THE CYBER DEFENSE REVIEW

Social Media—From Social Exchange to Battlefield

Author(s): Beata Biały

Source: *The Cyber Defense Review*, Vol. 2, No. 2 (SUMMER 2017), pp. 69-90

Published by: Army Cyber Institute

Stable URL: https://www.jstor.org/stable/10.2307/26267344

Social Media—From Social Exchange to Battlefield

Beata Biały

INTRODUCTION

SOCIAL MEDIA—BEGINNINGS

When discussing the origins of social media, researchers usually start in the 1980s and the Bulletin Board Systems (BBS). They were a kind of online meeting room that allowed users to download games and other files, and leave messages to co-users. The social aspect of this exchange was pretty clear, but the interaction was rather limited and slow due to technological reasons. What is more important, the social interaction had a rather random character—people did not know who was sitting at the other end of the telephone line.

However, BBS proved a growing interest in this kind of communication and inspired other platforms to emerge from the early Internet. The big success of sites like *Classmates.com* confirmed the need for a virtual exchange of memories, ideas, and views. This time, users could enter into social interaction with precisely chosen people, and create networks of "friends", based on their common school experience. *Classmates.com* has equivalents in countries all over the world. The best example is the webpage *Odnoklasniki* (classmates), which is very popular in Russia and other former Soviet, Russian-speaking countries of Ukraine, Kyrgyzstan, Uzbekistan, and Georgia.

The second half of the 1990s has numerous examples of emerging platforms built on a similar principle, for example, *SixDegrees.com* (founded in 1997). But the real social network revolution started at the beginning of the 2000s when the *Friendster* website was launched. After just one year it had gathered a community of three million users (the first site with such a big audience). "Participatory culture" became a buzzword, enhanced by dynamic technological development. Different platforms were founded, using different "sociality" models. A particularly interesting example is *Linked-In* (2003) which is a platform for professional networking, where one's contacts were not friends

Beata Biały is a senior expert at the NATO Strategic Communications Centre of Excellence. She is a graduate of the Warsaw University in French Philology and Business Administration and completed an MBA program of the University of Illinois Urbana-Champaign. Before her civil service career, she worked as a manager in Polish media for 15 years. Beata was deputy CEO for one of the leading dailies publishing groups and deputy director of Polskie Radio Channel One. As a civil servant, she worked in the Polish Ministry of Transport where she was in charge of EU affairs, and later as director of Public Affairs Department for the Ministry of National Defence. She was responsible for creating the Strategic Communication structure in the Polish MOD and represented Poland in the NATO STRATCOM COE Steering Committee. Beata has been pursuing her passion for literature by writing books, and translating more than twenty French and English literature books.

but professional connections. It is interesting to note that *LinkedIn* has kept this particular character until the present day.

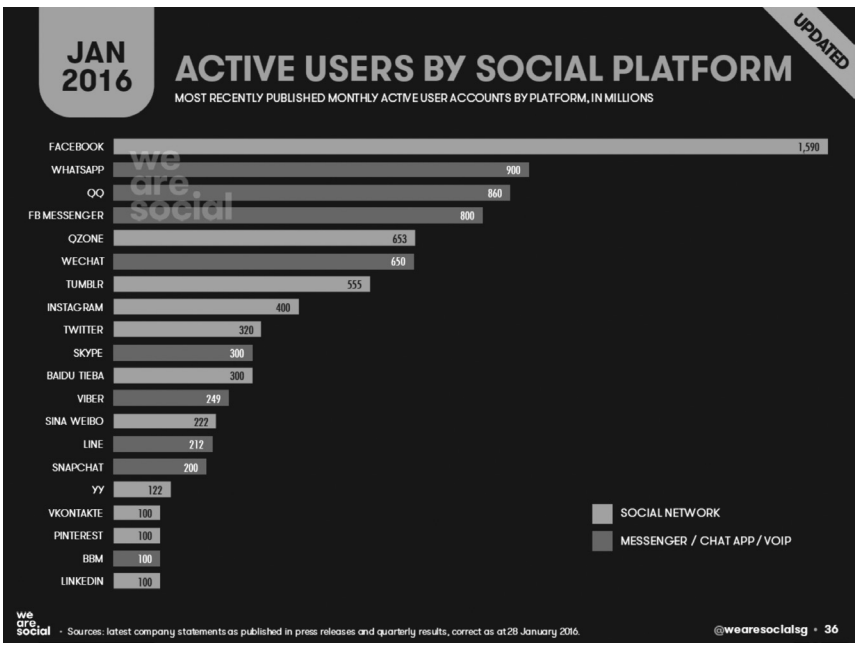
One year after *LinkedIn* was launched, Mark Zuckerberg and his Harvard University classmates, created the site *thefacebook.com* which evolved into one of the most powerful and successful social media platforms in the world with over 2 billion active users in September 2016.[1] It is user-friendly, with many easily accessible features, it has become a global brand, deserving the recognition: if you are not on *Facebook,* very likely you don't exist. *Facebook* also introduced the "like" click, which was an excellent addition, allowing users to easily express their emotions, thereby underlining the platform's social character.[2]

Created in 2006, *Twitter* focused on network conversation. Thanks to the introduction of a "hashtag" feature, users' 140-character messages can be easily tracked and grouped, which is vital on a site where every second an average of 6000 tweets are posted (about 200 billion tweets per year). Among its 313 million active users[3] (over 1.3 billion accounts) are politicians (according to some statistics, 83% of the world leaders have an account on *Twitter*[4]), journalists (24.6% of all accounts[5]), information agencies, and companies.

