automated bots, a deceptive tactic meant to inflate Daesh's *Twitter* following, but does include multiple accounts maintained by human users.[107] According to the study, 60% of the accounts analysed were created in 2014.[108] This correlates with the advancement of Daesh activities on the ground and the increase in its propaganda efforts.

Although there is no overt recruitment on *Twitter* (that takes place on closed chat platforms such as *WhatsApp*, *Kik*, *Telegram*, etc.), the platform is used to attract wider attention, make initial contacts, and draw people into the closed networks where further radicalisation happens. After initial contact through *Twitter* the conversation quickly migrates to direct messaging or more discrete platforms.[109]

Twitter is a suitable medium for Daesh information activities since it is 'diverse in its demographics, global in its reach, easy to use, and is much more suited for anonymous and yet open-while-encrypted communications', it also makes it possible to post unrestricted content as long as it is linked to an outside source. This is why Daesh uses *Twitter* as a connecting medium for all of its distributed content all over the web—videos, photos, messages, and press releases posted in uncontrolled and unsupervised sites (such as *justpaste.it* or *archive.org*). By using these pages, Daesh can reach supporters who have previous knowledge of the locations of those messages, however for recruitment and publicity they must share the links to these pages in public domains, such as *Twitter*. The sharing is not limited to *Twitter*; they also use other mediums, such as *Facebook* or *Snapchat*, but *Twitter* allows 'for faster recovery from suspended accounts, possesses stronger encryption for private messaging and a much broader audience'.[110]

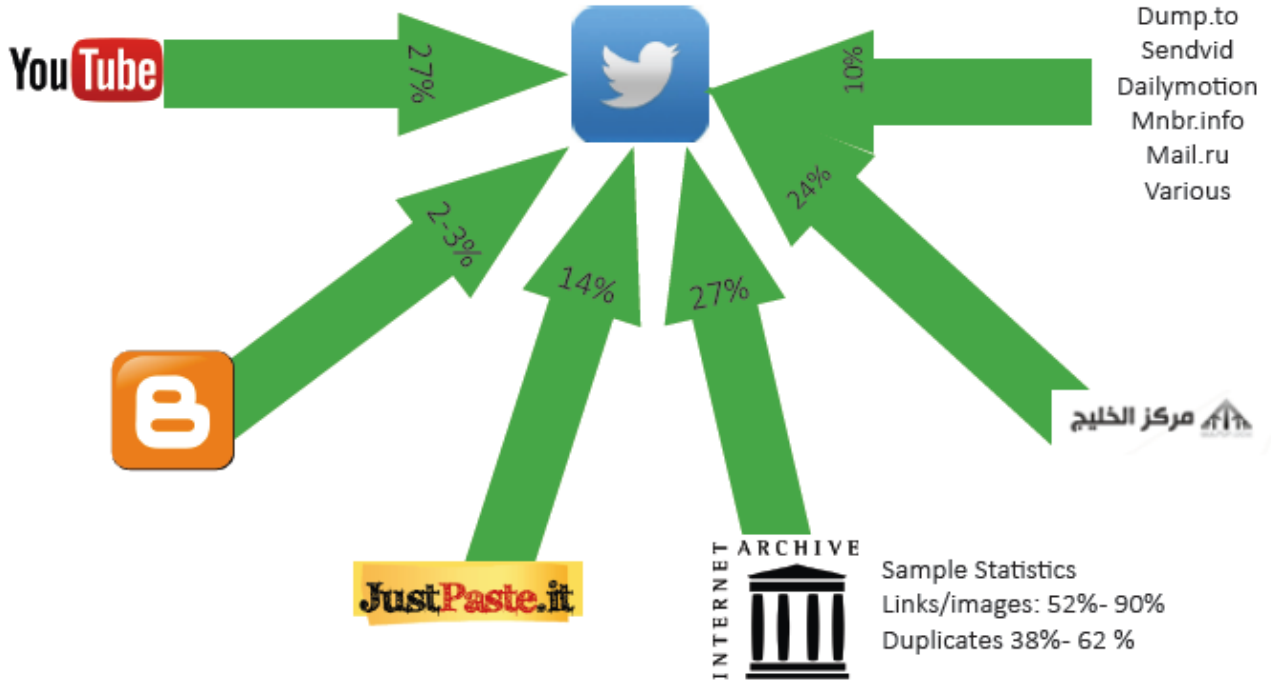
106 700 000 ISIS related tweets (using #The Islamic State and #The (State of) Caliphate in Arabic) were analysed during the period of 6 July to 3 August 2015 in Shaheen, 'Network of Terror'.

