Social Media in Operations – a Counter-Terrorism Perspective

A WORKSHOP REPORT FROM
THE NATO CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM AND
THE NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

Social Media in Operations – a Counter-Terrorism Perspective

27-28 September 2017

COE-DAT, Ankara, Turkey

by Berfin Kandemir (Workshop Rapporteur)

Alexander Brand (Workshop Director)

For NATO StratCom COE

Ben Heap (Strategic Communications Advisor)

Iona Allan (Copy Editor)

Inga Ropsa, inga-design.com (Graphic Design & Layout)

COVER IMAGE – SHUTTERSTOCK

Social Media in Operations – a Counter-Terrorism Perspective

Contents

Preface

Social media has assumed a fundamental role in today's society. As a technology with a high level of reach, billions of people are connected daily through global platforms, where they share personal experiences, documents and visual content. Social media has become one of the main channels through which people connect and communicate.[1]

NATO, as an organisation of 29 member states with different historical and cultural backgrounds, has made great efforts to develop its social media capabilities. NATO and its key decision makers are present in nearly all major social media networks and have gathered thousands of fans and followers. The current #wearenato campaign conveys the message that every day NATO allies work and train together to keep their citizens safe and that NATO, through partnership and cooperation, has secured peace and freedom for nearly 70 years. Most of NATO's current social media efforts are focused on this 'message delivery role', aiming to raise awareness about NATO as a brand and to resonate with key opinion formers within a younger audience.

Since September 2014, when NATO's Strategic Communications Centre of Excellence (StratCom COE) was established in Riga, Latvia, substantive progress in the study and understanding of social media has been made. The StratCom COE has published a number of research papers exploring current trends in social media and leading discussions on future strategy and related concepts, including the delivery of courses in social media analysis.[2]

NATO is involved with two major strands of work, both of which explore more flexible approaches of analysing and engaging with social media. First, the 'Digital and Social Media Playbook' currently under development by NATO's Science and Technology Organisation (STO) will constitute an up-to-date information environment assessment tool. Second, through the Multinational Capability Development Campaign (MCDC), NATO has supported the development of two social media-related concepts to be

[1] "New Trends in Social media", StratCom COE, December 2016, p 4.

[2] Particularly relevant in the context of this report are "New Trends in Social media" (December 2016), and "Social media's role in 'Hybrid Strategies'" (September 2016).

used specifically in operations.[3]

Although there are a number of academic publications that cover the use of social media for military purposes[4] or provide recommendations on how social media can support military actions on the ground,[5] few previous projects have focused on the exploitation of social media in the context of Counter-Terrorism (CT). This is understandable, as according to NATO's CT policy and concept,[6] terrorism is dealt with at the national level by law enforcement agencies under state control and supervision. In most cases NATO would support Member States at their request, or as part of an operation in an environment in which law enforcement forces of the nation state are overstretched or non-existent. Apart from a collective defence scenario, this is unlikely to happen within the territories of the Member States and has more relevance for non-aligned nations.

As part of ongoing efforts to further develop the CT perspective on social media, the NATO Centre of Excellence-Defence against Terrorism (COE-DAT) and the NATO StratCom COE conducted a workshop on 'The exploitation of social media on operations' in September 2017. The views were collected of over 20 social media experts and analysts, as well as NATO CT experts. The aim of the workshop was to develop the overall approach of the military's use of social media to deliver effects in CT scenarios. As such, the workshop can also be seen as part of both centres' contribution to strengthening of NATO's fight against terrorism.

This report provides a summary of those discussions. A brief outline of the panel's main presentations is provided as well as a summary of the following questions discussed during the Q&A.

- Can hard-line terrorist groups with extremist narratives be effectively countered with messaging or would it be better to focus on those individuals and groups on the brink of radicalisation and joining a terrorist group?

- Assuming that former terrorists enjoy high credibility within the target audience (with reference to "Breaking the ISIS Brand"[7] by Anne Speckhardt), how could or should they be integrated within military operations? What would such operations look like?

- Can offensive Cyberspace and Information

[3] "Social media in Support of Situation Awareness" (2014), "Exploitation of Social media in coalition operations" (2016), MCDC.

[4] "The Weaponization of Social media", Thomas Elkjer Nissen, Royal Danish Defence College 2015

[5] Elina Lange-Ionatamishvili and Sanda Svetoka, "Strategic Communications and Social media in the Russia Ukraine Conflict", NATO CCD COE (2015).

[6] NATO Counter-Terrorism Policy Guidelines (2012), NATO Military Concept for Counter-Terrorism MC 0472-1 (2016).

[7] *http://www.icsve.org/tag/breaking-the-isis-brand*, Anne Speckhardt, International Center for the Study of Violent Extremism (ICSVE).

Operations extend the role of the military within Countering Violent Extremism (CVE) programmes?

- How could CT-related social media expertise be integrated into HQ structures?
- Is it possible to develop reach-back capabilities to support deployed forces?
- What tools are there to offensively counter aggressive strategic narratives and which of them are in use in military entities of NATO and the nations?
- Which information from social media is relevant from an intelligence analyst's viewpoint and which tools are used for social media analysis in military entities?
- Once key influencers and propaganda distribution centres have been identified, should the military take measures to impede the spread of certain messages? In such cases, is the military capable of doing so or would this require external / industry support?
- How are CT aspects reflected in the roles and responsibilities of existing functions and capabilities, such as StratCom, Info Ops, PA, and PSYOPS? Which concepts / doctrine could be improved and updated?
- How does the social media industry counter terrorism and where would cooperation with the military be beneficial?