At more or less the same time, the online community witnessed the creation of such platforms as *Myspace, YouTube,* and *Google+,* closely followed by *Instagram*, *Snapchat,* and dozens of others. The recent appearance of mobile technology has strongly affected users' behavior and forced social media platforms to adapt to this new environment by introducing mobile applications. At the beginning of 2016, more than 2.3 billion people were using social media: of these, 1.9 billion users were accessing social media via their mobile phone.[6] Mobile

technology enhanced in particular the development of photo- and video-sharing platforms, such as *Instagram* or *Snapchat,* entertainment location apps (e.g. *Foursquare*), dating services (like *Tinder*), and last, but not least, direct messaging applications (like *WhatsApp*). [7]

The social media landscape is far from stable. For the last few years, companies like *Facebook, Twitter* and *Google* have been massively investing in new platforms. Big acquisitions have taken place–*Instagram* and *WhatsApp* were purchased by *Facebook, Twitter* acquired *Vine* (in October 2016, Twitter decided to close the service when it did not meet expectations), and *Google* purchased *YouTube.* The social media landscape has been evolving from relatively small local services (initially *Facebook* was dedicated exclusively to Harvard University students) to powerful companies with global reach. From more than 2.3 billion social media users (data from 2016) [8] nearly 1.6 billion have chosen *Facebook,* giving it the clear position of market leader. In the US, 79% of online adults (68% of all adults) use *Facebook,* 32% – *Instagram,* 31% – *Pinterest,* 29% – *LinkedIn,* and 24% – *Twitter.* [9]



Over time, social media platforms have become huge pools of data for advertising and marketing companies. Within the last three years, *Facebook* alone noted a 120% increase of brands placing paid promotion on the platform. Social media companies have also developed e-commerce features, allowing their users to shop directly from the social media website, following the example and advice of social network "friends". [10] Social and commercial activities have become two powerful drivers of social media platform development.

When it comes to data, it is worth dedicating a few lines to the concepts of Big Data and social media mining. As the authors of the book "Social Media Mining" state, "social media data is undoubtedly big," [11] which is only one of many challenges that must be faced by those who want to explore it. The others are the unstructured character of data, its noisiness, and social relations hidden there with friends, connections, following–followers.

These particular characteristics call for data analysis methods, which can encompass an understanding of user-generated content, including a wide range of social relations. This technique, termed social media mining, draws on the different disciplines of computer science, machine learning, social network analysis, statistics, sociology, and many others, as well as interdisciplinary concepts and theories.

Social media mining "searches for hidden patterns and relationships correlations, in addition to interdependencies that exist within large databases that the traditional information gathering methods (...) may fail to notice". [11] It aims at discovering the relations between "social atoms" (individual users), "social entities" (content, sites, networks), and interactions between the two previous categories. [13] It helps to identify communities on a social network and determine who the most important people are in a social network (the influencers).

Social media mining, draws on the different disciplines of computer science, machine learning, social network analysis, statistics, sociology, and many others.

Such analysis is useful for marketing purposes, by targeting users who are likely to effectively disseminate brand awareness and increase the reach of potential customers. In a similar way, social media mining can be used by other actors, who aim to build advocacy for their narrative. Some experts' claim that it is useful for predicting future behavior of given groups (e.g. terrorists), based on a special algorithm. [14] In any case, Big Data and social media mining are two emerging concepts with a breathtaking future.

FROM SOCIAL EXCHANGE TO SEARCHING FOR CONTENT

The appearance of social media offered Internet users an unprecedented opportunity to connect with other people. The exchange of memories, experiences, opinions, views and agendas became easy and–over time–very cheap. Suddenly, one could find former classmates and reestablish regular contact and also discover new "friends" in dynamically growing social networks. And these "friends" could come from any part of the globe with Internet access, which means from almost all over the world.

Obviously, there can be various motivations for using social networks. In April 2015, *Global Web Index* published a report presenting the reasons why people use social media (see the next chart). Among the top ten, reason number one is clearly "social"—"to stay in touch with what my friends are doing". There are also other responses on the list, like sharing one's opinion or details of one's private life, sharing pictures or videos, networking with people, meeting new people, and being there "because a lot of my friends are on it"—all of these show high social motivation. But it is worth noting number two on the list—"to stay up-to-date with news and current events", which has nothing to do with the social character of "social networking services" (as it was stated in the survey question). Looking for information, not necessarily about friends, but for information in general, has been a growing trend among social media users. Social networks are more and more considered a source of content, although this content is generated by the users themselves.

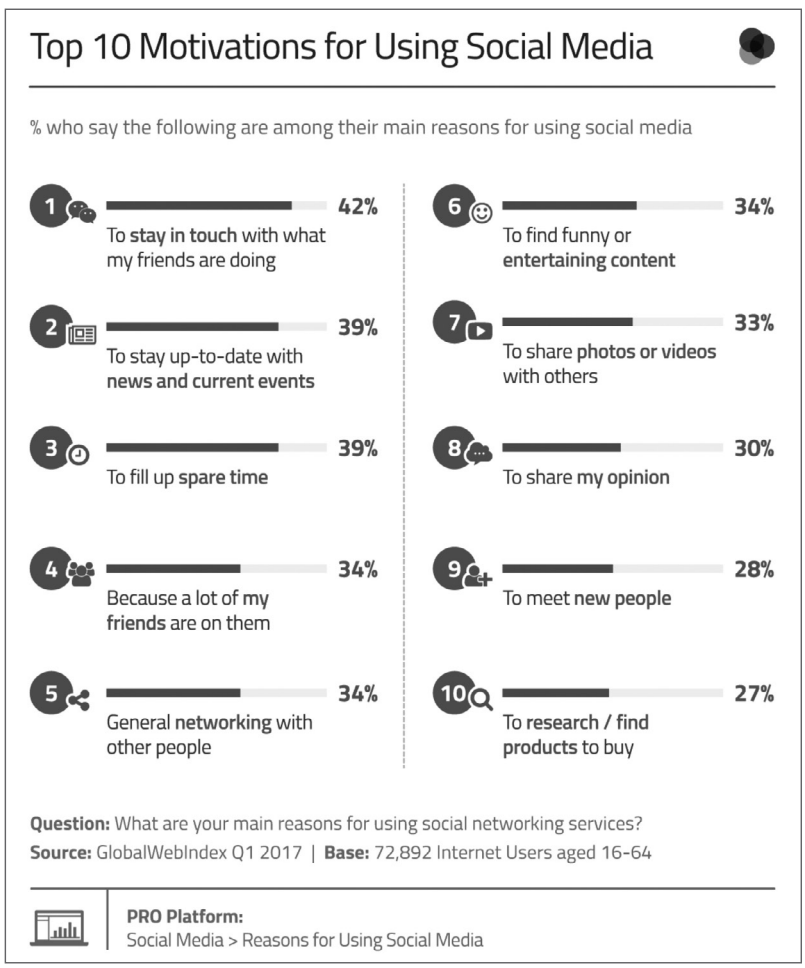


Figure 1. Source: http://www.globalwebindex.net/blog/top-10-reasons-for-using-social-media