107 J. M. Berger and Jonathan Morgan, 'The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter', The Brookings Center for Middle East Policy. March 2015, p. 7.

108 Ibid. p. 16.

109 ''Nearly 50,000' pro-Islamic State Twitter accounts', BBC, 6 March 2015, http://www.bbc.com/news/world-us-canada-31760126

110 Shaheen 'Network of Terror', p. 8.



ATTRACTIVE BRANDING AND CONTENT

Similar to other terrorist organisations, for Daesh social media is a way to prove the existence of the 'state' and maximise the group's influence. Although Daesh lacks a unified territory, social media provides a brilliant platform for the creation of an abstract 'virtual state' and to demonstrate to the rest of the world that they should be perceived as a respectable state-like entity.

Daesh communication **objectives** for achieving this ambition can be divided as following:

- **Support** (recruiting new supporters and raising funds)
- **Unify** (gathering Sunnis around an artificial state)
- **Frighten** (intimidating both internal and external enemies)
- **Inform** (proclaiming the effectiveness of the Caliphate)[111]

The brutal videos that have attracted the attention of Western media are just a small percentage of Daesh communication efforts. The organisation has generated a comprehensive brand that offers an alternative way of living, promising their supporters 'immediate change and the ability to transform their future in the long term'.[112] According to Charlie Winter, this brand is composed of 6 main narratives—brutality, mercy, victimhood, war, belonging, and utopianism. If brutality is the most prominent narrative for Western audiences, utopianism is the most important narrative for recruiting new supporters.[113]

Based on the analysis of the most prominent Daesh *Twitter* accounts conducted in April 2015, Aaron Zelin categorized Daesh tweets into six main topics—military, governance, 'da'wa' (preachers), 'hisba' (moral policing), promotion of the caliphate, and enemy attack.

111 Daesh Information Campaign and its Influence, NATO StratCom Centre of Excellence, 2015, http://stratcomcoe.org/daesh-information-campaign-and-its-influence-1

112 Charlie Winter. The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy, Quilliam, 2015, p. 6

113 Ibid.

Similar themes reoccur in all these messages— Daesh members portray themselves as 'winners, competent and pious, while [the group] casts its enemies as unjust and unbelievers'.[114] Furthermore, 88% of Daesh content is visual (63% picture, 20% video, 5% graphic) showing a high proportion of emotional media content.[115]

One of the important aspects of Daesh propaganda efforts on social media is the ability to produce information materials with features that can attract the younger generation who are more likely be technology savvy and more likely to respond to Hollywood-style imagery and concepts. Several strengths can be identified that make Daesh content attractive for potential supporters.[116]

- **relevancy** to current news and thematic public discourse
- **brevity**, in contrast with Al Qaeda propaganda which typically consists of long tirades by Al Qaeda leaders
- **musicality**, use of Islamic music/ chants and sound effects where appropriate
- **quality**, use of high quality and high definition video editing and recording
- **engagement**, content tends to follow a larger narrative, engaging target audiences
- **simplicity**, easy to understand and act upon
- **diversity** in content (action/battles, normal life, political, and religious).

EXTENSIVE USE OF BOTS AND APPS

Daesh does not rely solely on their 'media soldiers' and volunteers to create and distribute content, but constantly look for the ways to maximise their presence on social networks by using technologic solutions. Automatically created content distributed by bots or apps provides a cheap and easy option for dramatically increasing Daesh reach.