In closing, a number of suggestions regarding the following key issues identified are provided:

- Counter-Narratives
- Identities
- Social Media Analysis in support of Intelligence
- Information Operations, Psychological Operations and Counter-Terrorism

These suggestions include future steps which might be beneficial for further CT-related exploitation of social media in military operations.

We hope that those who could not attend the workshop can enjoy the content of this publication – as well as spark their interest in future activities dealing with this important topic.

Introductory lectures

This chapter provides brief outlines of each panel's introductory presentation. All panels are linked to the questions listed in the introduction. Those questions, as well as the presentations, have been discussed by the participants and lead to the findings and suggestions included within the corresponding chapters. For clarity, some elements from the introductory lectures are covered in the findings and recommendations chapter.

Turkish-speaking Daesh supporters' case study [8]

In the long history of terrorism, inducing fear in populations has always been one of its central aims. However, the availability of social media and the use of cyberspace and psychology have created a number of new opportunities for terrorist groups. For international terrorist organisations, with its leaders and followers dispersed widely across the globe, social media has become an important tool for sharing information and reinforcing a sense of cohesion and group identity. For governments trying to counter the threat and spread of terrorism, this has presented a new set of challenges.

Defining and understanding the issue is a prerequisite for solving it. On the battlefield – the classic military encounter – the enemy can be clearly identified. However, that is not the case in cyberspace, where it is quite difficult to identify the accounts used by terrorist groups. According to Hootsuite's social media penetration study, only 38% of the general population in the Middle East have active accounts on leading social network sites, which is a relatively small percentage compared to other regions.[9] The Turkish speaking Daesh community offers a particularly useful example of how terrorist organisations engage with and exploit the various dimensions of social media. The workshop used this as a case study to explore the role that social media plays within terrorist communication strategies.

The methodology used in the Turkish-speaking Daesh supporters' case study is a mathematical approach based on the technique of J.M. Berger and Jonathon Morgan from Brookings Institute[10]. According to this approach, the first step is to identify 'seed' accounts – the starting point for identifying a Twitter network. In turn, this enabled analysts to seek out Level 1 accounts – a network of

[8] Bedi ÇELİK, a retired Turkish Armed Forces Colonel and has been working at the Center for Middle Eastern Strategic Studies (ORSAM) as a social network analyst and visiting researcher since 2015.

[9] 'We Are Social- Digital in 2017 Global Overview', *https://wearesocial.com/special-reports/digital-in-2017-global-overview*

[10] J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter"

friends and potential Daesh supporters linked to the seed accounts. In the second stage, further data regarding the Level 0 and 1 accounts (the profile information and the most recent 200 tweets) was collected. In the third stage, noise reduction of the Level 1 accounts was conducted (cleaning the dataset: deleting irrelevant accounts and attributing them as either supporter or not). Lastly, for the fourth stage, the dataset was analysed, all

statistics were visualised, and relationship maps & findings were established.

In word clouds taken from the analysis, the top five repeated words were; "Allah" (3,561 times), "Infidel" (1,819 times), "Aleppo" (291 times), "Coup" (215 times), and "PKK" (182 times). These figures suggest that religious subjects are overwhelmingly at the centre in these tweets.

Another important finding is that there has been a significant decrease in Daesh's support base and Twitter activity. Findings indicate this is due to the effectiveness of Twitter's suspension campaigns. However, it is widely assumed that this support base has moved underground to the 'dark web' and continues their activities covertly on encrypted messaging platforms like Telegram. The accounts still exist on Twitter even though they are not active, presumably because they don't want to lose their network of followers.

The next frontier of Countering Violent Extremism (CVE): Offensive Cyberspace / Information Warfare?[11]

Social media analysis plays a crucial role in Information Operations (Info Ops), helping governmental and military organisations remain one step ahead of violent extremists.[12] The field of CT employs a broad

[11] By Evanna HU, who is CEO of Omelas and an award-winning tech entrepreneur working in the US, the Middle East and Africa. She also served as a consulting strategist and as Subject Matter Expert in technology and countering violent extremism (CVE) for US Government, USIP, and the World Bank.

[12] The NATO definition of Information Operations is 'A staff function to analyze, plan, assess and integrate Information Activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and North Atlantic Council approved audiences in support of Alliance objectives'. In some cases when experts refer to 'Information Operations' they are often referring to what could be better defined as 'Information Activities'.

spectrum of tools including behavioural surveys, case studies, and improvised tracking methods. The main limitation however, is that there is no standard measure of these methods' effectiveness. One starting point is the assumption that people are more honest online. To some extent, they are outspoken and controversial online because they want to attract more people, and most online activities have no societal barrier or taboo.

Therefore, collecting and combining data from social media sites like Facebook, Twitter, Instagram, VKontakte (VK) and Pinterest provides numerous results, especially when not looking at the text content first.[13]

Pictures and videos should become a priority for social media analysis. Extremist users often post content in the form of pictures rather than text, since there is less risk that images can be identified and censored through key word searches. Nevertheless, there are algorithms which are able to identify which images and videos originated from an extremist website or online forum.

