CDS

158 CDSDG 17 E bis
Original: English

NATO Parliamentary Assembly

COMMITTEE
ON THE CIVIL DIMENSION OF SECURITY

THE SOCIAL MEDIA REVOLUTION: POLITICAL AND SECURITY IMPLICATIONS

REPORT

Jane CORDY (Canada)
Rapporteur
Sub-Committee on Democratic Governance

www.nato-pa.int

7 October 2017

TABLE OF CONTENTS

I. INTRODUCTION

1. The rise of social media[1] is one of the most recent and far-reaching manifestations of the digital computing and communication revolution that marked the beginning of the post-industrial era (i.e., the Information Age) several decades ago. The proliferation of social media in recent years has been truly extraordinary[2]–facilitated by the rapid growth in internet-enabled mobile devices (smartphones). For many across the globe, social media are a main news source; in 2016, 62% of US citizens got their news from social media sites–44% from Facebook alone (Gottfried and Shearer). Based on a survey of about 50,000 youth from across 26 countries, social media has already surpassed TV as the main source of information for that generation (Wakefield).

2. This dramatic transformation of information and communication technology cannot but have an impact on all aspects of life: education, the economy, and also politics. Changing communications, computing and information storage patterns are challenging notions such as privacy, identity and national borders. The profound changes inherent in this revolution are also changing the way we look at security, often in unanticipated ways, and demand innovative responses. Twitter and Facebook both amplify the voices of and decrease the cost for people to connect more intimately and to communicate and organise among themselves and with their governments. As well, the anonymity that is possible on social media can embolden those who propagate hate speech as equally as those fighting against authoritarian regimes without fear of reprisal.

3. Furthermore, social media also provides new opportunities for those who seek to disrupt the liberal democratic world order by abusing the intrinsic openness of the cyber domain. Social media is being used by terrorist organisations as a recruiting and propaganda tool. They are also being exploited by states that seek to influence and undermine liberal democracies, their government institutions and their social fabric – at times, to great effect. This has become known as the "weaponisation" of social media. Because social media is such a recent phenomenon, all potential consequences of this revolution are difficult to foresee. The aim of this report is first and foremost to raise awareness and launch a discussion among members of the NATO Parliamentary Assembly on this emergent theme and to offer some initial thoughts on ways to counter the malicious use of social media.

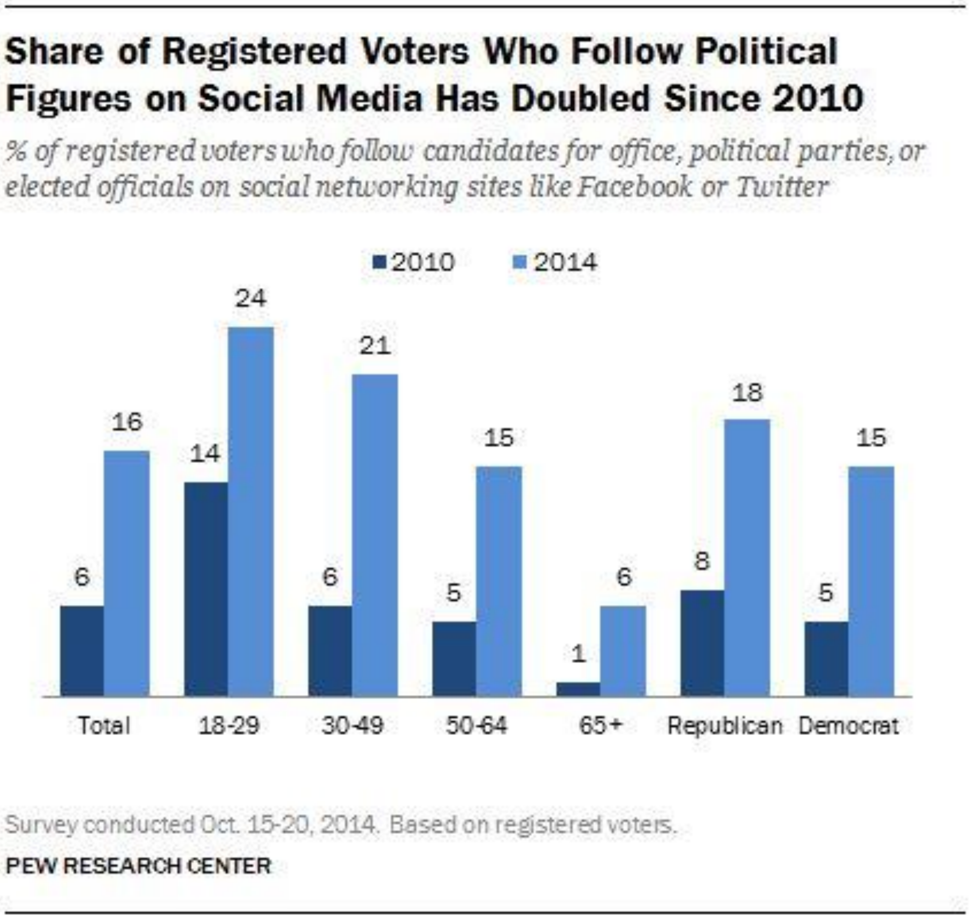
II. SOCIAL MEDIA AND DEMOCRATIC GOVERNANCE

4. The social media revolution has had a profound impact on democratic institutions and political life across the globe. Over the course of the last decade, citizens in general and political actors in particular have used social media sites, such as Twitter and Facebook, to challenge the political establishment and rally voices across the political spectrum. In the United States, for example, over a third of new social media users regularly direct their activity to commenting on government and politics. Twitter reported that the US presidential election was tweeted about over one billion times, and nearly 128 million accounts talked about the presidential race on Facebook

[1] "Social media" are defined by the following characteristics: users create their personal profiles/accounts, making them completely or partly public; user profiles and their generated content is networked. Various social media platforms have certain specificities: for instance, Twitter focuses on short messages, Instagram specialises in videos and pictures, and LinkedIn on professional/career information. Facebook is the most comprehensive platform. Some messaging platforms such as WhatsApp are also referred to as social media, although they are mostly used for chatting and file exchanges among a small group of people, often between two users.

[2] In 2005, only 5% of adult in the U.S. used one of these platforms; in 2011, that share grew to 50%, and currently it reaches almost 70%. Some 88% of young adults (ages 18-29) in the U.S. are on Facebook. Globally, there were about 2.7 billion social media users in January 2017 (37% of the world's population), almost half a billion up from January 2016. Facebook alone has almost 2 billion users. The fastest growth is in developing countries.

in the United States. In his capacity as the President of the United States, Donald Trump has highlighted the value of communication via social media, particularly Twitter, which he noted gave him the opportunity to connect directly to the citizens, bypassing certain mainstream media outlets that, according to the President, produce "fake news". To the north, in Canada’s 2015 federal election, civic society teamed up with Google to find innovative ways to increase voter turnout.



Share of Registered Voters Who Follow Political Figures on Social Media Has Doubled Since 2010

% of registered voters who follow candidates for office, political parties, or elected officials on social networking sites like Facebook or Twitter

Survey conducted Oct. 15-20, 2014. Based on registered voters.

PEW RESEARCH CENTER

5. More than just a source and a sounding board, user activity on social media sites is proving to be anecdotally predictive of campaigns. After the US presidential election, researchers found a strong correlation between the candidate a voter followed on Twitter and who that individual voted for on election day (Thompson). Pollsters even found that user activity on Facebook was more predictive of the US election than traditional polls. During the United Kingdom’s EU referendum, scholars observed more activity on and support for the ‘Leave’ campaign on Instagram and Twitter than with the ‘Remain’ campaign. Although activity does not mean support, commentators concluded that campaigners underappreciated the popularity of ‘Leave’ on social media and how that would translate into votes (Polonski).

6. The ability of social media to turn any individual into an information actor benefited civil society and human rights activists both in democratic and authoritarian states. Social media lowers the cost of communication across internet-enabled devices to help movements overcome isolation or fragmentation. Similarly, social media produces information cascades—when dissenting and risk-taking first-movers express their grievances, those who may have otherwise not participated feel more comfortable joining in. This has two effects: the public sphere grows and protests can be coordinated across large geographic areas; also, the cost of repression, especially for authoritarian regimes, increases because, thanks to social media, certain regions (i.e., the Middle East) have “developed a robust infrastructure for publicising abuse of protestors” (Lynch).