According to *The ISIS Twitter Census*, **overall 20% or more of all tweets** are created using bots or apps. Based on the census, some of the apps are 'devotional in nature, tweeting prayers, religious aphorisms, and content from the Quran, although they may also serve as identity markers or fulfil some kind of signalling function'. However, the content they post does not overtly pertain to Daesh. In addition to their wide popularity both inside and outside of Daesh circles, these apps create noise in social networks and are used to hinder analysis.

Other apps are intended to disseminate Daesh propaganda at a pace and volume that enables their wider distribution. The most successful of these was known as the 'Dawn of Glad Tidings.' In mid-2014, thousands of accounts downloaded for the app, which was endorsed by top Daesh online personalities. At its peak, it sent tens of thousands of tweets per day. The app was terminated by *Twitter* in June 2014. [117]

After *Twitter* to shut down these accounts, the group moved some of its operations to 'closed' messaging platforms such as *Telegram*, *VK*, *Friendica*, *Diaspora*, and others, however these platforms have

114 Aaron Y. Zelin. 'Picture or it didn't happen: a snapshot of the Islamic State's official media output', Perspectives of Terrorism, Vol. 9, Issue 4, August 2015, p. 90

115 Ibid. p. 94

116 Shaheen 'Network of Terror' p. 11,

117 Berger and Morgan, The ISIS Twitter Census, p. 24.

also taken steps to remove the accounts of Daesh supporters. Therefore, the group continues to develop their own encrypted apps that can be distributed among their supporters and available only by acquiring specific codes.

Recent efforts include the creation of an Android app for broadcasting the Daesh propaganda radio station Al-Bayan. It allows listeners to receive Al-Bayan broadcasts outside the territories where Daesh operates. However, the app cannot be downloaded through the Google store, but can only be installed with AKP files that circulate online among Daesh supporters.[118]

SELF-REPAIRING AND SELF-REPLENISHING SUPPORT NETWORKS ON SOCIAL MEDIA

After a series of videos depicting brutal murders of Daesh hostages were released, *Twitter* began closing down Daesh accounts. Since then the group has learned to adapt to *Twitter* policies by creating new tactics for distributing content. They have created multiple dissemination accounts so that if one account is taken down others will still be operational. The blocked account comes back online using an alternative handle and the remaining accounts tweet its location. This authentication mechanism has largely worked since the late fall 2014.[119]

Daesh uses two inventive mechanisms to ensure the continuity of their information dissemination campaign. After the suspension or deletion of an account, new accounts are created at a rapid rate and use number of techniques to integrate them into the 'follow/friend' network so fellow Daesh members can quickly resume their use of the information. Once these accounts reach a certain level of popularity they can become operational as needed and begin tweeting and disseminating information using recognized hashtags. This is clearly a well-defined process for tactical and strategic planning.[120]

NATO StratCom COE fellow Joseph Shaheen proposes using the DEER model to describe Daesh defences against efforts to limit the distribution and reach of their propaganda. The acronym is made of a list of techniques Daesh uses to adapt to on-going changes, including the suspension and deletion of accounts and online content. The process begins with dissemination, is thwarted by deletion, moves through evolution, and finally moves on to expansion and replenishment. Shaheen argues that 'any fundamental strategy adopted to limit Daesh influence on social media must take this process into account'.