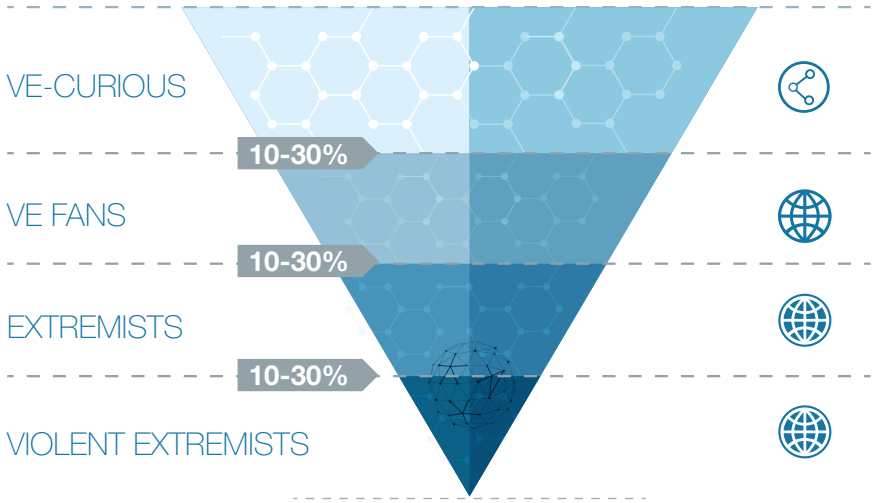
Overall data can be examined in a way which calculates the 'radicalisation score'. This score is based on algorithms that have been created for machine learning. The score ranges from 1 to 100, indicating how well new discoveries match the online behaviours of known violent extremists online. The bigger the number, the more radical person / place. Even though the number itself matters, what's more important are any significant shifts. For example, when analysing a very conservative, religious society, they might score 70 throughout the entire process. But when there is a change from 20 to 85, this needs to be explored in more detail. Those details can be aggregated in different ways: geographic analysis; network analysis and content spread, to name a few.

When analysing online Violent Extremism (VE) content for Info Ops planning, it is important to understand the way in which the target audience is segmented. The section with the most people can be considered the VE-curious, including people from academia and researchers. Depending on the content, 10-30% of the VE-curious become VE-fans. This could be because they are drawn to the sense of adventure, the feeling of community, or the fact that they find the ideology attractive. Of this group of VE fans, only 10-30% go on to become violent extremists.

On the whole, the VE-curious use social media channels which can be easily tracked, whereas VE

[13] 'ВКонта́кте' a Russian-based online social media and social networking platform *https://vk.com/*

fans and extremists use encrypted apps. The final stage is Tor, an online platform which enables access to the dark web.[14] At this stage it's hard to use social media campaigns against extremists. For the military, it makes more sense to focus their PSYOPS and Info Ops activity on people within the VE-fan layer. Once it gets down to the extremist and violent extremist levels, it is often too late to intervene with counter messaging.



Counter-messaging doesn't resonate with the target audiences if the source is too detached from their environment. It is therefore necessary to profile people and provide context which speaks directly with those individuals. This helps raise ideas about how, for example, NATO can engage more effectively with target audiences. People from the same religion or who share similar backgrounds tend to be more credible, and thus more effective communicators. This is why local organisations are often more successful at implementing counter-narratives than global ones.

Shared grievance and a longing for identity and belonging are significant factors driving people towards extremist ideology. People tend to be drawn towards simple and easily comprehensible ideas. Counter extremist messaging needs to take this into account, offering persuasive and straightforward alternatives. Crucially, these counter messaging campaigns must not look like an obvious attempt at influencing target audiences, otherwise both the message and the communicator lose their power.

[14] Tor is a kind of software developed to enable anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router"

Twitter as a Tool to Help Assess Extremism – A Practitioner's Experience[15]

Military doctrine refers to the fundamental set of principles which guides military thinking and helps define and achieve strategic objectives. Understanding the enemy and getting into their strategic mindset is a crucial part of this process. During the Cold War, the military placed a great emphasis on this type of understanding. Analysts were trained to think, respond to and perceive situations exactly like their Soviet counterparts. Deconstructing their decision-making process played an important part of operational analysis. Today, however, few military analysts follow this approach and struggle to anticipate the reactions and strategic decisions of their adversary.

Threats can be identified such as this military training for children in Syria.

Correctly identifying the nature of the threat is often the most challenging task for the military. In the context of violent extremism for example, the traditional emphasis on the violence overlooks the growing threat posed by non-violent forms of extremism. Although we normally associate extremist Salafist-Jihadist groups like Al-Qaeda with violence and excessive brutality, the group also places a huge emphasis on educating, recruiting and indoctrinating new members – none of which involves explicit forms of violence. Focusing excessive attention on the most violent and visible elements of extremism can therefore distract us from the equally destructive non-violent forms of extremism.

The success of military and Information Operations therefore depends on a thorough and nuanced understanding of target audiences. Twitter is a particularly useful tool in this respect and the exploitation of Twitter information was seen as early as the 2008 conflict between Russian and Georgia.[16] It can be easily done by creating an account and following organisations and known individuals without the need to tweet yourself. Twitter tends to 'push' information towards the user, meaning that you often end up discovering information you weren't necessarily looking for or even knew existed.

[15] By David BLOSE, a former US Army Officer and instructor at the US Army Command and General Staff College. He is currently working as a Strategic Analyst in Izmir, Turkey, as part of NATO's LANDCOM HQ.

[16] Jolicoeur, Pierre & Seaboyer, Anthony. (2014). "The Evolution of Russian Cyber Influence Activity; A comparison of Russian cyber ops in Georgia (2008) and Ukraine (2014)".