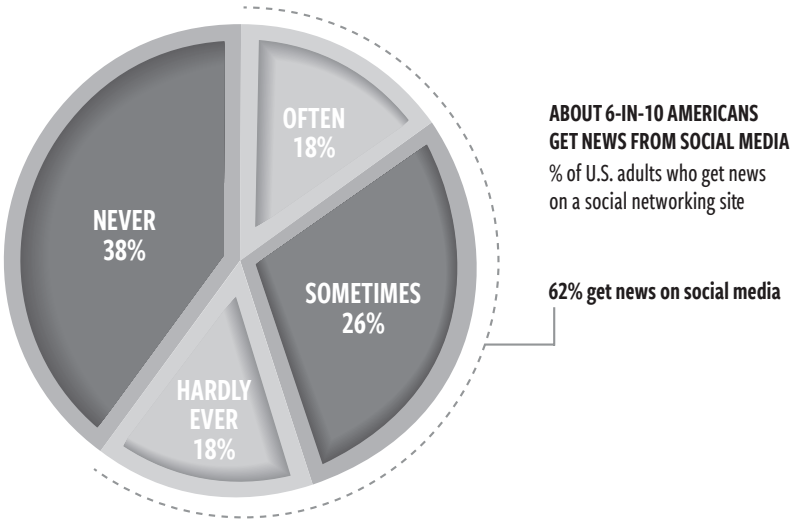


Figure 2. Source: Survey conducted January 12- February 8, 2016. "News Use Across Social Media Platforms 2016" **Pew Research Center**

This trend was also observed by researchers from SWOCC (research organization linked to the department of communication studies at the University of Amsterdam). Their study, carried out in 2016, showed that users' perceptions of social media had changed considerably. Some platforms are perceived as being less "social", and more "informative" (e.g. *Twitter*). Other research from 2016, conducted by Pew Research Center, concludes that 62% of US adults are getting their news from social media. The growing trend seems obvious, in 2012, this number was 49%.

Although it would be risky to say that social media platforms have become a direct competitor to mainstream media, their role in the flow of information is prominent. What is more, they have become a source of content for traditional media. Information agencies and journalists establish their *Twitter* or *Facebook* accounts not only to disseminate their message but also to hunt for news posted by other social media users. In such a way, information generated by a "grassroots journalist" [15] can obtain an unexpectedly large reach. This can become problematic if the news appears to be inaccurate or simply fake. An excellent example of such misinformation is the "Senator Cirenga case"; a sensational post on the *Facebook* account of a non-existent Italian senator, which was used and covered by several newspapers, and turned out to be untrue. [16]

The above-mentioned example shows how challenging and risky it is for an Internet user to consider social media a source of information. Easy access, the possibility of anonymity, and no gatekeepers are a dangerous mix. In traditional media, journalists are supposed to observe the rules of the profession, and editors check if an article meets the standards of accuracy, and reliability, then decide if it can be published. On social media, anybody can become a 'journalist' and, anything can become 'news'.

FROM SOCIAL EXCHANGE TO BATTLEFIELD

Over the last six years, the number of social media users increased more than twofold (0.97 billion in 2010 to 2.34 billion in 2016 [17]). These numbers, together with changing usage patterns, have made social media a very attractive communication channel. Low access cost, various target audiences, global reach, and the unprecedented speed of information flow—all these factors encourage different actors to use social media for their purposes. Marketing experts discovered its potential very quickly and placed social media in the heart of their promotion campaigns. But they were not the only ones.

Because, apart from its monetizing potential, social media has also become an excellent channel to mobilize support, disseminate narratives, wage information operations, or even coordinate military operations in the real world. States and non-state actors have started to extensively use social media to influence perception, beliefs, opinions and behaviors of their target audiences. Although social media has been a very useful communication channel to support legitimate and worthy actions (such as humanitarian aid in disaster areas), it is more and more used for other, far less noble aims. The chart below, from Dr. Rebecca Goolsby's article on social cyberattacks [18], shows how social media conversations can be used for different purposes.

ON CYBERSECURITY, CROWDSOURCING, AND SOCIAL CYBERATTACK

CRISIS RESPONSE	COMMUNITY DIALOGUE	INFLUENCE	SOCIAL CYBERATTACK
Disaster Relief	Anti-Propaganda	Propaganda	Crowd Manipulation
Humanitarian Assistance	Rumor Squelch	Rebellion Cry	Hysteria Propagation
Crisis Monitoring	Community Outreach	Hate Messages	
PROMOTES:	**PROMOTES:**	**PROMOTES:**	**PROMOTES:**
Order and Discourse	Discussion Expansion	Special Point of View	Chaotic Mass Behavior
Cooperative Behavior	Spread of Verifable Information	Bandwagon Effects	Escalation of Rumor
Information Sharing		Conflict and Argument	Confusion, Panic and Violence
		Mass Protests	

Figure 3. Source: Office Of Naval Research Arlington VA http://www.dtic.mil/get-tr-doc/pdf?AD=ADA580185

The recent conflicts in the Middle East and Ukraine demonstrated that social media could be a very useful means to support military operations. Since then, it has been exploited to such an extent that it seems justifiable to call social media an information confrontation battlefield. Obviously, there are many different ways of using social media

for supporting military objectives. Tomas Elkjer Nissen identifies six of them: intelligence collection, (geo-) targeting, cyber operations, command and control, defense, and psychological warfare (inform and influence). [19]