7. The most prominent examples where social media played a central role in large-scale political mobilisation include the Iranian protests in 2009, when people took to the streets to protest the electoral win of former-President Mahmoud Ahmadinejad, forcing the Iranian regime to temporarily suspend access to new social media until the government regained control of the crisis. However, it was the Arab Spring in 2011 that most clearly demonstrated the power of social media. The Facebook-organised protests on 25 January 2011 drove Egyptians to public squares across the country to demand bread, dignity and freedom. Eventually, Egyptian President Hosni Mubarak’s 29-year regime toppled under civilian protest and military pressure. Another powerful example of social media’s role in mass mobilisation was the pro-democracy movement in Ukraine that ousted President Viktor Yanukovych. Twitter and Facebook were used to organise and solidify protesters in the Euromaidan and to enable key figures to communicate effectively with demonstrators.

8. Social media also empower human rights and anti-corruption activists. An example of this can be found in what happened when a prominent Russian anti-corruption crusader, Alexei Navalny, produced a 50-minutes video which revealed the stunning wealth of Prime Minister Dmitry Medvedev, exploiting, *inter alia*, Medvedev’s passion for posting pictures on social media. Russia’s state media ignored Navalny’s video, but it spread rapidly across the Russian society through social networks and YouTube.

9. Protesters in NATO countries routinely use social media networks. The Occupy Wall Street campaign in New York in 2011, and protests in Istanbul’s Gezi Park in 2013 are two examples. In the latter case, Twitter was so effective that the Turkish government temporarily disabled the service for Turkish users during demonstrations. Also in Turkey, social media played a critical role in defeating the coup attempt in July 2016: President Recep Tayyip Erdogan famously broadcasted his address to the nation using a FaceTime application on his smartphone. His message urging people to take to the streets was quickly disseminated via Twitter, Facebook, WhatsApp and other social channels.

10. However, the correlation between the emergence of social media and democratisation is not as strong as one would hope. Adroit use of social media does not necessarily cultivate productive discourse nor does it automatically strengthen democratic institutions. Further, not all actors are necessarily interested in democratising their societies. An important characteristic of online political activity is how deeply segregated it is. A data journalist at MIT’s Media Lab studying the 2016 US presidential election, suggests that political commentary online is segregated because users occupy ideological or issue-area 'bubbles' (e.g., immigration or gun rights) within which they conform. Whether segregated networks lead to polarised politics is unclear. The data itself cannot explain why users are so polarised.

11. User preference algorithms and social media ‘bots’ do, however, seem to play an important role. Facebook and Twitter enable self-segregation in that they are designed to provide personal, curated content based on individual user preferences (e.g., their ‘like’ history). Both platforms use algorithms to curate content for users. Using data collected on their past behaviours and preference, these algorithms filter content displayed on individual user feeds according to its relevance to their interests and preferences. This curation increases the likelihood of engagement with like-minded users and exposure to pictures, discussions, news, and opinions that support an individual user’s preferences. It also reduces users likelihood of exposure to dissenting or conflicting views (Lee; Thompson). Notably, Facebook and other platforms are reluctant to introduce a “dislike” button.

12. The increased frequency of debate does not necessarily translate into a robust exchange of conflicting or diverse ideas. Social media ‘bots’ increase polarisation by manufacturing and disseminating content that reinforces skewed user beliefs. ‘Bots’ are easily programmable accounts on Facebook and, especially, Twitter that automatically generate content. Often, authentic account holders who receive fabricated content do not know they are interacting with

‘bots’ (Guilbeault and Woolley). ‘Bots’ are in widespread use and have already demonstrated a capacity for disruption. For example, a study of the recent US presidential campaign found that a sizeable share of pro-Trump and pro-Clinton tweets during the US presidential campaign were generated by ‘bots’, programmed to search and disseminate specific messaging instantaneously. A single ‘bot’ account can send out thousands of tweets a day, drowning out real Twitter users who may offer relevant, and potentially productive, dialogue on social media. Searching for content using key terms, ‘bots’ are designed to redistribute (e.g., retweet) this material without verifying its validity. Marginal and/or extremely partisan actors can co-opt trending discussion to give their issue areas traction especially when they program ‘bots’ to redistribute their content on their behalf. In recent months, it came to light that ‘bots’ were used as disruptors in the final days of the French presidential election against Emmanuel Macron’s campaign.

13. The relative success of many anti-establishment parties in the Euro-Atlantic area may be attributed to skilful social media strategies. Often the most prolific political accounts are far-left and far-right anti-establishment party leaders and groups. Their accounts usually post more online content, use colourful and even inflammatory language, and interact more intimately with their constituents than their more mainstream counterparts (The Economist, 2015).

14. Social media networks have facilitated the propagation of false and disruptive stories, which users accept at face value. The danger is that fake news has already started to shake the confidence citizens have in their institutions and leaders. The proliferation of alternative, non-traditional media sites (i.e., fake news) has accelerated this in recent years. The incentive to misinform on social media networks is, in fact, profit. Dramatic and often false stories increase clicks on sites trying to attract readers. The advertisement payment structure used by Google and Facebook is based on this "per click" model (Alexander and Silverman). False stories can be rapidly transmitted to multiple websites, gaining traction in the news cycle before content editors at major news agencies have time to intervene and question sources (BBC, 2016). A survey conducted by Ithaca College in New York found that 40% of local newsrooms *do not* have procedures to fact-check social media content before it is included in a newscast (Adornato). This can have devastating consequences for public perceptions on any number of issues. For example, polls suggest that there is a positive relationship between the proliferation of fake or hyper-partisan news and increased negative perceptions of one’s government. Gallup’s polling data supports the claim that mistrust in government is on the rise and is reaching record highs.

15. In sum, social media have had a profound effect on democracies and in authoritarian countries. Social media can make societies more pluralistic, but not in the traditional sense. It may be better, instead, to describe the confluence of democracy, political activism and social media as “chaotic pluralism” as some experts suggest. This is a pluralism that offers a diversity of mobilised voices [and movements], but that is often unpredictable, unstable, and unsustainable (Margetts et al.). While political engagement on social media has enriched democratic discourse and opened new avenues for information flow, it has also entrenched users within ideological cocoons. The loudest and most engaged voices online are producing deep political change, but those calls increasingly come from polar ends of the political spectrum.

III. THE ‘WEAPONISATION’ OF SOCIAL MEDIA

16. The scale of the social media revolution cannot but have an effect on global security. There is a growing interest among some state and non-state actors in using social media against their adversaries–a process that Thomas Elkjer Nissen, of the Royal Danish Defence College, refers to as the ‘weaponisation’ of social media. Nissen identifies several ways of using social media for military purposes, including intelligence collection, psychological warfare and even command and control (C2) activities (e.g., opposition groups in Syria that have no formal C2 structure resort to using social media for coordinating and synchronising actions, and in some cases giving commands or direction) (Nissen). Nigel Inkster, former deputy chief of Britain's Secret Intelligence

Service (MI6) notes that for intelligence officers, social media analysis can provide an unprecedentedly fine grain picture because images taken on ground level can often yield more information than satellite or aerial reconnaissance footage. Activities on social media are virtual, but they can have real-life effects, for instance by instigating mass protests, withdrawing money from banks, or attacks on certain groups or by portraying individuals as the enemy (Lange-Ionatamishvili and Svetoka).

17. Examples of convergence between social media and military domains include: the US airstrikes against one of Daesh's command based on information received from a social media post by a Daesh[3] militant in June 2015; the monitoring of Twitter feeds from Tripoli by NATO intelligence officers during the Libya campaign; the extensive tweeting by dedicated teams of the Israeli army during the 2014 conflict in Gaza, sometimes engaging directly in online exchanges with Hamas operatives; and, the confusion over a fake news story on Twitter that led Pakistan's Defence Minister to threaten the use of nuclear weapons against Israel. During a military exercise in June 2016, Australian intelligence analysts were able to identify the location, equipment, and organisation of opposing forces participating in the exercise by analysing information freely available on social media.

18. While Allied and partner militaries have had success in operationalising social media platforms in combat, non-state actors such as Daesh and states such as Russia have also achieved a high degree of proficiency in weaponising this new medium.