Such information can facilitate (inter alia) gaining knowledge on:

- Identification of factors that indicate changes in the operational environment.
- Identification of emerging threats.
- Existing extremist targeting priorities.
- Understanding of extremist tactics, techniques and procedures.
- Extremist's operational capabilities.
- Awareness of new equipment.
- Structural changes in extremist groups.

From an intelligence viewpoint however, there are certain risks:

- Assessing the validity of information and sources, and being able to distinguish data from analysis.

- Interrupted information flow – Twitter may close accounts or remove resources due to extremist content, but also sources (feeds) may have breaks in reporting or cease their operations.

- Reliance on translations – information might get lost in (automatic) translation from reporting sources.

Nevertheless, Twitter can be seen as a very valuable source of information to understand current trends in extremism since it as it offers a number of benefits:

- Twitter facilitates information networking and sharing of analysis, as such it presents extensive analyses and brainstorming of ideas, imagery analysis, data analysis, preparation of defences, extremist intelligence collection, analytic context, greater depth in cultural context, current situation.

- The information network expands by itself: those followed might post or have posted on their feeds information from other users of interest. Those users then can be followed as well.

- Even if new publications/resources reach only parts of the network, there is a high probability that they are further shared through retweeting and automatic alerts.

Given the importance of Twitter as a tool of analysis, a greater emphasis must be placed on educating and training analysts and developing a more sophisticated Twitter monitoring programme.

Military organisations could benefit from managed databases of feeds based on the aforementioned topics. On operations, it should be considered essential to have social media monitoring done by the

military, even though legal aspects and restrictions for this kind of work still have to be regulated. It should also be noted that effective exploitation is best accomplished by analysts and not collectors, since analysts have a better understanding of the target audience and relevant content.

Dealing with CT as part of PSYOPS[17]

Although the definition and principles of propaganda have changed little over past centuries, the channels of communication and the way that propaganda reaches its intended audiences have transformed drastically.

Social media has come to dominate the information space in recent decades, although remains a highly ambiguous and often misunderstood environment. People have a tendency to view social media in overly simplistic terms, believing that a carefully crafted online message, such as those created and sent out as part of Psychological Operations (PSYOPS), can solve a whole range of complex problems.[18] However, as Mencken reminds us "there is always a well-known solution to every human problem – neat, plausible, and wrong".[19]

Audiences on social media can be divided into two distinct parts. The first is the domestic audience, which need to be thoroughly convinced that military operations are worthwhile, legitimate and supportive of their interests. In some cases, this is called Strategic Communications rather than PSYOPS; an attempt by governments and decision makers to disassociate their work from 'propaganda'. The second target audience is your adversary; the principle focus of PSYOPS. This audience can be split further into several subdivisions, including civilian, military and armed populations. The aim of PSYOPS is therefore to influence each target audience with a highly tailored and specific approach.

Culture and religion play an important role in constructing messages that resonate effectively with each target audience. These principles should be reflected within the four major elements of any PSYOPS approach:[20]

- Inhibiting potential terrorists from joining terrorist groups

[17] By Dr. Ron SCHLEIFER, Senior Lecturer at the School of Communications, Ariel University Center (AUC) and fellow at the Institute for Counter Terrorism Policy, IDC Herzliya. He also acts as a consultant to Israel Defence forces on information warfare issues.

[18] Psychological operations (PSYOPS) is defined as "The planned use of communications to influence human attitudes and behaviour. It consists of political, military, and ideological actions conducted to induce in target groups behaviour, emotions, and attitudes that support the attainment of national objectives.", see Alfred Paddock, Jr., "Military Psychological Operations," in Political Warfare and Psychological Operations, edited by Carnes Lord and Frank R. Barnett (Washington, D.C.: National Defense University Press, 1989), 45.

[19] H. L. Mencken, "The Divine Afflatus" in New York Evening Mail (16 November 1917).

[20] Jerrold M. Post, "Psychological Operations and Counterterrorism", JFQ issue 37 (2005), p 106.

- Producing dissent within groups
- Facilitating exit from groups
- Reducing support for groups and their leaders

It is equally important to defend against the act of terrorism itself, and its central aim of spreading fear and anxiety through society. "If the act of one extremist can derail fragile movements toward dialogue and reconciliation, terrorism is being rewarded".[21] In order to avoid this outcome, sustained public education is required. This process must start before conflict has been begun and must be tailored to the interests of each target audience.

It is also important to realise that your adversary, just like yourself, will be using some type of manipulation and influence technique. The difficulty is that most violent extremists don't follow official doctrine. They employ a highly flexible approach to psychological warfare, and combined with their use of guerrilla tactics and social media, this can be extremely difficult to counter.

How industry counters terrorism and where cooperation with the military could be beneficial[22]

The widespread use of social media has prompted various attempts from law enforcement and intelligence agencies to control and monitor its usage. Modern social media networks are analysed by governments and private companies around the world, with "US, China and Russia being the countries that are most active in this field, but authorities from Iran and Syria have also demonstrated some interest for different purposes".[23] What makes social media analysis appealing to the military is its ability to support military functions such as Psychological Operations (PSYOPS), open source intelligence (OSINT), strategic messaging and, although arguably not a military responsibility, cyber espionage. As discussed in the previous panel on Twitter, it should also be taken into account that social media analysis can provide helpful information for force protection, improved threat awareness and even offensive purposes.