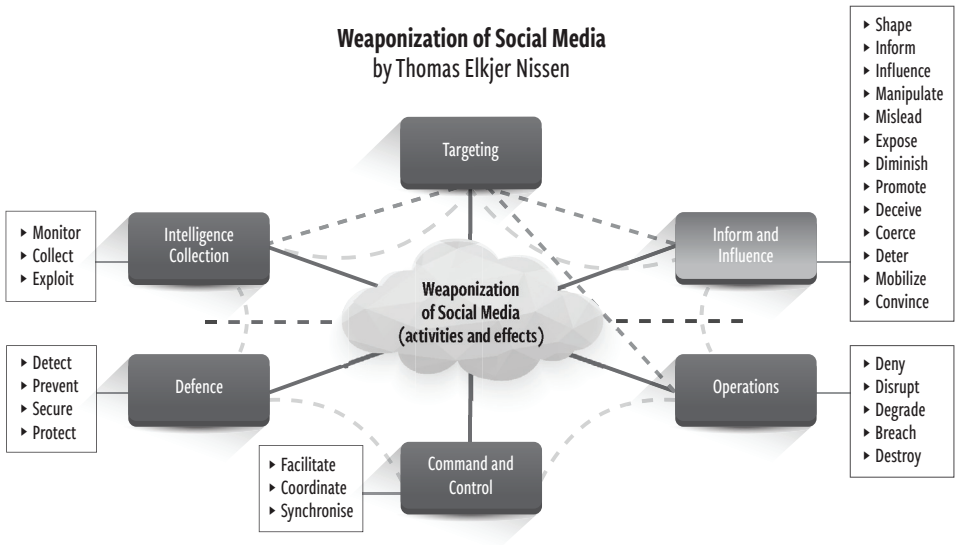


Figure 4. Source: Social Media as a Toll of Hybrid Warfare, NATO Strategic Communications Centre of Excellence, Riga, July 2016, p. 11

Intelligence collection–monitoring and analyzing the information that can be found in social networks, such as social media profiles, specific social media communities, conversations' content and temperature. The collected information can be useful for target audience analysis, which is crucial for planning information operations. It is also helpful for planning kinetic activities on a given theater.

(Geo-) targeting–exploring virtual reality (in this case, social media) to identify targets for military operations carried out in the real world. Such analysis uses geo-tagged pictures, the content of users' conversations, and geo-located data. The risk of geo-targeting has been recognized early-on by different actors. For example, in 2014 the Islamic State of Iraq and the Levant (ISIL) or Daesh prohibited its *Mujahideen* from switching-on the original *Twitter* geo-tagging function. [20]

Cyber operations–breaching passwords, hacking social media or email accounts, altering the content or making some accounts unusable. Cyber operations can be carried out to collect intelligence, prevent other actors from using social networks, sow disinformation and confusion. The picture below shows an example from April 23, 2013 when the Associated Press *Twitter* account was hacked to disseminate a false claim of explosions at the White House. [21]

Figure 5. Source: Twitter @AP The Associated Press

The temporary suspension of the AP account was only a minor effect of this operation. The violent reaction of the Dow Jones Index (see the chart below) is a perfect illustration of serious impact.

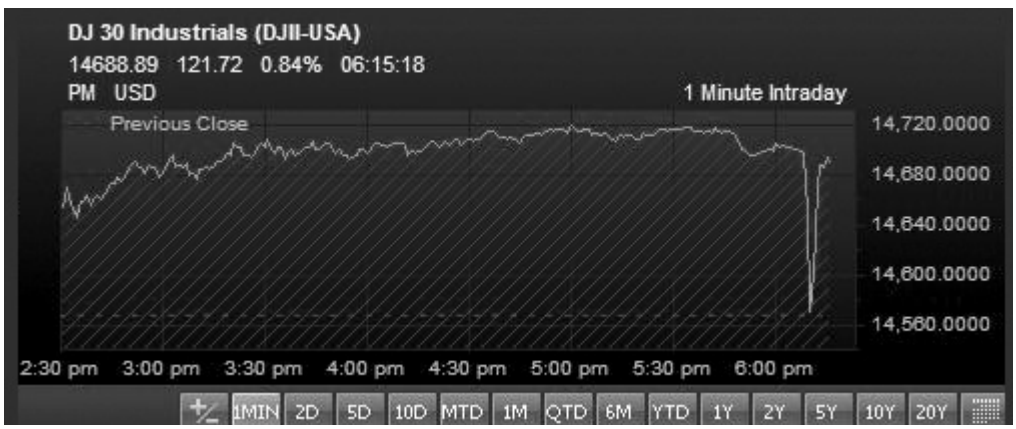


Figure 6. Source: http://www.theverge.com/2013/4/23/4257392/ap-twitter-hacked-claims-explosions-white-house-president-injured

Command and Control (C2)–using social media platforms for internal communication and coordination. Depending on their objectives, different actors can use more or less open networks to synchronize their operations. An especially interesting example is the *PlayStation* game network used by Daesh for coordination of its actions.[22] Obviously, different social media platforms represent varying levels of security. For this reason, actors like terrorist organizations often choose closed networks for their communication. For example, Daesh uses the adaptive structure of its network to defend it against possible infiltration or external influence.

Defense–all kinds of activities whose objective is to protect a given social network against being penetrated by adversaries. This includes such activities as encryption, anti-tracking, IP concealing, or the above-mentioned use of adaptive structures. Joseph Shaheen describes this technique as a DEER process: Dissemination (of public propaganda); Deletion or suspension of the account (by an adversary); Evolution of (network) structure or methods; Expansion of influence or methods; Replenishments of accounts and resources.[23] Defense also means making social media users aware of the risk they encounter by communicating via different social media platforms. An example of such "instruction" is the guide circulated by Daesh in January 2016 (see the chart below) giving Daesh followers' clear indications of platforms considered "safe" and "unsafe".[24]