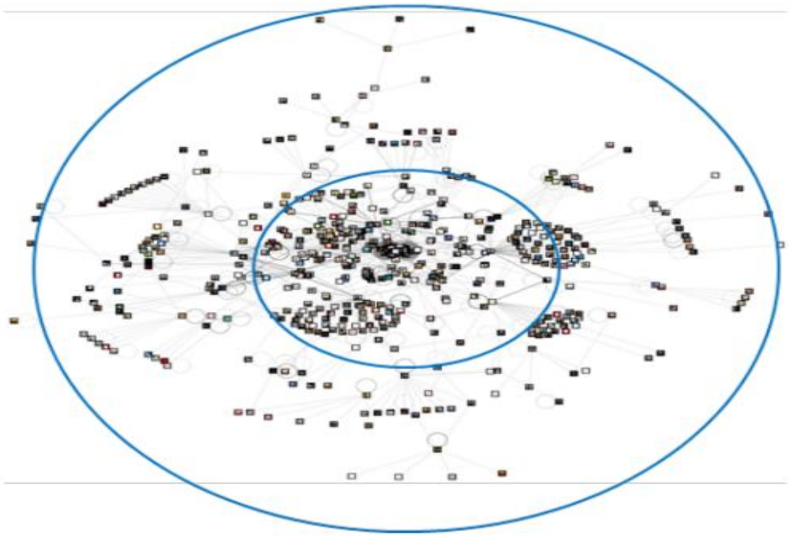
A. DAESH AND SOCIAL MEDIA

19. Daesh is not the first terrorist organisation to grasp the importance of social media. Members of Hamas have reportedly used platforms such as Facebook and Twitter to disseminate their ideology. Al Shabaab used Twitter to claim credit for its attack on the Nairobi Westgate shopping mall, posting pictures of it in near-real-time. In April 2015, the Al-Nusra Front (now known as the Jabhat Fateh al-Sham) launched a social media-enabled campaign called "Mobilize", that managed to recruit some 5,000 children to join its ranks. Several NATO Allies have experienced home-grown terrorist attacks that were inspired through online means of communication: for instance, perpetrators of some high-profile attacks in the West were inspired by online sermons of radical preacher Anwar al Awlaki (Ruane).

20. However, it is widely agreed that Daesh has elevated the malicious use of social media to a new level. Daesh seems to have grasped the feature of social networks called the "power curve". On one end of this curve, few dominant contributors drive the conversation on the network in the so-called "broadcast mode." On the other end, networks scale down to very small groups where high-quality conversations take place ("conversation mode"). Modern terrorists have figured out that the advantage is to work both ends of the curve: they manage to get a dominant influencer to convey their messages, while also luring individuals into small group conversations where they can attract new recruits or radicalise the other discussants (Carafano). The architecture of Twitter is particularly attractive for Daesh because it is well suited for anonymous communications with a broad audience and enables a faster recovery when accounts are suspended (Shaheen).

21. Experts from NATO Strategic Communications COE (StratCom) have analysed Daesh's Twitter traffic network and discovered that the terrorist group developed a so-called Core-Periphery structure on Twitter: namely, that there was a high number of accounts with low centrality measures (peripheral), and only a few accounts with high centrality scores (core group). However, the core group were responsible for 76% of the traffic. It is plausible that the core group accounts are managed by an even smaller group of Daesh operatives. Daesh's offshoots in other parts of the Middle East and North Africa (MENA) region may retain a degree of autonomy, but overall, Daesh's messaging machine appears to be highly centralised and coordinated (Shaheen).

[3] Arabic acronym of the terrorist organisation "Islamic State in Iraq and Syria"



Core-periphery structures are noted for a central group of actors followed by a larger but less dense network. This figure shows an example of one of our collected traffic networks with an added circular visualization to illustrate coreness.

Source: http://stratcomcoe.org/network-terror-how-daesh-uses-adaptive-social-networks-spread-its-message

22. It may seem that centralisation of Daesh’s social media activity is a liability because it means the group’s core accounts can be identified and closed. However, Daesh operatives have developed a series of measures to overcome this problem. Typically, Daesh cyber operatives create several idle Twitter accounts that are part of a network surrounding a core account. Once a core account is closed, an idle account is activated and is either turned into a core account itself or it informs the rest of the followers – using a system of hashtags and symbols – about the identity of the old account when it re-opens under a new name. Daesh also uses certain techniques to avoid detection and closure of accounts. For instance, usernames and, thus, the URLs[4] of its core accounts are periodically changed, which enables these accounts to elude URL-based detection software used by state security services. Daesh operatives also slightly alter popular Daesh-related images to avoid detection by image recognition software. Daesh operatives seem to understand well the dangers of using Twitter’s native geo-tagging function which provides a GPS-produced tag with geographic coordinates attached to each tweet: in fact, in December 2014, Daesh issued an edict forbidding its fighters from turning on Twitter’s geo-tagging function (Shaheen). Finally, Daesh social-media operators know how to post tweets, including links, hashtags and images, in a way that would not trigger Twitter’s spam-detection algorithms (Farwell).

23. In sum, Daesh seems to have developed remarkable technological proficiency and has effectively turned into a Twitter hydra. It is estimated that since 2013, tens if not hundreds of thousands of Daesh Twitter accounts have been suspended or deleted on Twitter (Shaheen) but that did not prevent Daesh from generating as many as 90,000 tweets every day (Schmitt). Daesh’s Core-Periphery approach and a clever use of hashtags give the terrorist group a high degree of visibility on social media. For instance, as Daesh marched into Mosul, its supporters produced up to 44,000 tweets a day, making the group’s message among the most prominent when one searched Twitter for ‘Baghdad’ (Farwell). According to RAND, the number of active Daesh opponents on social media is six times larger than pro-Daesh accounts. Yet, Daesh supporters routinely out tweet opponents, producing 50% more tweets per day (Bodine-Baron et al.).

[4] The URL (Uniform Resource Locator) is the hyperlink address that one enters into an internet browser in order to reach the intended account’s profile page.

24. Other characteristics of Daesh’s use of social media include:

- Daesh understands well the importance of visual contents on social media: it is estimated that 88% of Daesh content is visual (63% picture, 20% video, 5% graphic) (NATO StratCom, 2016a), which is particularly attractive to the younger generation. This visual content is of very professional quality;
- Daesh tweets in several languages including English, Arabic, German, Farsi, Hindi, and French;
- Daesh messages are relevant to current news, short and easy to digest;
- Daesh also practices hijacking popular hashtags such as those linked with the World Football Championship in Brazil (Farwell) or #*Bruxelles* and #*Belgique* that emerged in the wake of the terrorist attacks in Brussels and originally were intended to be used to express support for the victims (NATO StratCom, 2016b);
- It is also estimated that at least 16% of Daesh accounts were in fact automated (‘bots’) (Shaheen).

25. On the ground, Daesh is losing territory. Over the last year, the so-called Caliphate lost over 50% of its territory in Syria and over 70% in Iraq. Even so, it is believed that Daesh will increase its online activities. The sophistication of the Daesh social media machine creates the impression of a solid and effective organisation, seemingly one that is worth joining (NATO StratCom, 2016a). Daesh presents itself on social media as a true defender of Islam and an agent of change. Its image as a brutal and fearsome fighting machine is combined with warmer images, for instance showing foot soldiers eating Snickers bars and nurturing kittens (Farwell). Experts observe that since 2015, Daesh has produced more content geared to normalising the so-called Caliphate, than content depicting violence (Matejic). This narrative appears to be quite successful in attracting new recruits for Daesh.

26. It is estimated that more than 30,000 people, including about 5,000 EU citizens, travelled to Syria and Iraq to join the ranks of terrorist organisations since the break-out of the conflict there in 2011. It is difficult to assess how many of them were radicalised and recruited via social networks, but according to the US Department of Justice, most young terrorist recruitment is linked to social media. Recruitment typically starts on a public platform as an exchange of radical ideas, and then the conversation moves to one of the encrypted platforms (such as WhatsApp, Kik or Telegram) where the recruitment can continue in private. Daesh has an elaborate system of questioning potential candidate to ensure that he or she is not an intelligence operative (NATO StratCom, 2016b).

27. In addition to propaganda and recruitment, Daesh also uses social media to provide technological advice and guidance to their followers. Social media is also a vital part of Daesh’s fundraising strategy (NATO StratCom, 2016b). However, Daesh tries to minimise the use of social media for command-and-control functions in order to conceal identities and location of its leadership (Farwell).