Nevertheless, in most cases, the monitoring of social media and online extremist threats

[21] Ibid, p.109.

[22] By Lt Col Alexander BRAND, who currently serves as the Branch Head Concept & Policy at COE-DAT. He has been working as a mass data analyst and also given social media related lectures during COE-DAT's "Terrorist Use of Cyberspace" course.

[23] Pierluigi Paganini,"Social media use in the Military Sector", posted in GENERAL SECURITY on January 31, 2013, h*ttp://resources.infosecinstitute.com/social-media-use-in-the-military-sector/#gref*

is conducted by national and international law enforcement agencies. Unfortunately, due to the ever-growing amount of social-media content and limited capacities of law-enforcement agencies, it has been argued that "Counter-terrorism is being slowly privatised"[24] and increasingly carried out by major private technology companies such as Facebook, Google and Twitter.

In 2017, Facebook explained that it intended to investigate terrorist activity across the family of Facebook apps, including WhatsApp and Instagram, as terrorist actors frequently use multiple platforms.[25] In addition to a workforce of experts tackling extremist propaganda and recruitment, Facebook's efforts rely on algorithms and computing power using the following techniques:

- *Image matching* – which recognises and prevents the upload of terrorist propaganda images or videos that have previously been flagged
- *Language understanding* – which uses artificial intelligence to recognise terrorist content through 'text-based signals'
- *Algorithms to find clusters* – using known terrorism-associated pages, posts, groups or accounts and investigating whether related material also supports terrorism

Google has also increased the number of independent experts in YouTube's Trusted Flagger programme, and aims to expand its work with counter-extremism groups to help identify content that may be being used to support radicalisation.[26] In addition to proactively scanning content and funding trusted flaggers, who help by moderating their own sites, Google also uses the so-called 'redirect method' which tries to divert those target audiences deemed most susceptible to extremist messaging towards alternative YouTube videos which debunk the intended message and recruitment narratives.[27] The development of this methodology was supported through interviews with defectors from terrorist organisations. An eight-week pilot program provided key insights about the kind of content that potential terrorist recruits search for, and what kind of content does and does not work as counter-propaganda.

With more than 390 million accounts globally, Twitter stated in its second half of 2016 transparency report that of the 376,890 accounts suspended for posting terrorism-related content, just two percent

[24] *https://www.theguardian.com/technology/2017/jun/29/silicon-valley-counter-terrorism-facebook-twitter-youtube-google*, retrieved 20 September 2017

[25] Monika Bickert and Brian Fishman „Hard Questions: How We Counter Terrorism", 15 June 2017, *https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism/*

[26] *https://www.theguardian.com/technology/2017/jun/18/more-must-be-done-about-extremist-content-online-says-google*, 19 June 2017, retrieved 20 September 2017

[27] *https://youtube.googleblog.com/2017/07/bringing-new-redirect-method-features.html*, retrieved 4 September 2017

were the result of government requests to remove data. Twitter said 74% of extremist accounts were found by "internal, proprietary spam-fighting tools".[28] The report also said Twitter had shut a total of 636,248 accounts for promoting terror since August 2015, when it first began tracking numbers.

IMAGE – BIGTUNAONLINE / SHUTTERSTOCK.COM

Facebook, Google and Twitter have also been involved in further international CVE efforts, supporting the publication of a code of conduct in 2016 by the European Commission, with Microsoft as an additional stakeholder.[29] One year after its adoption, the code of conduct on countering illegal hate speech online has already delivered some important progress.[30]

Despite the success of industry and civil society organisations and the implementation of the code of conduct, leaving the main monitoring and analysis responsibilities in the hands of industry may affect the availability of social media content to government organisations. This will impact government's ability to identify emerging threats, understand extremist tactics and their targeting priorities.

Transferring responsibilities towards industry because it is "partly a law enforcement capacity issue and partly because tech giants don't want to give states access to large amounts of data"[31] may not directly affect the military. Nevertheless, when operating in environments where law enforcement entities are limited or absent, having access to social media content before it is blocked or automatically removed is extremely important militaries. In such scenarios, collaboration with industry should be considered and developed.

[28] *https://transparency.twitter.com/en/gov-tos-reports.html*,

[29] *http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf*, retrieved 4 September 2017

[30] *http://europa.eu/rapid/press-release_IP-17-1471_en.htm*, retrieved 4 September 2017

[31] *https://www.theguardian.com/technology/2017/jun/29/silicon-valley-counter-terrorism-facebook-twitter-youtube-google*, retrieved 4 September 2017

Findings

In this section we offer some answers to the questions asked at the workshop and outlined in the preface to this report.

Can hard-line terrorist groups with extremist narratives be effectively combatted via messaging / communication?

In the context of Counter-Terrorism, developing a counter-narrative will have a limited effect on those already radicalised. Perception of the communicator is also an important factor here: military forces are unlikely to be the most credible messenger, so it's important to involve local civil communities as well as law enforcement and security agencies.

Can hard-line terrorist groups with extremist narratives be effectively countered with messaging, or is it better to focus on those individuals and groups on the brink of radicalisation and joining such a terrorist group?

As before, effects on those already radicalised are limited, so efforts should be focused on those who are at the very beginning of the radicalisation process. Social media analysis can effectively contribute to profiling people from such target audiences, and develop messaging strategies to influence them.

Can offensive Cyberspace and Information Operations extend the role of the military within CVE programmes?