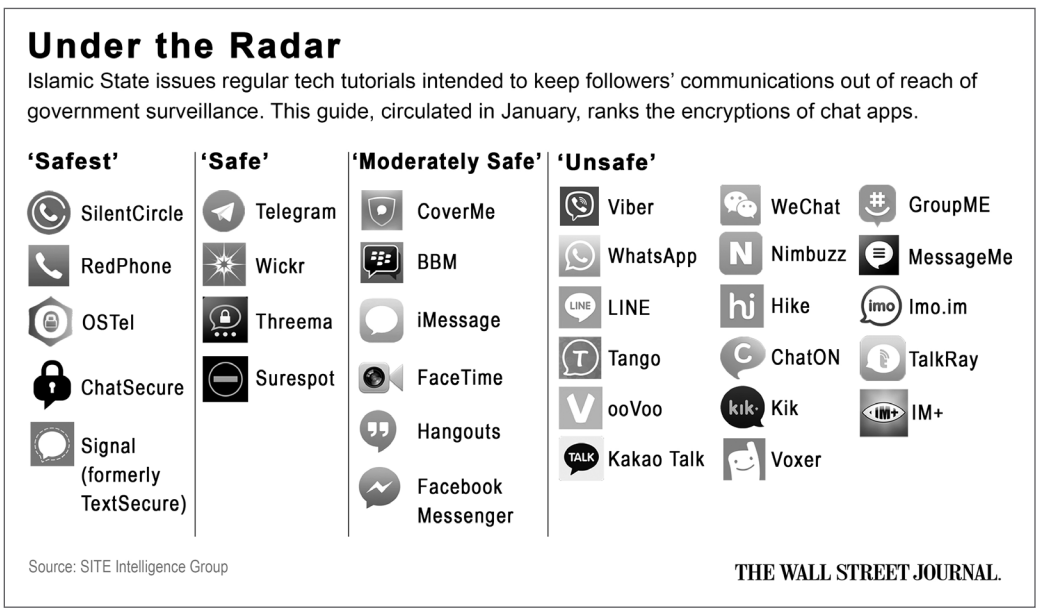


Figure 7. Source: The Wall Street Journal (SITE Intelligence Group)

Psychological warfare (inform and influence)–using social media as the channel for disseminating messages whose objective is to influence (change) target audiences' opinions, beliefs, perceptions, and behaviors. It means achieving some military effect in the cognitive domain using misinformation (including disinformation) and propaganda.

Without minimizing the importance of the first five above mentioned hostile activities, we will examine closely the last one–psychological warfare on social media.

SOCIAL MEDIA—INFORMATION WARFARE BATTLEFIELD

Psychological warfare on social media can take different forms—overt or covert, depending on the target audience and objectives. Overt methods consist of acting via official social media accounts and channels. Covert methods involve creating false accounts, using social media trolls (called by some experts "hybrid trolls [25]) or bots, addressing closed social networks. The second category of activities is abundantly explored by those actors who do not observe democratic legal and ethical standards, such as terrorists or authoritarian states. On the other hand, there are democratic countries and organizations acting according to democratic values and principles, which exclude these kinds of covert activities carried out in peace time.

The social media landscape has been evolving from relatively small local services to powerful companies with global reach.

For example, the NATO Allied Joint Doctrine for Psychological Operations states that "PSYOPS may be conducted ... across the full spectrum of military operations." [26] In the same document, Information Operations are defined as "a staff function that analyzes, plans, assesses and integrates information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries, and North Atlantic Council (NAC) approved audiences in support of Alliance mission objectives." [27] Ergo, psychological operations may only take place in the context of military operations, and the target audiences need to be approved by the highest NATO decision-making body.

In the case of terrorist organizations or authoritarian states, the boundaries between war and peace are often blurred, and covert influence activities are used even if no war has been officially declared. This kind of approach lies at the basis of Russia's information warfare theory. As Dr. Jolanta Darczewska at the Polish Centre for Eastern Studies remarked, this theory had been built in opposition to the western concept of cybersecurity. The latter is mostly about using technology for military and intelligence purposes. Russia's theory understands information warfare as "influencing the consciousness of the masses as part of the rivalry between the different civilizational systems adopted by different countries in the information space by use of special means to control information resources as 'information weapons'". [28] Military and non-military orders are muddled up, and discrepancies between "civilizational systems" are a sufficient justification for carrying out psychological operations in the information space.

In information warfare, actors use different tactics. Ben Nimmo, Information Defense Fellow at the Atlantic Council Digital Forensic Research Lab, singles out four such methods, situating them in the context of the Ukrainian conflict, and calling this set of tactics the "4D Approach". [29] The four Ds stand for dismiss, distort, distract, and dismay.

Dismiss–undermining the opponent, denigrating him, or simply denying uncomfortable facts. An interesting example of this tactic is the use of the term "Russophobe" by Kremlin supporters. If somebody criticizes Russia, he/she automatically becomes Russophobe, which means ignorant, one whose opinions are grounded in prejudices, and therefore not worth noting.

Figure 8. Source: Sputnik's Twitter account

Distort–twisting facts, misinterpreting and putting them out of context, or last but not least, producing a partly or totally false version of reality. This tactic is abundantly used by Kremlin partisans, and its extreme form is the "rewriting of history" extensively present in social media messages posted by pro-Russian users. Another example of this tactic is Daesh propaganda videos disseminated on *YouTube,* which aims to convince the Islamic audience how expertly organized is the "Islamic State's" healthcare, and how much the "ISIL" cares about its citizens and supporters. [30]

Distract–turning the audience's attention away from the actor's activities, and focusing it on activities of the opponent. For example, pointing out that NATO is an aggressive organization that is sending troops all over the world, or accusing the US of expansionist policy when the social network discussion is about Russian annexation of Crimea.

Dismay–frightening the target audience with verbal warnings or disturbing pictures and videos. The Kremlin has mastered this method and uses it broadly both towards the internal and international audience. Kremlin statements about the "adequate response" that will be given by Russia to NATO's or US "aggressive policy" are willingly taken up and repeated in social network discussions. Another example is Daesh propaganda videos showing crucifixions or beheadings of the "unfaithful".