28. Still, social media is a double-edged sword and is being used by counter-terrorism agencies to collect information and prevent terrorist attacks. For instance, Israeli security services use specially developed algorithms to monitor the social media accounts of young Palestinians to identify potential terrorists, and in some cases, were able to prevent suicide attacks (The Economist, 2016a). NATO StratCom analysts also argue that, given enough data, they could infer the total number of future recruits Daesh gathers from platforms such as Twitter, and also deduce the total number of fighters on the ground, some of their attributes (age, gender, level of education etc.), and thus provide limited predictions on potential tactics and strategies employed (Shaheen).

B. SOCIAL MEDIA AS A FOREIGN POLICY TOOL: THE CASE OF RUSSIA

29. President Vladimir Putin’s Russia exploits and mobilises new and old forms of media through information operations to achieve its foreign policy goals. The Kremlin has "weaponised" information turning media into a weapon of mass deception/distraction and a *de facto* extension of its military and diplomacy. The roots of this strategy can be traced back to the Soviet era when the USSR employed methods such as ‘reflexive control’ and ‘active measures’ to mislead, manipulate and intimidate its opponents in the West. The effectiveness of these methods during the Cold War was limited. However, the rise of the Internet and social media has opened remarkable new opportunities for the Kremlin’s information warfare.

30. Moscow’s intention to use information and cyber space as critical elements of national security is articulated in a number of documents, the most recent being the 2014 Military Doctrine, the 2015 National Security Strategy and the 2015 Information Security Doctrine. These documents portray Russia as a victim of the West’s "information aggression", stress the need to counteract information threats to Russia’s sovereignty and security, and advocate for the development of an effective means to influence public opinion abroad. In his oft-cited article outlining the principles of the hybrid warfare, Russia’s Chief of General Staff Valery Gerasimov pointed out, *inter alia*, that "[t]he information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy" (NATO StratCom, 2015). Speaking at the State Duma on 22 February 2017, Defence Minister Sergey Shoigu announced that “information operations forces have been established that are expected to be a far more effective tool than all we used before for counter-propaganda purposes” (Rettman).

31. According to Timothy Thomas, a renowned expert on Soviet/Russian information warfare, Russia views information war as having two aspects: information-technical and information-psychological. The former includes technological means to collect useful digital data. The latter includes the concept of “psycho viruses” designed to influence the subconscious and behaviour of the population. Another prominent expert on Russia, Mark Galeotti, notes that the Kremlin’s focus on information warfare and other hybrid techniques “reflects the parsimonious opportunism of a weak but ruthless Russia trying to play a great power game without a great power’s resources”. Former Deputy Director of the NSA John Chris Inglis believes that Russia is 10 years ahead of the United States in using social media for information operations (Calabresi).

32. The objectives of Russia’s information warfare are two-fold: 1) for the state to monopolise the information space within Russia in order to "neutralise" external information activities targeting Russians, "particularly young Russians, with the goal of undermining traditional Russian spiritual and moral values"; and 2) to project Russia’s interests abroad using new technological capabilities.

33. In terms of domestic media control, President Putin came to power with the clear agenda of building an unchallenged “power vertical” and gradually subduing all key stakeholders, including media outlets, placing them under the control of the Kremlin. Under President Putin’s watch, Russia’s ratings by Freedom House[5] have progressively deteriorated; the country has been listed in the “not free” category since 2005. Until recently, Internet access in Russia had been essentially unrestricted. However, the freedom of online activities in Russia has been jeopardised by a series of measures adopted in the past few years: the Blogger Registration Law (requiring bloggers with more than 3,000 followers to register as a media outlet; also giving the authorities the right to access user’s information), a law that allows the government to shut down any website (the right

[5] Freedom House is an independent watchdog organisation dedicated to the expansion of freedom and democracy around the world. Freedom House uses a rating system to assess political rights and civil liberties enjoyed by individuals in specific countries. The scores are assigned each year through evaluation by a team of in-house and external analysts and expert advisers from the academic, think tank, and human rights communities. The analysts use a broad range of sources, including news articles, academic analyses, reports from nongovernmental organisations, and individual professional contacts.

was used to block websites of opposition figures Alexey Navalny and Garry Kasparov), the law on personal data storage (requiring Internet service providers who handle Russian customer data to physically keep their servers on Russian soil, thus enabling security institutions to monitor their activities) (Giles) and new ‘anti-terrorism’ legislation that allows government authorities to penalise or even imprison Russian citizens for re-posting or “liking” articles on social media that the regime considered hostile (Gregory). Russia’s government authorities have also enforced a change of ownership of the country’s social media giant *VKontakte*.[6] The founder of *VKontakte* Pavel Durov left the company in 2014, citing difficulties “to remain with those principles on which our social network is based”.

34. Reportedly, Russia is stepping up its cyber cooperation with China and studying the "Great Firewall of China" method to control the Internet. In July 2017, President Putin signed a law that bans the use of so-called virtual private networks (VPNs) and other ‘anonymiser’ technologies. These technologies allowed Internet users to mask their identity by funnelling their online activity through a third-party’s computer. Users were then able to access online material banned by state-controlled internet service providers. By banning VPNs, Russia’s government is essentially able to censor the Internet through a similar approach used to that of China.

35. Finally, pro-Russia hackers and “trolls”[7] regularly target opposition politicians and journalists. This includes frequent “Distributed Denial of Service” attacks against the remnants of free media, such as *Ekho Moskvy* radio station and *Novaya Gazeta* newspaper, and through the online dissemination of compromising materials (*kompromats*) on the regime’s opponents, obtained from Russia’s security services.

36. While consolidating domestic media control, Moscow skilfully exploits the pluralistic nature of the media in Western societies and the fact that Western governments have little control over the media in their countries. The West’s economic and information resources are infinitely greater, but Russia’s disinformation machine appears to have the edge due to its professionalism, lack of scruples and ethical boundaries. RAND experts have characterised Russia’s approach to propaganda as “the firehose of falsehood” because of its two distinctive features: high numbers of channels and messages and a shameless willingness to disseminate partial truths or outright fictions (Paul and Matthews). In recent years, Russia has significantly increased its footprint in global media by spending hundreds of millions of US dollars to enhance its multi-language outlets such as *RT* and *Sputnik*.

37. The Kremlin’s external information strategy is also effective because, unlike the Soviet Union, President Putin’s Russia does not project a clear ideology; its propaganda machine does not have to convince audiences that Russia’s model is superior. *RT* and *Sputnik* do not focus on Russia. The goal is to demoralise and divide Western societies and to establish moral equivalence between Russia and the West by promoting the notion of Western hypocrisy. For instance, the Kremlin’s response to extensive Western reporting that Russia’s parliamentary and presidential elections were rigged was to suggest that elections in other countries are no better (IISS).

[6] The suspected control and exploitation of *VKontakte* by Russia’s security services prompted the Ukrainian government to ban the use of Russian social media platforms on Ukrainian territory.

[7] “Trolls” are individuals who create and manage several fake online identities and accounts in order to promote a certain agenda and to attack opponents in the online media. It has been widely reported that the Russian government has built an army of “trolls.” A “troll farm” in St Petersburg is an oft-cited example, but there are many more such farms across Russia. Trolling activities are becoming increasingly sophisticated, and some of them – for instance, ones referred to as “bikini trolls” by NATO StratCom experts – manage to prompt interaction with their target thus building up a degree of apparent legitimacy and escaping detection by anti-trolling mechanisms. One NATO StratCom project examined 200,000 comments posted on Latvia’s three main online news portals between 29 July and 5 August 2014 and found 1.45% of those comments were from “hybrid trolls”, identified partly by their poor grammar, repetition of content and IP address. But in some stories relating to Russia, more than half of the comments were by Russian “trolls”.

According to Matthew Sussex, an expert in Russian foreign and security policy, "the Russians have picked up that across the West there is a widespread apathy amongst voters and mistrust of politics and government. Anything you can do to increase that distrust serves Russian interests". This approach is also relatively inexpensive as it does not require engaging in time and money-consuming investigative journalism. As a result, while Russia was unable to prevent the deterioration of its global image in the wake of its aggression against Ukraine, its cyber and information activities have still managed to contribute to growing general uncertainty and fragmentation in the West.