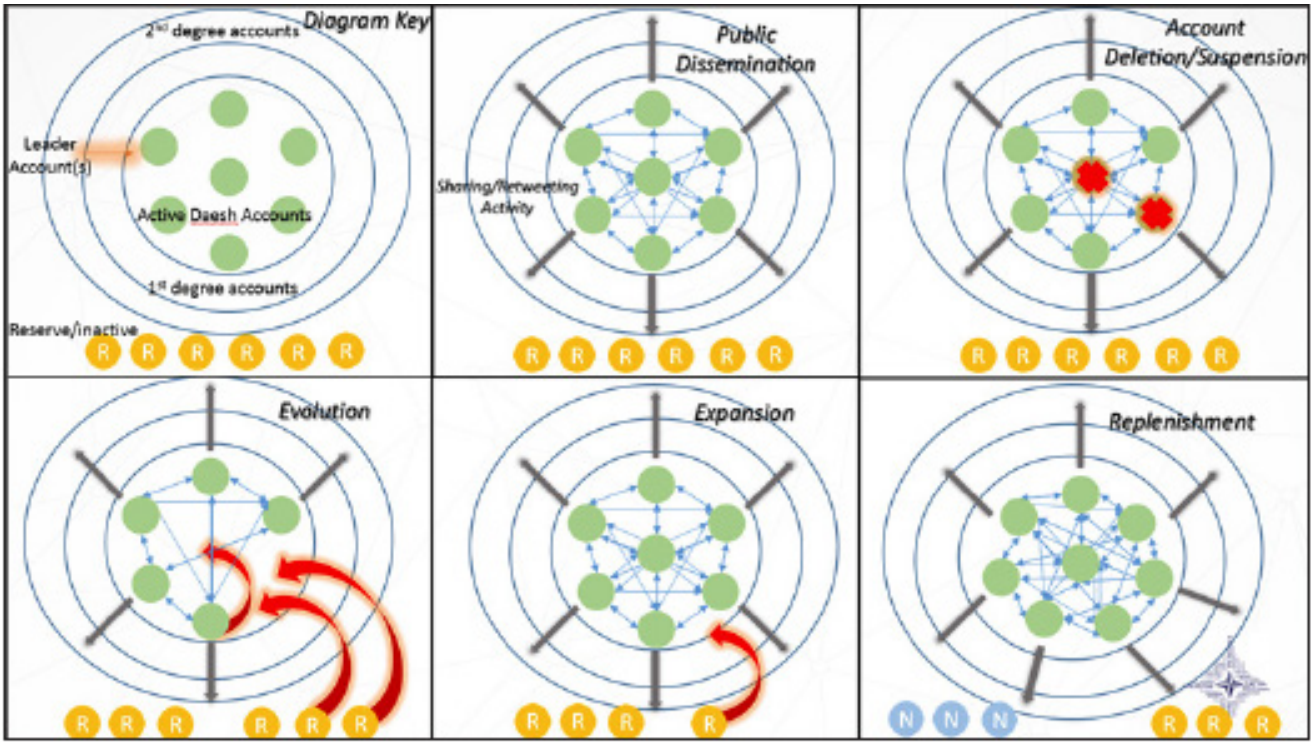
DEER process

1. Dissemination of public propaganda
2. Deletion or suspension of accounts by adversaries
3. Evolution of (network) structure or methods
4. Expansion of influence or methods
5. Replenishment of accounts and resources.

118 'ISIS launches first Android app to broadcast terror', Vocativ, February 1 2016, http://www.vocativ.com/news/278106/isis-launches-first-official-android-app-to-broadcast-terror/

119 Zelin, 'Picture or it didn't happen'.

120 Shaheen 'Network of Terror, pp. 21-22



Other Daesh methods to avoid counter-actions on *Twitter* include:

- Using independent actors to amplify the central message created by Daesh originators, while maintaining the independent nature and behaviour of these individual actors.
- Signalling to each other in order to avoid the discovery of Daesh accounts.
- The use of symbols and other tricks in account information and posts to avoid detection. This is why strict reliance on automated image detection becomes unsustainable.
- Speedy and adaptive recovery after account closure—to regain the previous levels of influence new accounts include requests such as asking others for 1000 retweets of the new account.
- Using system vulnerabilities, for example being able to change usernames and their URLs in *Twitter*.[121]

121 Shaheen 'Network of Terror', pp. 17-20

CONCLUSIONS

The exploitation of cyberspace to conduct attacks on infrastructure and influence human psychology for the support of military activities is here to stay. Given our increasing dependency on information technologies for communication and many daily tasks, it is more than likely that the diverse use of cyberspace for both good and ill will continue to expand. The rapid growth of Internet use around the world, including the use of social media platforms and mobile apps, has already demonstrated this trend.

Recent conflicts demonstrate how different actors have adapted their strategies based on changes in communication habits and the development of the information environment. It will be no surprise that more sophisticated and unpredictable methods will be used to influence target audiences in the future in.