Figure 9. Source: Twitter

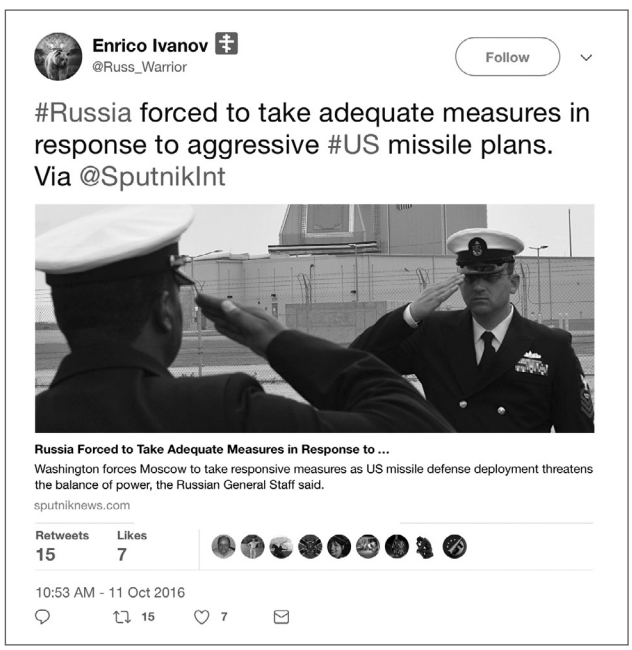


Figure 10. Source: Twitter

Although Ben Nimmo assigned the 4D Approach specifically to Russia, these tactics are also used by other actors, and social media is a very convenient platform for their application. Internet users who more and more frequently consider social media as their main source of information are an attractive target for those who do not hesitate to manipulate or falsify facts and present their version of reality, supporting their particular agenda. To increase effectiveness, they use a variety of techniques and methods, examined below.

METHODS AND TECHNIQUES

One of the most striking characteristics of social media is the high speed of information flow combined with unlimited range, cost-efficiency and availability 24/7. The conversations in social networks can be conducted almost in real time, and—as has already been mentioned—the quantity of messages (posts) appearing on the user's screen can make his/her head swim. This is a big challenge for somebody who wants their message to be visible. Therefore, one of the techniques used by different actors on social media is posting **automatically generated content** or **human generated content which is automatically spread through fake accounts using bots and apps.** Within the last few years, the number of these social media accounts has noticeably increased—according to different studies, at least 8 percent of *Twitter* accounts [31] and between 5 and 11 percent of Facebook accounts are bots. [32] According to *The ISIS Twitter Census,* 20% or more of all Daesh tweets are created using bots or apps. [33] Although social and IT scientists have been inventing more and more effective tools for the detection of bots, the other side has not remained passive with bots becoming more sophisticated, more 'human', and therefore, difficult to discover and eliminate.

Low access cost, various target audiences, global reach, and the unprecedented speed of information flow—all these factors encourage different actors to use social media.

It is important to note **the extensive use of mobile technology** to convey messages directly to users. The mobile revolution mentioned at the beginning of this article creates a great opportunity for those who want to effectively spread their message. The mobile app *Dawn of Glad Tidings* was distributed by *Daesh* to supporters in 2014 and enabled them to use their *Twitter* accounts to automatically tweet *Daesh*-related content. This was the first attempt by the organization to use a mobile app for the automatic distribution of its messages. Although it was closed down by *Twitter* pretty quickly, it was able to mobilize 40,000 people to sign up for the app. Currently, a new Android app is in place allowing the *Daesh* radio *Al-Bayana* to broadcast outside the boundaries of their operating territory. In May 2016,

a new app was developed to teach the alphabet to children, but one can find a large number of references to weapons and *jihad.* [34]

Another technique used to increase the exposure of a given narrative on social media is **trolling.** However, it is important to note the fundamental difference between a "classic" internet troll and a "hybrid" troll. The first category has been present in digital media from the very beginning and designates a particular kind of social media user who, for purely personal reasons (frustration, unhappy life, and psychological problems), tries to disrupt social network conversation by offending other users, provoking, and posting unpleasant comments or comments out of context. The other one is a kind of social media warrior, hired by a state or a non-state organization for supporting this organization's cause and executing its agenda. [35] These "information *spetsnazes*", as they are called by one of the eminent Russian theorists of information warfare, Igor Panarin [36], are tasked to post comments to either promote the narrative of their patron or to destroy the narrative of his opponents. They overwhelm social media with a huge volume of posts, using different manipulative techniques and methods which have enabled researchers to discern a couple of interesting categories of hybrid trolls: "bikini troll", "Wikipedia troll", "aggressive troll", "attachment troll", and "conspiracy troll" (also called "blame the US troll"). [37] The good news is that social media users are not defenseless against hybrid trolls, and a minimum level of awareness and practice can help to detect and expose them. In one of its reports, the NATO Strategic Communications Centre of Excellence published an "Internet Trolling Identification Tutorial" [38] presenting a four-step approach which can help in countering hybrid trolls' activity.

The most striking characteristics of social media is the high speed of information flow combined with unlimited range, cost-efficiency and availability.

Trolling (especially "attachment trolls") **can also be used for conducting cyber operations,** such as intelligence collection. The Latvian Information Technology Security Incident Response Institution (CERT) discovered that pro-Russian trolls were using the comments sections of Latvian web portals to disseminate propaganda and encourage other users to click on web links containing spying malware. [39]

An effective method of increasing the impact of a narrative or specific messages is the **coordinated use of multiple channels**—open and closed. The communication goes through public conversation platforms, such as *Twitter,* and within closed networks, such as encrypted messengers or—as it was mentioned earlier—even via *PlayStation Network* which is extremely challenging for decryption, and more difficult to track than *WhatsApp.* Documents leaked by Edward Snowden in 2013 revealed that the NSA and CIA attempted

to infiltrate terrorist conversations by taking part in games like *World of Warcraft.* [40] Public networks are mainly used for spreading propaganda or misinformation, while closed social networks may be an efficacious channel for coordination of activities (C2), recruitment and the mobilization of support.

An interesting mutation of the above-mentioned technique is the Kremlin's **cross-media communication approach** broadly used in the Ukrainian conflict. The idea consists of feeding the mainstream media with information, mostly fake, posted on social media or—vice-versa—disseminating materials made by pro-Kremlin media (e.g. TV channels controlled by Kremlin or pro-Kremlin websites) via social media conversations. A striking example of this method is the case of "Doctor from Odessa", an alleged emergency physician who described on his *Facebook* account a dramatic story of his fight to save wounded civilians. In the post, the "Doctor from Odessa" he depicted, in a very emotional way, the cruelty of pro-Ukrainian extremists who stopped him from tending to his patients. Although bloggers investigating the "Doctor's" case discovered that such a person did not exist, and the *Facebook* account was blocked, the story immediately became very popular and was covered by the media. [41]

For spreading a given message even further, the cross-media communication approach can also be combined with other techniques, such as the use of botnets. And last, but not least, it has become a general rule to integrate pro-Kremlin online media: Russia Today, and Sputnik with social media (*Twitter,* etc.).