38. The explosion in the use of social media provides additional opportunities for Russia to influence populations and politicians in targeted countries. The nature of the social media techniques discussed in this report is conducive to the Kremlin propaganda strategy, which is to confuse rather than convince and to challenge the notion of the existence of objective truth. Russia’s information warriors react to major international events with remarkable speed and reach out to wide international audiences disseminating pro-Kremlin narratives and spreading unverified or falsified stories and conspiracy theories. According to RAND experts, people assume that repeated information from multiple sources must be true, while little attention is paid to the credibility of those sources (Paul and Matthews). In social psychology, this is referred to as the “illusory truth effect”. In the context of social media, where quantity of information becomes affirmation of it, Russia’s information machine is highly effective in capitalising on this trait by widely using "trolls"and "bots"[8] with the aim of achieving its objectives.

39. The Kremlin has engaged in an intensive social media-driven disinformation campaign that was launched during the Euro-Maidan revolution in Ukraine and which continues today. Since 2014, Russia’s online information warriors flooded social media with fabricated reports or doctored images of atrocities allegedly committed by the Ukrainian forces, including the torture and murder of children, the use of civilians for organ trafficking, and even acts of cannibalism. A number of wild conspiracy theories have mushroomed on Russian social media following the downing of Malaysian Air flight MH17 in 2014, with the aim of convincing the public that objective truth about the incident will never be established. Exploiting the fact that information on social media is often conveyed through images, pro-Kremlin widely portrayed Ukraine and Ukrainians in contexts of fascist symbolism and violence. These disinformation campaigns are designed **to confuse and to disinform** social media users. Counter-propaganda teams such as StopFake.org and EU Mythbusters continue exposing Russia’s fake social media reporting on Ukraine almost on a daily basis.

40. Russia’s fake news campaigns on social media have increasingly targeted Western audiences as well. In November 2016, German Chancellor Angela Merkel expressed her concern that "social bots" and “trolls” could be used to sway public opinion during the upcoming electoral campaign in Germany as they were in France and the United States. The head of the German intelligence agency also raised concerns about Russia’s potential interference in Germany's election through the use of fake news. NATO continues to be the target of Russia’s “trolls”, the most recent example being the dissemination of a fake story about a teenage Lithuanian girl raped by a German soldier who was deployed in Lithuania as part of NATO’s enhance Forward Presence (eFP) mission in the Baltic States and Poland. In recent years, Russia has also visibly stepped up its information attacks against its Nordic neighbours Denmark, Sweden and Finland. Russia has also allegedly targeted countries outside of the Euro-Atlantic community. For instance, in May 2017, it was reported that US intelligence and law enforcement officials concluded that pro-Russia hackers were behind a cyber-attack on the Qatar News Agency, planting a fake news story that contributed to a major crisis among several Gulf states and the US.

[8] According to a recent study by the University of Oxford, around 45% of highly active Twitter accounts in Russia are ‘bots’.

41. The Kremlin information warriors use various approaches to spread disinformation: a) through creating multiple social media accounts, including authoritative-sounding ones, such as the Finnish language accounts @Vaalit, @Eduskuntavaalit (Elections, Parliamentary Elections) (Giles), b) by hijacking accounts (e.g., the Twitter account of the Swedish TV4 channel and a Twitter account opened in Swedish Defence Minister Peter Hultqvist's name), and c) by hijacking hashtags (e.g., Russia's MFA used #UnitedforUkraine, hashtag created by the US State Department in support of Ukraine, to post tweets with comments by Foreign Minister Sergey Lavrov).

42. Russia's state-sponsored "trolls" have also been used to **spread panic**: in 2014, a coordinated campaign of hundreds of tweets triggered alarms in the United States by reporting an alleged chemical accident in a Louisiana factory. A New York Times investigation traced the tweets to a location in St. Petersburg. Another example involved terrifying the people of Donbas (Ukraine) who "learned" from social media that the regional water supply had been poisoned (NATO StratCom, 2016a). The success of such disinformation campaigns could encourage similar endeavours on a larger scale in the future.

43. These "trolls" have also conducted orchestrated attacks designed **to intimidate** and silence the Kremlin's critics such as Finnish journalist Jessikka Aro who personally experienced an extraordinary degree of online harassment, including the publication of details of her personal life. Another prominent target was Elliot Higgins, the founder of investigative journalism network *Bellingcat*, which has been reporting on Russia's activities in Ukraine. The pro-Kremlin hacker group *CyberBerkut* hacked his email, iCloud and social media account and posted his personal pictures, a scanned copy of his passport, his girlfriend's name and other private information online. In May 2017, a Canadian research organisation, The Citizens Lab, published a report unmasking a large-scale cyber campaign against more than 200 high-profile Kremlin critics (government officials, journalists and civil society activists) in 39 countries. The goal of this campaign was to steal personal digital data, doctor it and then leak it in order to discredit the victims. Aggressive and intimidating pro-Russia trolling has led several media portals, such as *Reuters* and *CNN*, to close off their comments section. Unfortunately, such policies have also curtailed the possibility of meaningful online debate.

44. Russia targets its adversaries not only on an individual level, but also on an industrial scale. The use of social media, for instance by Western military personnel posted in Ukraine, provides Russia's government agencies and their sympathisers with an opportunity to harvest large amounts of personal data. Pro-Russia information warriors have used such data in the past to harass and intimidate: for instance, in January 2014, when individuals taking part in the Maidan protests in Kyiv were sent threatening SMS messages and in November 2015, when Polish military personnel were telephoned *en masse* (Giles). Pro-Russia hackers have also reportedly sent tailored messages carrying malware to more than 10,000 Twitter users in the Defense Department with the aim of getting access to and control of the victim's phone or computer as well as their Twitter accounts (Calabresi). Now and into the future, the Kremlin will likely continue using these tools to demoralise and incapacitate its adversaries– a particularly important reality for NATO Allies participating in the eFP mission.

45. Finally, social media can **reinforce** messages spread by more **traditional media channels**, such as RT and Sputnik. RT produces a tweet every two minutes, many of them shared hundreds of times. However, the analysis shows that most RT retweets and Facebook post "likes" come from relatively few followers. An analysis shows that of the 50 accounts that most often retweet RT, 16 are probably "bots" (The Economist, 2016b). These manipulations have contributed to reinforcing RT's claim to be one of the world's leading media outlets. It has to be noted that the reinforcing relationship between social and traditional media works both ways. For instance, when Russia's *Ria Novosti* news agency re-published a clearly fabricated report about 3,600 US tanks to be deployed in Poland (the actual number was 87), it gave certain credibility and wider attention to a story that was produced by an obscure group of Donbas-based online propagandists.

46. Russia's use of social media is highly sophisticated and resourceful and poses a real challenge to the Euro-Atlantic community. However, the Kremlin is not invincible in this field. Since the beginning of Russia's aggression against Ukraine, the West has substantially increased its awareness and understanding of Russia's information warfare. Techniques are being developed to identify "trolls" and 'bots' with greater accuracy. In Latvia and Lithuania, for example, communities who label themselves 'elves' are identifying pro-Russia bots and debunking fake news as a volunteer, civilian national guard. Furthermore, social media also presents a certain liability for Russia: the careless use of social media by Russia's soldiers deployed in Donbas and Crimea has provided ample and convincing evidence of Russia's military involvement in Ukraine, discrediting the Kremlin's denials. That said, Russia can be expected to further develop information warfare capabilities and techniques in response to Western counter-measures. Therefore, Russia's information activities are likely to remain one of the key challenges for the Euro-Atlantic community in the foreseeable future.

IV. RESPONSES TO SOCIAL MEDIA'S SECURITY CHALLENGES

47. It is increasingly understood that the challenges of the social media revolution for national and international security are complex and require the combined efforts of international, regional and national authorities and the private sector as well as sub- and trans-national groupings of individual activists. NATO has taken some steps to incorporate the social media dimension into its activities, particularly when it comes to public outreach. NATO has more than 1.2 million followers on Facebook and more than 400,000 on Twitter. NATO's Secretary General, SACEUR and other senior officials have been using social media, some more actively than others. This past spring NATO launched the *We Are NATO* campaign online to "explain NATO's core mission of guaranteeing freedom and security". NATO Assistant Secretary General for Public Diplomacy Tacan Ildem explained that the campaign seeks to educate and inform the younger generations in NATO member states as well as the wider world about NATO's role in global security. According to the NATO Military Public Affairs Policy booklet, NATO personnel are reminded to exercise caution while using social media and "advised to consult with their chain of command before publishing NATO-related information and imagery to the internet." In September 2014, SHAPE adopted a social media directive that identifies best practices for using social media to enhance NATO's engagement with key audiences during peacetime and military operations.