A CVE scenario which features a major military role might be considered as a 'black swan', as in most cases – particularly 'home-grown' terrorism – national law enforcement agencies and local civil society organisations will play the leading role. Nevertheless, in an all-of-government approach, the military should seek to understand the dynamics and mechanisms of radicalised groups and how they evolve. Military entities should also consider sharing information with national law enforcement agencies on how they exploit social media in support of Information Operations.

What would such operations look like in general?

The main aim of Information Operations is to shape your opponent's perceptions, influence their decision-making process and structure their behaviour in a way which undermines their physical and communication capabilities whilst strengthening your own. An effective information activity will change your opponent's perception of the situation and cause them to respond differently to your actions. This could result in the diversion of resources, or a change in military strategy.

Assuming that former terrorists enjoy high credibility within the target audience, how could, or should, they be integrated into military operations?

As social media "in itself creates a hype-infused culture of envy – from who has more followers or likes, to content-based one-upmanship",[32] conducting an infusion of Info Ops into official and unofficial social media channels might be as simple as applying old-school deception and mis-information tactics with the ability (relying on the ex-insiders' expertise) to change the perceptions of target audiences.

There are a number of examples where ex-terrorist organisation members helped law enforcement and intelligence agencies, although not necessarily for credibility with the target audience. [33] Their expertise is not only valuable from the military analyst's perspective but also in profiling members of the target audience and understanding how they can be influenced through social media. Therefore, wherever possible, this expertise should be made available for planning military operations as well.

Which information from social media is relevant from an intelligence analyst's viewpoint and what tools are used for social media analysis in military entities?

As discussed above, information from social media can enable the identification of indicators and emerging threats, assist in the understanding of extremist tactics, techniques and procedures, provide awareness of new equipment and enhance understanding of the structural changes within extremist groups. However, it was also found that there is no standard toolset in use. A deeper analysis of the various tools currently in use was recommended as a possible follow-on activity; however, such analysis would require a secure environment and the output would most likely be restricted material.

Is there sufficient training, either provided internally or outsourced?

Currently there is no NATO specific education and training policy in place. Social media analysts are mostly trained on-the-job, with brief introductions to the various tools in use. Therefore, a demand for specific training on social media analysis, combined with a more in-depth overview on the tools in use is recommended.

How to integrate CT related social media expertise into HQ structures?

Currently no common structure of how to integrate social media expertise in HQs has been established. In certain cases, responsibility rests with Public Affairs, in others it is part of the operations branch or the responsibility of a special advisor. In a few cases it is integrated into the intelligence process. It should be considered for all operational HQs to have dedicated social media expertise

[32] Nicole Matejic, *http://www.infoopshq.com/2014/07/01/men-stare-goats-psi-ioinaction/*.

[33] e.g. Mubin Shaikh, a de-radicalized AQ recruiter who supported Canadian intelligence agencies.

integrated into the intelligence process as it can provide a lot of gains as detailed above. Continued sharing of best practices of all those involved within the HQ structure should be encouraged.

Is it possible to develop reach-back capabilities to support deployed forces?

As social media happens online, i.e. in a virtual domain, its analysis is not bound to any physical location. Therefore, a reach-back concept – preferably with the integration of experts with a background on culture and other relevant factors of the operational environment – could be a useful approach. The establishment of something like a "social media analysis cell" at higher command levels would mean that more than one operation could be supported at any time.

Once key influencers and propaganda distribution centres have been identified, should the military take measures to impede the spread of certain messages? In such case, is the military capable of doing so or would this require external / industry support?

Once such identification has been conducted and confirmed, the military is in general capable of preventing the spread of messages. This is achieved through the use of electronic warfare rather than by interfering directly with social media software.

How does the social media industry counter terrorism?

The social media industry uses various approaches to CT. In addition to human analysis, algorithms and artificial intelligence are used, mostly due to the high volume of data available (which continues to increase). However, such automatic processing has a possible downside. It might block content designed as counter-narrative messaging, and filter out content before any analysis is possible, reducing the opportunity to gain intelligence.

What is the military's role and where would cooperation be beneficial?

In an operational environment, where limited or no law enforcement entities are present, having access to social media content before it is blocked or automatically removed would prove beneficial for the military. This does not mean "back doors" as this might be counterproductive or open to exploitation. For operational reasons however, frequent information exchange and collaboration between the military and industry should be established before deployment.

Does it make sense to put more legal pressure on tech giants? Could that affect free speech?

One of the key findings of the workshop was that aspects of social media exploitation, especially analysis, exist in a legal 'grey zone', touching upon a number of basic principles like the right for privacy or freedom of speech. Furthermore, not all NATO

countries apply similar laws or have similar legal limitations. As a consequence, it is recommended that when exploring the exploitation and analysis of social media the legal framework should be regulated more carefully and standardised for operational and intelligence purposes.

How are CT aspects reflected within the roles and responsibilities of existing functions and capabilities, such as StratCom, Info Ops, Public Affairs (PA), and PSYOPS?

Despite the blurring of boundaries between different communications capabilities there are currently very few aspects of CT embedded into these functions, particularly regarding the use of social media. However, as the NATO Command and Force structure continues to establish CT 'Point of Contact' (POC) within their entities, it can be expected that this capability will grow over time.[34] Further improvement should be ensured through constant information exchange between relevant stakeholders of the communications functions and the CT POC concept.

Is the above sufficient? If not, which concepts and doctrine should be updated?