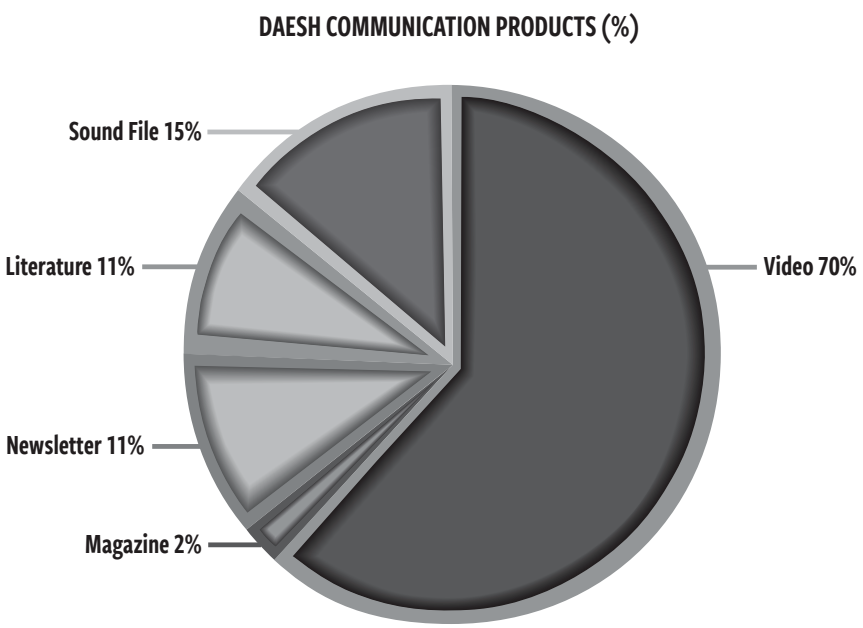


Figure 11. Source: NATO StratCom COE report The DAESH Strategic Narrative, June 2016

To be effective on social media, **attractive, memorable,** and **emotional content** is essential. Different actors, such as Daesh, understand the **primacy of visual content** over verbal messages; it is much easier to capture the audience's attention and achieve its engagement when using images–the most engaging posts on *Facebook* are photos. [42] The majority of *Daesh* products are pictures, videos, games, and music.

An interesting example of such content is *Nasheeds,* chants which are a mixture of religious and social narratives inspiring Daesh supporters. *Nasheeds* are available on the *YouTube* "Best *Nasheed* Channel", and have recently started to appear in different European language versions. [43]

Visual content has two major functions - to impress or to dismay. It rarely has a purely informative character. It is also interesting to note the **significant role played** in psychological warfare **by humoristic drawings and pictures.** A famous example is the picture montage tweeted by the Russian deputy prime minister, Dmitry Rogozin (see below), illustrating the "different values and allies" (original tweet: *У нас разные* ценности *и союзники*) of Russia and the USA, which became rather popular (retweeted 2500 times).

Figure 12. Source: Dimitry Rogozin's Twitter account

CONCLUSIONS: WHAT CAN WE DO?

Social media is one of the most dynamically developing communication platforms. It has been subject to many significant changes, evolving from small, scattered, local community websites, to consolidated companies with global reach. Social media has also witnessed a leap into mobile technology, which has had a tremendous influence on human behavior, including social media usage patterns. Last, but not least, over time, users motivations to participate in discussion on social media have also changed. The purely "social" motivation has been gradually replaced by other motivations, such as the search for information, which has situated social platforms much closer to traditional media.

Social media has also witnessed a leap into mobile technology, which has had a tremendous influence on human behavior.

A dramatic change took place in this information environment that can be called the weaponization of social media, which means transforming social networks into a field of hostile information activities carried out on target audiences in the gray zone between peace and war.

Thanks to its exceptional features, such as global reach, high accessibility, low cost, huge volume and speed of information exchange, and—to some extent—user anonymity, social media is attractive to multiple actors with hostile agendas. Paradoxically, what has been its big advantage, has become a considerable weakness. Platforms which—by definition—were born to be "social", have witnessed a great number of activities having a clearly anti-social character.

Hence, it seems highly justifiable to call social media a battlefield on which an intense fight for hearts and minds is taking place. It is a battlefield where we can observe different military strategies and tactics, such as deception, disinformation, propaganda, threatening opponents, mobilization of supporters, and coordination of actions. The development of technology plays a prominent role, making all those activities easier and more effective. Human actors are extensively assisted or even replaced by bots and apps, and the content (message) becomes—thanks to the development of multimedia—more and more attractive.

The question then arises as to what the democratic world can do to counter hostile activities on social media, and in the information environment in general, given that the adversary does not observe the same legal rules and ethical principles as a democracy, and does not share democratic values. Moreover, the adversary is cunning, fast, flexible and adaptive, due to the particular character of its organization—authoritarian (Kremlin) or dispersed (Daesh), whereas democratic countries and institutions are obliged to follow specific procedures with lengthy decision-making processes.

The challenge is enormous, but the future is not lost. Observation of the social media environment and the activities of "bad actors" enable us to formulate a few key recommendations.

Be present on social media with attractive, well-tailored content. It is a vital part of the information environment, and it should be considered as an obvious element of communication campaigns. Instead of choosing platforms, it is wiser to choose target audiences, and to follow them—they have already chosen their platforms.

Use what technology offers. Our adversaries use it effectively, creating attractive content and disseminating it via multiple channels. "Think mobile" is not just a catchy slogan. Neither is "cross-media activity". But do not forget that "social media is about sociology and psychology more than technology" [44].

Advance your own narrative and develop attractive branding. A well prepared offense is usually a more certain path to victory than defense. When promoting your narrative, be consistent and credible.

Build your brand and narrative advocacy. Find credible voices within the target audiences that can speak for you. Humanitarian organizations' experience with crowdsourcing can serve as a very useful model.