48. Since the Russia-Ukraine conflict, NATO has stepped up its communication capabilities and strengthened its Public Diplomacy Division. It has increased public outreach assistance to partner countries such as Ukraine and Georgia. NATO's "NATO-Russia relations: the facts" website uses facts to debunk myths promoted by the Kremlin on issues such as NATO enlargement or the alleged NATO threat to Russia. In January 2014, several Allied nations took a significant step when they established a NATO Strategic Communications Centre of Excellence in Riga, Latvia. The Centre has produced a series of leading-edge studies that indicate how NATO and its members can counter hostile and disruptive cyber activities.[9] The NATO Science and Technology Organisation has also developed the Digital and Social Media Playbook, a continually-updated, information-environment assessment tool aimed at understanding the goals and methods used by adversaries in the information space.

49. NATO is also beginning to incorporate overt information operations through social media in its military exercises: during Trident Juncture 2015, participants trained on how to quickly produce high volumes of pro-NATO content through official accounts on social media to counter anti-NATO messaging. It was established during this exercise that anti-NATO sentiment decreased gradually as the messaging from pro–NATO voices (in local languages) increased. It needs to be stressed

[9] Recent studies that are particularly relevant in the context of this report are "New Trends in Social Media" (December 2016), "Daesh Recruitment. How the Group Attracts Supporters" (November 2016), "The Kremlin and Daesh information Activities" (October 2016) and "Social media's role in 'Hybrid Strategies'" (September 2016).

that, at this time, NATO doctrine does not foresee the use of covert information operations, such as the use of fake identities, ‘bots’ and ‘trolling’, against target audiences and furthermore, psychological operations in general can only be used in the context of a military operation declared by the North Atlantic Council (NATO StratCom, 2016a).

50. The **EU**’s efforts to counter fake online news and hostile propaganda have been concentrated in two new institutions, East Stratcom Task Force and the Europol’s Internet Referral Unit (IRU). The former, also referred to as EU "Myth-busters", is a team of ten nationally-seconded diplomats, tasked with exposing Russia’s online disinformation on a daily basis. It disseminates its findings on its website–via email and social media platforms. It does not have a separate budget and relies heavily on data provided by a network of more than 400 experts, journalists, officials, NGOs and think tanks in over 30 countries. In November 2016, the European Parliament adopted a resolution calling for an increase in the Task Force’s capabilities. IRU is tasked with monitoring terrorist content on the Internet and social media platforms and working with service providers to flag and remove such content. According to a July 2016 report, the IRU has assessed and referred over 11,000 messages from across 31 online platforms for removal. As a result, the online providers in question removed over 91% of this content (Morelli and Archick).

51. A number of measures have been adopted in recent years on a national level. The **United States’** leading counter-propaganda tool is the State Department’s Global Engagement Centre (GEC), created in 2011 and re-branded and strengthened in 2016. GEC is charged with coordinating US counterterrorism (mainly counter-Daesh) messaging to foreign audiences, primarily by nurturing a global network of ‘positive messengers’, including NGOs and investigative journalists. GEC is quite active on Twitter and its tactics include promoting anti-radical messages using pro-Daesh hashtags such as *#accomplishmentsofISIS*. US authorities have also taken action regarding other security-related uses of social media; they include:

a) a May 2016 Directive signed by former-Director of National Intelligence James Clapper, that permits the collection of publicly-available social-media information on potential federal employees during the security clearance process (it is important to underline that this policy places restrictions on federal agencies to protect privacy rights: for instance, investigators cannot request or require the individual to provide passwords to private accounts, or collect information on individuals other than the individual being investigated unless there is a clear national security concern); and

b) the July 2017 Bill, which was adopted with an overwhelming majority in the US Congress, that imposes additional sanctions on Russia as a result of the US intelligence community’s report in which it concluded that pro-Russia agencies hacked into the servers of the Democratic National Committee and released information with the intent of influencing the outcome of the US presidential election.

It is also worth noting that the US Department of Homeland Security declared the US electoral system as "critical infrastructure, which facilitates the involvement of the Department of Homeland Security in aiding state and local authorities to protect their election systems.

52. In the **United Kingdom**, a dedicated police Counter Terrorism Internet Referral Unit (CTIRU) refers content that it assesses as contravening UK terrorism legislation to industry. Industry voluntarily removes such content if it agrees that there is a breach of its terms and conditions. CTIRU does not remove content itself. Since its inception in February 2010, CTIRU has established relationships with over 200 communication service providers and has secured the removal of more than 260,000 pieces of terrorist-related content. The public broadcaster BBC joined the fight against fake news by boosting *Reality Check*, a fact-checking service that will work with Facebook. In 2015, the British army reportedly created “the 77th Brigade” comprised of experts skilled in using social media to conduct non-lethal information operations and to counter hostile messaging.

53. **Canada**, too, is concerned about fake news and other hostile uses of social media. The House of Commons Standing Committee on Canadian Heritage recently examined this issue as part of a broader study of Canada’s changing media landscape. The Canadian government views the collection of reliable data and identification of international best practices for countering terrorist messaging as core elements of its counter-terrorism strategy. The Canadian Network for Research on Terrorism, Security and Society (TSAS) has been an important element in achieving these goals. Established in 2010 under the auspices of Public Safety Canada, TSAS’s national and international network of affiliated academics have been contributing to the global body of knowledge on terrorist use of social media and counter-narrative strategies.

54. Authorities in Germany, France and the Czech Republic have grown increasingly concerned about attacks on their political systems using social media in the run-up to their national elections in 2017. In December 2016, the **German** Interior Ministry proposed creating a Centre of Defence Against Disinformation to tackle fake news on the internet and to promote a new culture of online behaviour, including the rejection of the use of social media ‘bots’. Eight **French** news organisations, including Agence France-Presse (AFP), BFM TV, *L'Express* and *Le Monde* teamed up with Facebook and Google to launch new fact-checking tools designed to root out fake news. Any news report deemed to be fake by two of the project’s partners would be tagged respectively. The French Newspaper *Le Monde* has also set up a fact-checking unit *Les Décodeurs* and plans to design a hoax-busting database which will enable readers to distinguish fake news sites from verified sites. The **Czech** government has announced the creation of the Centre Against Terrorism and Hybrid Threats, with 20 full-time specialists tasked with tackling disinformation, predominantly about migrants, spread by the Kremlin’s information warriors in what is believed to be an attempt to influence the results of the upcoming elections in October.

55. Given the characteristics of the new global information environment, governmental and traditional media actions alone will not suffice. Responsible action by the handful of **social media companies** that control this medium is critical to the success of the West’s efforts. Recently, major social media companies have launched several new initiatives. This spring, Facebook said it will be hiring 3,000 new staff to flag and track fake content. In December 2016, Facebook, Microsoft, Twitter and YouTube announced the creation of a shared database of “hashes”–unique digital "fingerprints"–for violent terrorist imagery, terrorist recruitment videos and other images that will be removed from these platforms. In June, these four companies announced the creation of the Global Internet Forum to Counter Terrorism, an information-sharing platform among tech giants with the aim of making their services inhospitable to violent extremists. In April 2017, Facebook had taken action against or removed 30,000 fake accounts from its site in France leading up to the French presidential election. Twitter claims to have removed 235,000 accounts for promoting terrorism in the first six months of 2016. Some politicians argue that more could be done. Photo-sharing platform Instagram launched a keyword moderation tool that prevents abusive comments from being posted and curbs the effectiveness of online trolling by automatically hiding comments that contain inappropriate and/or offensive words as pre-determined by the account holder. The Google Chrome web browser introduced a new extension called *First Draft NewsCheck*, helping users with the authentication of images and videos and enabling the sharing of findings with other users. Google is also collaborating with YouTube on a programme called the Redirect Method to target aspiring Daesh recruits and ultimately dissuade them from joining the group. Using keywords and phrases that people attracted to Daesh commonly search for, this programme redirects users to Arabic- and English-language YouTube clips like testimonials from former extremists, imams denouncing Daesh’s corruption of Islam, and clips depicting the dysfunctional nature of Daesh’s so-called Caliphate.

56. While social media companies are taking actions to remove terrorist-related content, there is a growing pressure on them to do more in this area. In May 2017, the Home Affairs Select Committee of the British parliament published a report which said that social media firms are "shamefully far" from tackling illegal and dangerous content and repeatedly “failing to remove illegal content when asked to do so". The Committee urged the British government to consider

requiring social media firms to contribute to the cost of the police's Counter-Terrorism Internet referral unit as well as imposing "meaningful fines" for companies which failed to remove illegal content within a strict timeframe.[10] Reportedly, the UK and France are already working on policies to create a new legal liability for tech companies that fail to take action against unacceptable content. In June 2017, German legislators passed the Network Enforcement Act (popularly known as the Facebook law) to fine social media and internet technology companies up to EUR 55 million if those companies do not remove malicious content within 24 hours of it being posted.

57. Meanwhile, some experts have questioned the effectiveness of these new policies. For instance, some are sceptical of industry information-sharing platforms noting that social media firms remain competitors and there is no commercial incentive for them to share information. As well, free speech advocates such as Joe McNamee, executive director of European Digital Rights, are concerned about proposals that give private companies the discretion and responsibility for deciding what content is good for the public interest; they believe that such initiatives could backfire. Social media operatives may also lack the expertise required to determine whether or not they are dealing with terrorists. For instance, recently Facebook mistakenly censored a group of supporters of Chechen independence, *Independence for Chechnya!,* by labelling these government dissidents as terrorists.

V. CONCLUSIONS AND RECOMMENDATIONS

58. Like every major technological invention, the explosion of social media presents both challenges and opportunities. Hostile non-state actors and aggressive authoritarian states have shown a remarkable ability and willingness to exploit this new medium to pursue their agenda. The Euro-Atlantic community's response so far can be described as haphazard, uncoordinated and irresolute. To a degree, this has to do with ethical and legal constraints pertaining to democratic societies. Nevertheless, there are a number of steps that the Euro-Atlantic nations should seriously consider in order to better adapt to the new realities of the information age.

59. The populace, and especially the younger generation, need to be taught to be cautious about manipulation on social media. Techniques are being developed to recognise the use of trolls and 'bots' and these techniques should be widely shared—similar to those being implemented in Swedish primary schools, where efforts to improve digital competence also include teaching children how to differentiate between reliable and unreliable sources. With respect to protecting the electoral process, governments, political parties, and electoral commissions should study best practices such as the approach used by France's new President, Emmanuel Macron, whose skilled technical team thwarted the Kremlin's attempts to harm his campaign. Social media users should also be familiar with best practices, including the security measures to protect their private information. Schools and the mainstream media should promote the value of genuine, fact-based debate and critical thinking, encourage social media users to come out of their virtual bubbles, expand their interactions on social media and engage in constructive exchanges with people holding different views.

60. In the age of information overflow, people will continue to look for trusted information sources. Responsible media can remain competitive, provided that it embraces innovative technological solutions to help assess the veracity of social media messages with 'breaking news' potential. For instance, UK-based international news agency *Reuters* developed an algorithm based on how many people follow the source of the news and the structure of messages themselves. This gives *Reuters* enough confidence to tweet a breaking news story itself - thereby

[10] In response, in June 2017, Facebook launched the Online Civil Courage Initiative, designed to train organisations about how to monitor and respond to extremist content. Facebook also created a dedicated support desk where concerns can be flagged. https://www.theguardian.com/technology/2017/jun/23/facebook-launches-drive-in-uk-to-tackle-online-extremist-material.

staying relevant in the fast-paced information environment. As NATO Deputy Assistant Secretary General Jamie Shea put it: “The [traditional] media must not be bullied into silence but focus on traditional reporting and fact checking. A disoriented public will turn back to quality journalism—provided it still exists. Governments must empower press councils to enforce objective standards in the media by exposing and penalising outlets that deliberately convey fake news”.

61. NATO member states, that have not yet done so, should create or designate specific government units to conduct – in cooperation with social media companies – round-the-clock monitoring of detrimental uses of social media, exposing fake news and hostile propaganda, and countering them with facts. Academic research and think tanks specialising in online communications should be further supported in order to stay ahead of the curve. Existing NATO and EU capabilities such as NATO’s Public Diplomacy Division and the EU’s East Stratcom Task Force should be provided with additional financial and technological capabilities as well as human resources to continue providing credible online responses as often as possible (even if matching the speed of fake news reporting might never be feasible). Policy towards classified intelligence information should be revisited to allow public diplomacy officers to use less sensitive information, including satellite imagery, in order to refute disinformation.

62. Euro-Atlantic institutions should routinely revisit their social media policies, adjust the content and the format of their communications to the needs of mobile users (messages should be short, coherent, graphic, targeted and numerous), and incorporate social media aspects in training and exercises for their personnel. Defensive measures to protect the identity and home addresses of soldiers’ families should be put in place across the Alliance. In military headquarters, a capacity to utilise social media should be built into every level of command rather than reserved exclusively to public affairs and intelligence officers. With due caution, social media and messaging platforms could offer convenient and user-friendly options for command and control – the FBI-Apple decryption dispute suggests that commercial security protocols are at least as efficient as many governmental ones (Tunnicliffe & Tatham, 2017).

63. In addition to the heightened social media presence of those spreading a democratic, moderate and facts-based narrative, certain restrictive measures are also necessary to curtail the social media activity of terrorists and state-sponsored trolls. As RAND put it, “don’t expect to counter the firehose of falsehood with the squirt gun of truth” (Paul and Matthews). Cooperation with social media industry in order to remove the extremist contents, hate speech and fake news from online platforms should continue, and the most influential information warriors, for instance Russia’s chief propagandists, should be subjected to Western sanctions.

64. In the case of Daesh’s core-periphery social media structure, NATO StratCom experts suggest focusing on removing entire clusters of accounts associated with Daesh, whether they are active or inactive, in order to prevent idle accounts taking over propaganda broadcasting when the active ones are closed. This approach would increase the incremental transaction costs for terrorists’ social media activities, forcing them to continually rebuild their infrastructure from the ground up (Shaheen). These activities of security services also need to be better coordinated across the Euro-Atlantic community.

65. Since most social media tools are owned by private, multi-national companies, cooperation with these companies needs to improve. National measures to take down unlawful content are often ineffective because, in most cases, this content is hosted beyond national borders. It is therefore important that the voluntary development and use of anti-trolling and fact-checking software as well as increasing network monitoring by industry be incentivised. To pre-empt excessive governmental regulations of the cyber domain, it would be preferable if social media companies were to adopt strict internal policies themselves. Social media companies should also continue revisiting some of their newly created tools to identify harmful content[11] to make sure they

[11] For instance, experts note that Facebook’s early efforts to debunk disinformation by marking a story

are not counter-productive as well as adapting algorithms to boost good investigative journalism rather than sensationalist titles. While demanding that social media platforms such as Twitter and Facebook assume greater responsibilities in removing terrorist messaging and fake news, Western governments should do so in a constructive and cooperative manner. One must take into account the fact that Western companies do not have a monopoly over social media, and that users can quickly migrate to other platforms, such as the acclaimed, China-based WeChat (although it is currently mainly tailored for the Chinese market). Governments should help train social media operatives to increase their competencies in recognising terrorist and extremist content and activities.

66. Civil society is a powerful ally of democratic governments in fighting extremism and fake news. Support for grassroots initiatives such as Stopfake.org (to expose the Kremlin’s fake news) and the mobilisation of credible local leaders as well as ‘elves’ (the volunteer hunters of “trolls”) could give Western societies the edge in the information space.

67. While the West may have invented social media, their genesis never promised that their networks or users would adopt Western values. Countering these new threats should be elevated to the top of the Euro-Atlantic community’s agenda. Terrorist and other hostile uses of social media have already resulted in the loss of human life, and have threatened to weaken and divide the Western world. Yet, it is important for the Euro-Atlantic community to maintain the higher moral ground in social media use and to refrain from using the methods of its unscrupulous opponents. Openness, pluralism and inclusion are key to separating truth from falsehood.[12] The Rapporteur hopes that this report will contribute to a growing realisation of the magnitude of this challenge.

“disputed” seem to have driven more traffic to these stories. Facebook was urged to call a spade a spade and change that designation to “false.” - http://www.atlanticcouncil.org/blogs/ukrainealert/will-facebook-finally-fight-disinformation-or-just-make-things-worse

[12] The architecture of Wikipedia is a case in point: its largely accurate content is a result of the ability of anyone to contribute material, and anyone to challenge that material by providing verifiable sources. During this open process, numerous revisions lead to reduced biases, inconsistencies and inaccuracies in Wikipedia’s content.

SELECTED BIBLIOGRAPHY

Adornato, Anthony C. “Forces at the Gate: Social Media’s Influence on Editorial and Production Decisions in Local Television Newsrooms.” *SAGE*, vol. 10, no. 2, 2016.

Alexander, Lawrence, and Craig Silverman. “How Teens In The Balkans Are Duping Trump Supporters With Fake News.” BuzzFeed, 4 November 2016. https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.

Anderson, Monica. “More Americans Are Using Social Media to Connect with Politicians.” Pew Research Center, 19 May 2015. http://www.pewresearch.org/fact-tank/2015/05/19/more-americans-are-using-social-media-to-connect-with-politicians/.

Ansley, Rachel. “Trump Must Stand Up to Russian Cyberattacks.” Atlantic Council, 11 January 2017.http://www.atlanticcouncil.org/blogs/new-atlanticist/trump-must-stand-up-to-russian-cyberattacks.

Bodine-Baron, Elizabeth, Todd Helmus, Madeline Magnuson and Zev Winkelman. Examining ISIS Support and Opposition Networks on Twitter. RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1328.html. Also available in print form.

Calabresi, Massimo. “Inside Russia’s Social Media War on America.” *Time*, 18 May 2017. http://time.com/4783932/inside-russia-social-media-war-america/.

Carafano, James Jay. “Twitter Kills: How Online Networks Became a National-Security Threat.” Text. The Heritage Foundation, 8 June 2015. http://www.heritage.org/defense/commentary/twitter-kills-how-online-networks-became-national-security-threat.

Duggan, Maeve, and Aaron Smith. “The Political Environment on Social Media.” Pew Research Center, 25 October 2016.

The Economist. “Extreme Tweeting.” 19 November 2015. http://www.economist.com/news/europe/21678828-few-social-media-stars-among-europes-politicians-are-centrists-extreme-tweeting.

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.

The Economist. “Tweetaganda.” The Economist, 10 September 2016b. http://www.economist.com/news/europe/21706534-tweetaganda.

Farwell, James P. “The Media Strategy of ISIS,” 1 December 2014. https://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-%20december-2014-january-2015-bf83/56-6-04-farwell-97ca.

Giles, Keir. “The Next Phase of Russian Information Warfare,” 2016. http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

Gottfried, Jeffrey, and Elisa Shearer. “News Use Across Social Media Platforms 2016.” Pew Research Center’s Journalism Project, 26 May 2016. http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/.

Gregory, Paul Roderick. “Under Russia’s New Extremism Laws, Liking My Writings On Ukraine Could Mean Jail Terms.” Forbes, 29 August 2016. http://www.forbes.com/sites/paulroderickgregory/2016/08/29/under-russias-new-extremism-laws-liking-my-writings-on-ukraine-could-mean-jail-terms/.

Guilbeault, Douglas, and Samuel Woolley. “How Twitter Bots Are Shaping the Election.” The Atlantic, 1 November 2016. https://www.theatlantic.com/technology/archive/2016/11/election-bots/506072/.

International Institute of Security Studies (IISS). “Information Warfare and the US Presidential Election,” 12 September 2016. https://www.iiss.org/publications/survival/sections/2016-5e13/survival--global-politics-and-strategy-october-november-2016-ff0a/58-5-03-inkster-bafe.

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.

Lee, Timothy B. “Facebook’s Fake News Problem, Explained.” Vox, 16 November 2016. http://www.vox.com/new-money/2016/11/16/13637310/facebook-fake-news-explained

Lynch, Marc. “After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State.” Perspectives on Politics vol. 9, no. 2, 3 June 2011.

Margetts, Helen, Peter John, Scott Hale, and Taha Yasseri. “Political Turbulence: How Social Media Shape Collective Action.” *Princeton University Press*, 11 January 2017. http://press.princeton.edu/titles/10582.html.

Matejic, Nicole. “Content Wars: Daesh’s Sophisticated Use of Communications.” NATO Review, 2016. http://www.nato.int/docu/review/2016/Also-in-2016/wars-media-daesh-communications-solis/EN/index.htm.

Morelli, Vincent L., and Kristin Archick. “European Union Efforts to Counter Disinformation.” Congressional Research Service, 1 December 2016. https://fas.org/sgp/crs/row/IN10614.pdf.

NATO Strategic Communications Centre of Excellence (StratCom). “Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia,” 2015. http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0.

NATO Strategic Communications Centre of Excellence (Stratcom). “Social Media as a Tool of Hybrid Warfare,” May 2016a. http://www.stratcomcoe.org/social-media-tool-hybrid-warfare.

NATO Strategic Communications Centre of Excellence (Stratcom). “Daesh Recruitment: How the Group Attracts Supporters,” November 2016b. http://www.stratcomcoe.org/daesh-recruitment-how-group-attracts-supporters-0.

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

Nissen, Thomas Elkjer. “#TheWeaponizationOfSocialMedia: @Characteristics_of_Contemporary_Conflicts.” Royal Danish Defence College, 2015. http://www.fak.dk/publikationer/Documents/The%20Weaponization%20of%20Social%20Media.pdf?pd%20fdl=theweaponizationofsocialmedia?pdfdl=TheWeaponizationOfSocialMedia.

Paul, Christopher and Miriam Matthews. The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation, 2016. https://www.rand.org/pubs/perspectives/PE198.html.

Pettigrew, Erin. “How Facebook Saw Trump Coming When No One Else Did.” 9 November 2016. https://medium.com/@erinpettigrew/how-facebook-saw-trump-coming-when-no-one-else-did-84cd6b4e0d8e.

Polonski, Vyacheslav. “Impact of Social Media on the Outcome of the EU Referendum.” The Centre for the Study of Journalism, Culture and Community, July 2016.

Rettman, Andrew. “Russian Military Creates ‘Information Force,’” 23 February 2017. https://euobserver.com/foreign/137004.

Ruane, Kathleen Ann. “The Advocacy of Terrorism on the Internet Freedom of Speech Issues and the Material Support Statutes.” Congressional Research Service, 8 September 2016. https://fas.org/sgp/crs/terror/R44626.pdf.

Schmitt, Eric. “U.S. Intensifies Effort to Blunt ISIS’ Message.” The New York Times, 16 February 2015. https://www.nytimes.com/2015/02/17/world/middleeast/us-intensifies-effort-to-blunt-isis-message.html.

Schultz, Teri. “Why the ‘Fake Rape’ Story against German NATO Forces Fell Flat in Lithuania.” DW.COM, 23 February 2017. http://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870.

Shaheen, Joseph. “Network of Terror: How Daesh Uses Adaptive Social Networks to Spread Its Message,” November 2015. http://stratcomcoe.org/network-terror-how-daesh-uses-adaptive-social-networks-spread-its-message.

Shane, Scott. “From Headline to Photograph, a Fake News Masterpiece,” The New York Times, 18 January 2017. https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html.

Thompson, Alex. “Journalists and Trump Voters Live in Separate Online Bubbles, MIT Analysis Shows,” 8 December 2016. https://news.vice.com/story/journalists-and-trump-voters-live-in-separate-online-bubbles-mit-analysis-shows.

Travis, Alan. “MPs Say Facebook, Twitter and YouTube ‘Consciously Failing’ to Tackle Extremism.” The Guardian, 25 August 2016, https://www.theguardian.com/politics/2016/aug/25/mps-facebook-twitter-youtube-extremism-isis.

Tunnicliffe, I., & Tatham, S. (2017, April 21). *Social Media—The Vital Ground: Can We Hold It?* Retrieved from The US Army war College: https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1349

Wakefield, Jane. “Social Media ‘Outstrips TV’ as News Source for Young People.” BBC News, 15 June 2016, sec. Technology. http://www.bbc.com/news/uk-36528256.