As the case studies analysed in the StratCom COE report show, the methods of influence Daesh and Russia are using range from overt dissemination of media news and official announcements to covert methods such as falsified images, fake accounts, spreading rumours, deception, social engineering, and other methods of crowd manipulation. These actors blur the distinction between peace-time and war-time activities, and are not restrained by the same legal and ethical considerations that NATO and its member states impose on themselves.

A common strength of these actors is that they have skilfully adapted to the new information environment and effectively combine their activities both in physical and virtual space to affect the attitudes and behaviours of their target audiences. Furthermore, they are using tools and techniques that have been developed by private businesses for marketing purposes and have already been proven effective. Because of their flexible organisation and procedures, non-state actors in particular are able to constantly adapt to the new opportunities that technological development can offer. Whereas states and organisations are relatively slow and ineffective in responding, because of the bureaucratic restraints they face and their lack tolerance towards mistakes made by their communicators.

The case studies demonstrate that Kremlin and the leaders of Daesh have understood the importance of public engagement, which is the main principle at work in today's information environment. Both those who truly believe in radical Islam or the Novorossiya project and paid 'employees' and fake bots accounts use mass dissemination of manipulative messages in their online social interactions. It does not matter if an online avatar is real or fake, mass messaging enhances their social media presence.

Efforts to control the dissemination of terrorist propaganda or other malicious use of social media, either through technical or policy restrictions, are not an effective solution.

It is a game of cat and mouse, where ‘bad actors’ continually develop new, sophisticated methods of influence and public opinion manipulation while social media platforms and security services play catch-up in countering them. A heightened social media presence is more productive than efforts to weaken other information actors by limiting the distribution of their messages. This is further proof for decision-makers that ignorance and lack of engagement in social media is no longer an option.

ANNEX 1
INTERNET TROLLING IDENTIFICATION TUTORIAL

STEP 1

IDENTIFICATION OF HYBRID TROLLS

- Comment is too long (more than 4 lines)
- Comment is "out of context"
- Commenter is recognised as a troll by other commenters
- Commenter is openly aggressive and hostile
- Commenter is semi-literate
- If you have found one hybrid troll, look for others – they typically post in groups (or one troll uses different identities and message types).

NB – even if all these factors are present, they do not prove conclusively that the commenter is a hybrid troll.

STEP 2

CHECKING FOR HYBRID TROLLS

- Ask a question – classic trolls typically respond, responses from hybrid trolls are near impossible because of language issues.
- Google them:
    - Same message, different profiles
    - Same message, many repetitions (same comment posted to articles on different subjects; over a long period – even as much as a year)

STEP 3

LABELLING HYBRID TROLLS

- Via a comment, for the knowledge of more vulnerable internet users
- If the troll has already been labelled, proceed to step 4

STEP 4

IGNORE!

It is vital to ignore hybrid trolls and not enter into further engagement, for several reasons:

- The more users engage with trolls, the more credible they become in the eyes of inexperienced users
- The more replies trolls receive, the more 'clicks' they will receive in the future (the snowball effect), even the negative reactions can serve the purpose of the troll
- Any reaction can serve for provocation in the future (subjectively selected excerpts can be used as a generalisation of "real views" by propaganda channels).

ANNEX 2
SOCIAL INFLUENCE TECHNIQUES IN THE POLISH, UKRAINIAN, AND RUSSIAN INFORMATION ENVIRONMENTS IN THE CONTEXT OF THE RUSSIA-UKRAINE CONFLICT