Immunize your audience against psychological operations. It is vital to raise citizens' awareness of the influence activities used by our adversaries. There are two main lines of defense: education and exposure of hostile activities. Education gives citizens (starting from relatively young age) basic knowledge about media and social media that helps build critical thinking and fact-checking habits. Exposure of hostile activities requires tracking online deception, manipulation and disinformation, and neutralizing it with the truth. Because however lofty it may sound, truth is a powerful weapon.

NOTES

1. http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

2. http://www.digitaltrends.com/features/the-history-of-social-networking/.

3. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

4. https://www.brandwatch.com/blog/44-twitter-stats-2016/.

5. Ibidem.

6. Report *New Trends in Social Media,* NATO Strategic Communications Centre of Excellence, Riga, December 2016, 13. All reports of NATO StratCom COE can be found here: http://www.stratcomcoe.org/publications.

7. Ibidem, 13.

8. Special Report: *Digital in 2016,* http://wearesocial.com/uk/special-reports/digital-in-2016.

9. http://www.pewinternet.org/2016/11/11/social-media-update-2016/.

10. Report *New Trends in Social Media,* NATO Strategic Communications Centre of Excellence, Riga, December 2016, 9.

11. Reza Zafarani, Mohammad Ali Abbasi, Huan Liu, *Social Media Mining,* Cambridge University Press, April 20, 2014, http://dmml.asu.edu/smm/SMM.pdf.

12. Daniel Armstrong, *Exploring Social Media's Influence during Conflict and Crisis,* Grounded Curiosity, November 2016, http://groundedcuriosity.com/exploring-social-medias-influence-during-conflict-and-crisis/#_ftn37.

13. Reza Zafarani, Mohammad Ali Abbasi, Huan Liu, Op. Cit.

14. Catherine Caruso, *Can a Social-Media Algorithm Predict a Terror Attack,* MIT Technology Review, June 16, 2016, https://www.technologyreview.com/s/601700/can-a-social-media-algorithm-predict-a-terror-attack/.

15. The concept of grassroots journalism was exquisitely developed by Dan Gillmor in his book *We the Media, grassroots journalism by the people, for the people,* O'Reilly Media, Inc., 2004.

16. https://www.weforum.org/agenda/2016/01/q-a-walter-quattrociocchi-digital-wildfires?utm_content=buffer-259d4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

17. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

18. Rebecca Goolsby, *On Cybersecurity, Crowdsourcing, and Social Cyber-Attack,* http://www.stratcomcoe.org/rebecca-goolsby-cybersecurity-crowdsourcing-and-social-cyber-attack.

19. Report *Social Media as a Toll of Hybrid Warfare,* NATO Strategic Communications Centre of Excellence, Riga, July 2016, 13.

20. Report *Network of Terror: How DAESH uses adaptive social networks to spread its message,* NATO Strategic Communications Centre of Excellence, Riga, December 2015, 9.

21. http://www.theverge.com/2013/4/23/4257392/ap-twitter-hacked-claims-explosions-white-house-president-injured.

22. Report *Social Media as a Toll of Hybrid Warfare,* NATO Strategic Communications Centre of Excellence, Riga, July 2016, 17.

23. Report *Network of Terror: How DAESH uses adaptive social networks to spread its message,* NATO Strategic Communications Centre of Excellence, Riga, December 2015, 21.

24. Report *New Trends in Social Media,* NATO Strategic Communications Centre of Excellence, Riga, December 2016, 32-33.

25. Report *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia,* NATO Strategic Communications Centre of Excellence, Riga, January 2016, 10.

26. AJP – 3.10.1, Allied Joint Doctrine for Psychological Operations, 2014, section IV – *Principles of PsyOps.*

27. Ibidem, section III - *PSYOPS within strategic communications and information operations.*

28. Jolanta Darczewska, *The Anatomy of Russian Information Warfare, the Crimea Operation – a Case Study,* Point of View, Centre for Eastern Studies, Warsaw, May 2014, 11-12, http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.

29. http://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

NOTES

30. You can watch one of these propaganda films here: https://www.youtube.com/watch?v=hiY7JFadLm8.

31. *Twitter Has Stopped Updating Its Public Tally Of Bots,* William Alden, *BuzzFeed,* November 10, 2015, https://www.buzzfeed.com/williamalden/twitter-has-stopped-updating-its-public-tally-of-bots?utm_term=.qylllVP6D#.pbYRR3mJZ.

32. *Facebook estimates that between 5.5% and 11.2% of accounts are fake,* Emil Protalinski, The Next Web, http://thenextweb.com/facebook/2014/02/03/facebook-estimates-5-5-11-2-accounts-fake/.

33. Report *Social Media as a Tool of Hybrid Warfare,* NATO Strategic Communications Centre of Excellence, Riga, July 2016, 37.

34. Report *New Trends in Social Media,* NATO Strategic Communications Centre of Excellence, Riga, December 2016, 34.

35. Report *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia,* NATO Strategic Communications Centre of Excellence, Riga, January 2016, 10.

36. Jolanta Darczewska, *The Anatomy of Russian Information Warfare, the Crimea Operation – a Case Study,* Point of View, Centre for Eastern Studies, Warsaw, May 2014, 16, http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.

37. For more information see the Report *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia,* NATO Strategic Communications Centre of Excellence, Riga, January 2016.

38. Report *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia,* NATO Strategic Communications Centre of Excellence, Riga, January 2016, 42.

39. Report *Social Media as a Tool of Hybrid Warfare,* Strategic Communications Centre of Excellence, Riga, July 2016, 31.

40. Appropriate fragments of the leaked documents can be found here: http://gawker.com/nsa-and-cia-spied-on-world-of-warcraft-other-online-vi-1479458437.

41. Report *Analysis of Russia's Information Campaign against Ukraine,* NATO Strategic Communications Centre of Excellence, Riga, July 2015, 23.

42. Report *New Trends in Social Media,* NATO Strategic Communications Centre of Excellence, Riga, December 2016, 23.

43. Report *Daesh Recruitment, How the Group Attracts Supporters,* NATO Strategic Communications Centre of Excellence, Riga, November 2016, 23-24.

44. Brian Solis' quotation used in the article by Nicole Matejic *3 things Anthony Robbins reminded me about communication:* http://www.infoopshq.com/2016/10/02/3-things-anthony-robbins-reminded-me-about-communication/.