Due to the limitations regarding the military vs. law enforcement and intelligence roles, for the time being the existing integration should be regarded as sufficient. However, existing concepts and doctrine can be developed further based on shared best practice and the lessons learned process.

[34] As recommended within NATO MC 0472 / "Counter-Terrorism".

Key issues identified

This chapter summarises key issues that have been explored throughout the panels and provides a basis for the recommendations made in the next chapter.

Counter-Narratives

When talking about strategic communications and counter narratives, social media is only one part of a more comprehensive response. It should be considered as part of a broader spectrum of preparation and response instead of as a 'magic bullet' solution. Analysts tend to be of the opinion that it is better to keep social media accounts running because the more we learn from them the more we can then adjust our activity to counter any negative effects. It also provides insights on the people who are vulnerable or moving towards radicalisation.

A strategy of counter-narrative or counter-messaging does not make sense if the source is not considered to be a credible voice by the target audience, or if the target audience has not been thoroughly profiled and understood.

Other important points regarding counter-narratives are as follows:

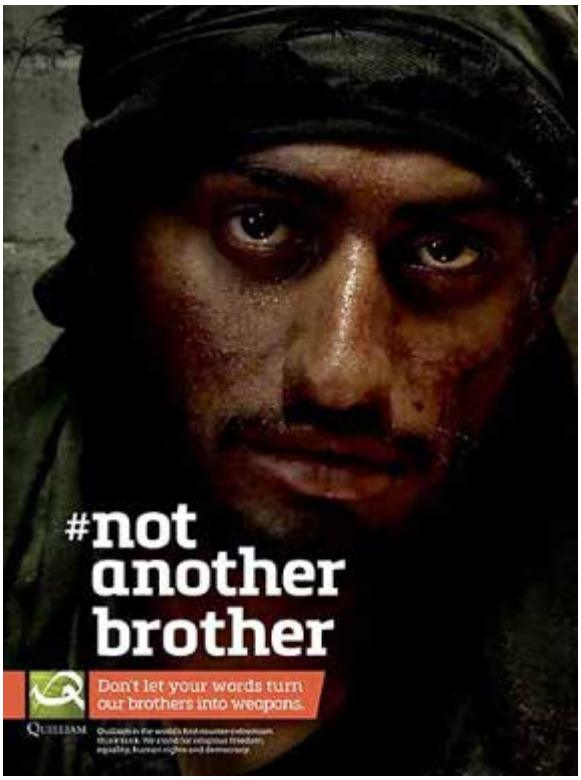
- First it must be understood how potential terrorist supporters on social media define themselves and their enemies.
- Considering the various dimensions of radicalisation, different counter narratives need to be formed for people coming from different cultures and geographies.
- The disseminator of the message is as important as the message itself in reaching the target population.
- Looking at follower maps, one can say that moderate discourses would not be useful against groups using militant discourse.

Identities

Identity, defined as the process of social categorisation and the feeling of 'sameness' and belonging with a particular group or character, is important when addressing different communities via social media.[35] Although it is questionable if 'Us / Them' identity constructions and legitimising strategies are beneficial for the overall approach, the main motivators which link people to a certain community have to be analysed in more depth. It is a sense of grievance, belonging and significance which are the main drivers attracting people towards a certain ideology.

[35] Tamara Kharroub, "Understanding Violent Extremism: The Missing Link", Arab Centre Washington DC (2015), p. 4.

It is possible to delve deep into the history of individuals using social media (for example to develop effective narratives). Nevertheless, it should always be taken into account that the average social media user is not necessarily



The Quilliam Foundation's 'Not Another Brother' campaign

interested into the complexity of an ideology or belief, but rather is attracted to catchy phrases or simplistic slogans. A second point which should be taken into account, is that people (especially with an immigrant background) might face identity confusion. This issue is also closely linked to integration and interwoven with the discussion on the difference between tolerance and acceptance.

Social media analysis in support of Intelligence

Social media analysis can offer valuable insights into the various actors within an information environment, including adversaries, groups of supporters and other key target audiences. This helps tailor messages to particular audiences and create more effective communication strategies.[36]

Accessing this information often requires operating within a legal "grey zone" for which there is no overarching NATO legal framework. In order to develop social media analysis further, a NATO wide legal framework or code of conduct must be established.

Another key issue discovered during workshop's discussion was that there is a broad variety of tools in use – a high number of which are provided by external contractors. Little of this information is available or shared with the Alliance's social media analysts.

Although there is no need to create one standardised tool for social media analysis, it would be

[36] Marcellino, William, Meagan Smith, Christopher Paul and Lauren Skrabala. Monitoring Social media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations. Santa Monica, CA: RAND Corporation, 2017. *https://www.rand.org/pubs/research_reports/RR1742.html*

useful to share some kind of 'shortlist', detailing the various tools and different types of training used. The promotion of further –possibly even formalised – information and best practices exchange between NATO and national social media analysts is also recommended.

Information Operations, Psychological Operations and Counter-Terrorism

When developing effective PSYOPS use of social media, it is helpful to look at some of the underlying processes from the perspective of collective behaviour. This may provide important insights into to the strengths and weaknesses of terrorist organisation and those seeking to counter their threat.

Educational factors, such as civics, critical thinking, values, ethics, cultural norms, traditions, worldviews, family and friends, personal experiences and identity start to develop at a very young age. People may go through a formal education system but as they begin to mature, their personal experiences and their worldview may change, affecting their vulnerability to extremist narratives.