Technique	Mechanism	Potential effects
Demonstrating superiority (civilizational or moral)	Use of messages that demonstrate greater cultural and civilizational development is frequently associated with depreciation of the achievements of other nations. ('When the Baltics were ruled by the Russians, those Republics developed and produced high-quality goods, but now all they can do is fish for sardines'). Claim of moral superiority of Russians ('we could murder, like you, but we prefer to send humanitarian convoys')	The use of this technique could reinforce the vision of large civilizational gaps between nations (in favour of Russians); it may also be a tool employed in classic trolling (a reader offended by this portrayal may escalate his verbal aggression towards such users).
Conspiracy theories	Users 'reveal the truth' to other interlocutors through supplying allegedly secret or inaccessible information showing 'the real causes' of phenomena and events. Based on this theory, the war in Ukraine is the fault of secret societies (Freemasons, Illuminati), worldwide organisations trading in gold and oil, and other similar groups.	The popularity of conspiracy theories and people's readiness to accept them is relatively significant. They are generally unverifiable (this is frequently taken as proof of their veracity). This could mean that some people ascribe at least partial responsibility for events to mythical perpetrators instead of the Russians.
Enemies want to create conflict	Users indicate that the conflict between countries is essentially generated by the activities of third parties (NATO, the EU, the US), which may strengthen their international position.	As in the case of conspiracy theories, users have a tendency to believe in such ideas and may relieve the real aggressors of responsibility.
Irony, sarcasm	Use of ironic phrases designed to mock behaviours, people or events. Most often, this type of post features spite directed to participants in the discussion. Example: 'of course, Ukrainians always want peace, just like they wanted to fight alongside Hitler'.	Use of irony and sarcasm is an effective strategy for gaining the upper hand in a discussion—people using this technique are perceived as far more favourable than usual 'trolls' who offend other discussion participants.

Technique	Mechanism	Potential effects
Slavic brotherhood	Emphasize that Slavic people (Poles, Russians, and Ukrainians) have much in common (much more than with the EU or NATO countries). Historical justification is often provided (e.g. fighting together in WW II).	Readers are encouraged to focus on commonalities with Russians, but, more importantly, on the differences between their own and Western culture.
Aggression against other participants (trolling)	Offensive slurs against other participants; personal attacks (incl. name-calling); vulgarisms	Discourages others from participating in the discussion or provokes them to equally aggressive behaviours. A substantive discussion ends or turns into a verbal conflict—in either case the troll's objective is achieved.
Labelling	The use of particular names and terms is designed to evoke specific associations among readers. The same people can be defined as 'separatist groups', 'terrorists' and 'people's militia', but each of these terms leads to entirely different cognitive consequences. The Russian propaganda expressions 'Banderites' and 'fascists' are the most common terms applied towards Ukrainians.	The continual and consistent use of labelling may change the manner in which an audience perceives and assesses the person/event labelled. The 'war for the Crimea' or 'the theft of Crimea' will be perceived differently from 'annexation', 'return to Russia' or #KrymNash ('Crimea is ours').
Reference to historical events	Events from the past are recalled (e.g. WW II). Tragic events are brought up to recall Ukrainian cooperation with fascists. The victories of the Red Army are invoked to show that it cannot be defeated.	Addressees are given additional factual confirmation of a particular point of view—propaganda ceases to be just the presentation of current affairs. The aim is to provide evidence that similar events have taken place in the past, always winding up in favour of Russia, thus justifying its actions.
'You have got bigger problems'	Dissemination of opinions that the Ukraine-Russia conflict is not good, however there are bigger problems to solve. This technique is used against 'third countries'—parties not directly engaged in fighting (Poland, Lithuania, Latvia, Estonia, etc.). The focus is thus shifted to local problems of those countries such refugees, budget, internal political disputes).	Participants of the discussion begin to perceive the Russia-Ukraine conflict as relatively distant from their own problems and lose interest in it.

Technique	Mechanism	Potential effects
'It's not your problem'	Technique applied primarily against 'third countries' (in this case Poland). Emphasize that the Ukraine-Russia conflict is only a local matter and has no relation to other countries.	This technique may increase the feeling of distance towards the conflict and the conviction that it is not particularly important for people living outside of the countries directly involved.
Social proof	Emphasizes that 'everybody does it', 'many have already decided', etc. used to highlight the sensibility of a particular solution or support for an idea (e.g. joining the Crimea to Russia or support for separatist forces in the Doneck and Lugansk region)	Readers are convinced that if their views differ from those of the particular narrative, they are in the minority as most of the people think differently.
'The biggest jerk in the neighbourhood'	Depict Russia with seemingly brutal honesty as 'the biggest jerk in the neighbourhood' – a country which can use its military might to break international law with impunity. Example - YouTube video: 'I'm the Russian occupant'.	This type of message develops feelings of both fear and lack of a real alternative to Russian domination. Readers get the impression that this manner of presenting the situation shuts off all potential for peaceful resolution and makes submission the only sensible solution for concluding hostilities.
Dehumanization	All enemies (in this case Ukrainians) are presented so as to suggest their lack of human characteristics. They are described as cold-blooded killers (descriptions of brutal executions, particularly of children), violating all human norms and customs.	Encourages the feeling that brutal actions towards an inhuman enemy are justified. What is more, if victims appear among the enemies, the natural solidarity with them is disrupted (as it is, and in accordance with propaganda narratives, they are not entirely people, and therefore do not deserve any sympathy).
Attacking with data	A large amount of data—percentages, facts, statistics —presented in posts. Generally given without sources, or with virtually impossible to verify sources ('secret data', confidential information from trusted sources, etc.). An example of this technique is information about problems of the Ukrainian army—'my friend works in the General Staff and said that 85% of the people drafted into the army run away and never show up'.	As people naturally trust data presented to them (consistent with the rule that '92.6% of people believe every sentence in which statistical data is given'), this information quickly makes an impression. As different studies have demonstrated, people rarely make the effort to verify the truth of such data; rather, they pass it along to others, enhancing its reach and credibility. This pattern of behaviour was also identified in the study 'Internet trolling as hybrid warfare tool: the case of Latvia', where it was acknowledged that the readers of web comments have problems identifying messages presenting facts and numbers as coming from 'trolls'.

OTHER PUBLICATIONS BY THE NATO STRATCOM COE

LEARN MORE ABOUT THE NATO STRATCOM COE

OUR MISSION

Our mission is to contribute to the Alliance's communication processes in order to ensure that it communicates in an appropriate, timely, accurate and responsive manner on its evolving roles, objectives and missions.

It is increasingly important that the Alliance communicates in an appropriate, timely, accurate and responsive manner on its evolving roles, objectives and missions. Strategic communication is an integral part of our efforts to achieve the Alliance's political and military objectives.

WHAT WE DO

The Centre provides comprehensive analyses, timely advice and practical support to the Alliance, designs programs to advance doctrine development, conducts research and experimentation to find practical solutions to existing challenges.

Centres of Excellence (COEs) are international military organisations that train and educate leaders and specialists from NATO member and partner countries. They offer recognised expertise and experience that is of benefit to the Alliance, and support the transformation of NATO. There has been 21 COE certified to date.

CONTACT US

- Riga, Kalnciema iela 11b, LV 1048, Latvia
  Ph.: 0037167335467
- Press, media and other inquiries
  info@stratcomcoe.org
- Doctrine, Concept and Experimentation Branch
  dce@stratcomcoe.org
- Education and Training Branch
  et@stratcomcoe.org
- Operational Support Branch
  os@stratcomcoe.org
- Framework Nation Support Branch
  fns@stratcomcoe.org
- Technical and Scientific Development Branch
  tsd@stratcomcoe.org

FIND OUT MORE

www.stratcomcoe.org
twitter.com/stratcomcoe
facebook.com/stratcomcoe

OUR HISTORY

- June 10, 2016
  Finland joins the NATO Strategic Communications Centre of Excellence as a Contributing Partner
- September 1, 2014
  North Atlantic Council approves the accreditation of the Strategic Centre of Excellence and activates it as a NATO military body
- July 1, 2014
  Estonia, Germany, Italy, Latvia, Lithuania, Poland, and the UK sign Memorandums of Understanding for the establishment of the NATO StratCom COE in Riga
- January, 2014
  StratCom COE is established as a national Centre of Excellence and starts preparations for the accreditation
- April 26, 2013
  Supreme Allied Commander Transformation (NATO SACT) submits its official letter of acceptance and gives Latvia the green light to develop a concept for a NATO StratCom COE
- February 20, 2013
  Latvia submits official offer to NATO SACT to launch a new NATO Centre of Excellence dedicated to Strategic Communications