Any message that challenges someone's worldview, implying it is 'wrong' is likely to be mistrusted and rejected. This scepticism needs to be challenged, so that target audiences are able to build trust in NATO military forces and be discouraged from further radicalisation. Additionally, while the use of social media for Info Ops and PSYOPS might not have a high chance of success when directed against members of terrorist groups already radicalised, however, they often prove effective against people in their virtual and physical community.

Suggestions

This workshop was intended as a starting point for further discussion on the use of social media in CT operations. Some suggestions refer to specific aspects of the topic, whilst others will be achieved through individual research and further workshops.

For a possible follow-on workshop, the scope of the operations as well their framework and policies should be specified in more detail. This is done in recognition of the limited military role attributed to CT operations within the Alliance's territory.

There was also a high demand for a more detailed study on which tools for CT-relevant social media analysis are in use. This could be best achieved by a workshop dealing only with best practices and lessons learned from the use of social media analysis tools. However, classification might be an issue for such an event. Nevertheless, as mentioned in the preface, StratCom COE will offer another social media analysis course in March 2018, where this idea might develop further.

The legal framework for the conduct of social media analysis in operations is also worth a closer look. This could be either done through a comparative research study compiling of NATO member and Partner Nations or through a workshop with a specific aim of developing guidelines or a "code of conduct" for (CT-related) social media analysis done by the military.

Further ideas generated during the workshop included the conduct of CT-related social media wargaming (i.e. discussing threat-based incidents and their handling with operational HQ staff and Subject Matter experts), also the possibility of a future addition into a NATO CT scenario currently under development.

Closing remarks

COE-DAT and StratCom COE greatly appreciate the contributions of all workshop attendees – speakers, participants, and staff alike – it helped us make it a successful venture.

In addition to the information and views exchanged, a number of acquaintances were made that hopefully will result in further study into the use of social media in operations from a CT perspective. This will help develop a more comprehensive approach, improve NATO and Partner Nations efforts' in countering terrorism and help build up resilience capabilities. Violent extremism is a global threat and one which can only be overcome if the international community come together and fight it collectively.

From the organisers' perspective, the workshop was very valuable in bringing together military practitioners and civilian experts. It enabled participants to exchange ideas and knowledge and engage in a meaningful discussion about how to improve our understanding of social media and violent extremism in the future.

.

Bibliography / recommended further readings

A

"Analytical Concept for the Use of Social media as an Effector" & "Baseline Assessment", Multinational Capability Development Campaign (MCDC) 2015-16, December 2016

B

Bates, Rodger A. and Mooney, Mara (2014) "Psychological Operations and Terrorism: The Digital Domain," The Journal of Public and Professional Sociology: Vol. 6: Iss. 1, Article 2. Available at: *http://digitalcommons.kennesaw.edu/jpps/vol6/iss1/2*

J

Jamie Bartlett, Louis Reynolds, "The state of the art 2015 a literature review of social media intelligence capabilities for counter-terrorism", September 2015, DEMOS, *www.demos.co.uk*

J

Jane Cordy, "The Social media revolution: Political and Security implications", NATO Parliamentary Assembly, Committee on the civil dimension of security, 30 August 2017, *www.nato-pa.int*

L

Lange-Ionatamishvili, Elina, and Sanda Svetoka. "Strategic Communications and Social media in the Russia Ukraine Conflict." NATO Cooperative Cyber Defence Centre of Excellence, 2015. *http://www.stratcomcoe.org/strategic-communications-and-social-media-russia-ukraine-conflict.*

M

Marcellino, William, Meagan Smith, Christopher Paul and Lauren Skrabala. Monitoring Social media: Lessons for Future Department of Defense Social Media Analysis in Support of Information

Operations. Santa Monica, CA: RAND Corporation, 2017. *https://www.rand.org/pubs/research_reports/RR1742.html*

N

"New Trends in Social media," NATO Strategic Communications Centre of Excellence (StratCom COE), December 2016, *http://www.stratcomcoe.org/new-trends-social-media*.

S

Shaheen, Joseph. "Network of Terror: How Daesh Uses Adaptive Social Networks to Spread Its Message", NATO Strategic Communications Centre of Excellence (StratCom COE), November 2015. *http://stratcomcoe.org/network-terror-how-daesh-uses-adaptive-social-networks-spread-its-message*.

S

"Social media as a tool of Hybrid warfare", NATO Strategic Communications Centre of Excellence (StratCom COE), May 2016, *https://www.stratcomcoe.org/social-media-tool-hybrid-warfare*

S

„Strategic Communication in Counter-Terrorism: Target Audience Analysis, Measures of Effect and Counter Narrative", NATO Defence against Terrorism Centre of Excellence COE-DAT, June 2014, *http://www.coedat.nato.int/publication/researches/01-StrategicCommunication.pdf*

T

The Economist. "Israel Is Using Social media to Prevent Terrorist Attacks." The Economist, 18 April 2016a. *http://www.economist.com/news/middle-east-and-africa/21697083-new-paradigm-intelligence-israel-using-social-media-prevent-terrorist*.

U

"Using Social media for Enhanced Situational Awareness and Decision Support", US Department of Homeland security, June 2014, *https://www.dhs.gov/sites/default/files/publications/Using%20Social%20Media%20for%20Enhanced%20Situational%20Awareness%20and%20Decision%20Support.pdf*

A WORKSHOP REPORT FROM
THE NATO CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM AND
THE NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE