DOI: https://doi.org/10.12797/Politeja.14.2017.50.08

Marcin SZYMAŃSKI
Jagiellonian University in Kraków
marcin.szymanski@uj.edu.pl

'DISTURBING POTENTIAL': MILITARY OPERATIONS IN SOCIAL MEDIA DOMAIN

ABSTRACT The author of the article pursues several vignettes drafted in the course of the military and academic discussions, related to the social media. Initial section of the publication is dedicated to the social sphere of the human nature. The reasons and motives inspiring people to create networks are investigated. The subsequent part provides a description of currently available social media platforms. The tools, their utility and basic characteristics are examined. Such summary is used as a framework to build few conclusions on the potential risks and opportunities, offered by virtual networks for the security community. Findings are consequently confronted with existing doctrines. Some structural assumptions are drafted within this section, in order to provide a conceptual point of reference for further research. The author than continues with selected case studies of the social media military application. The article is concluded by a few reflections encapsulating the role of non-kinetic, social media embedded warfare in the contemporary conflicts.

Key words: social media, psychological operations, information operations, terrorism, social networks, military operations

The evolution of the global security environment has been accelerated dramatically by the turbulent advent of the new millennium. Strategic effects achieved by spectacular terrorist attacks, economic drop downs, humanitarian catastrophes, military interventions and numerous other key events set the stage for continuous, chaotic change. A good number of scholars claim that despite these transformations, the general nature of war has remained monotonously unaltered. The clash of wills, *the continuation of politics with other means*, is still framed on the traditional triad of *primordial violence,*

uncertainty and rational calculus.[1] The backbone defined in the 19th century by German classic Carl von Clausewitz, according to many remains relevant until present day. Regardless of such conservative statements, one aspect is often brought to the attention, as an unquestionable advent of change.

The twenty-first-century warfare is about different purpose than it used to be throughout the centuries. Objectives of politically motivated violence are no longer defined by the desire to control geographic space, as it was in the past. 'Domination', which used to be the ultimate goal of armed clashes, has been altered by 'influence'. Actors of the contemporary security space are competing for 'control', which is not necessarily attributed to the physical occupation, or annexation of the territory. The principal purpose of the struggle today, is the ability to influence strategic decision-making. Such objective is pursued by different state and non-state entities in a variety of ways. Contemporary paths to the victory are paved by skillful and comprehensive use of the instruments of power being applied in the political, economic, military, social, information and infrastructure domains. Within such combination of orchestrated pressures, a range of non-kinetic options assumes an unprecedented value. The information and psychological operations, often conducted in the grey zone accommodated between the peace and war, systematically become more decisive. Such tendency provides an evidence of the strategic center of gravity being relocated from the physical to the cognitive domain. The ability to influence the decisionmaking cycle of the potential adversary is based on the assumed control of such cognitive centers of gravity. With these trends in effect, the battle space geometry has been expanded with one more dimension – a virtual space of the computer networks. This particular engagement area is dominated by the information and cyber warfare. Both spheres of the military activity, even though different in nature, are supporting and complementing each other.

The domain of the social media remains their principal common denominator. Thomas Elkjer Nissen defines social orbit of the cyber space as *technology and platforms that enable connectivity and the interactive web content creation, collaboration and exchange by participants, the public, and the media*.[2] The military utility of blogs, web pages, social media accounts and other interactive virtual tools is blatantly apparent. They are heavily utilized with different volume and purpose by state and non-state actors, competing for influence in the global security environment. As Jolanta Darczewska highlights, *the geopolitical doctrine treats information as a dangerous weapon: it is cheap, it is universal, it has unlimited range, it is easily accessible and permeates all state borders without restrictions*.[3] General Gerasimov, Chief of Staff of the Russian Armed Forces, quoted in one of the NATO reports, underlines the fact that *the information*

1 M.I. Handel, *Clausewitz and Modern Strategy*, Abingdon 2004, p. 59.

2 T. Elkjer Nissen, *#TheWeaponizationofSocialMedia. @Characteristics_of_Contemporary_Conflicts*, Copenhagen 2016, p. 35.

3 J. Darczewska, *The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study*, p. 7, at <https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf>, 1 June 2017.

space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy.[4] He continues stating that in nowadays warfare *it is necessary to perfect activities in the information space*. Being aware of the impact, which social media information campaigns caused during the latest conflicts, scholars and military thinkers initiated debates aiming to define and explore emergent opportunities. Reflections and conclusions of these polemics served as an inspiration to this article.

Information space opens wide possibilities – in order to grasp them, however, it is necessary to have the knowledge, to be aware and to be willing to proceed in an unconventional way. Despite the concerns to violate liberal freedom of the citizens' social space, the security community must realize that the use of the social media for the defense purposes is as important as an effective use of any other, traditional tool of politically motivated violence. Several questions have to be answered in order to make sure that the virtual dimension of the battle space is effectively exploited in the battle for influence. The study of human interrelations needs to be conducted in order to lay down foundation for understanding of the virtual networks. Scholars have to be aware why people choose to build networks: why do we share knowledge? Why do we build relationships and why does the cyber space facilitate these processes so well? How social interactions benefit from the capabilities delivered by the internet? Are virtual relations of the same value as their 'real world' counterparts? Why do we set up so strongly tied networks around shared ideas and why these cognitive phenomena pushes people to do things, despite risking their lives? Once this behavioral background is penetrated, the research should focus on the technical realm of the social networks. What platforms are most often used? What do they offer and how do they interact? What is the prospect of their evolution? Finally, an investigative effort has to be made in order to discover potential for the military utility of the social media sphere. Blogs, networks, platforms – tools to share ideas: what opportunities and risks do they represent for global security? Are they identified and taken into account by the decision makers? How do they contribute to the contemporary doctrines, practices, operational techniques?

The purpose of the article is to search for answers to at least some of these questions. In order to do so, the author pursues several vignettes drafted in the course of the military and academic discussions, related to the social media. Initial section of the publication is dedicated to the social sphere of the human nature. The reasons and motives inspiring people to create networks are investigated. The subsequent part provides a description of currently available social media platforms. The tools, their utility and basic characteristics are examined. Such summary is used as a framework to build few conclusions on the potential risks and opportunities, offered by virtual networks for the security community. Findings are consequently confronted with existing doctrines. Some structural assumptions are drafted within this section, in order to provide a conceptual point of reference for further research. The author than continues with selected

[4] "Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia", NATO Strategic Communications Centre of Excellence, p. 54, at <http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0>, 29 May 2017.

case studies of the social media military application. The article is concluded by a few reflections encapsulating the role of non-kinetic, social media embedded warfare in the contemporary conflicts.

SOCIAL NETWORKS

The concept of networking is as old as an origin of the human race. People have been building relations to sustain basic functions of survival since the very beginning of their existence. The way we communicate – using spoken and written language – enabled us to share thoughts, ideas and experience. This distinct feature of the human race: the ability to accumulate and share knowledge can be perceived as a key enabler for our domination in the world of the nature. The extent of the networks, based on social concepts of family, clan, tribe, chiefdom or state has been always geographically restrained by the capabilities of available communication tools. Information technology offered new – as Manuel Castells called it *multidimensional space of social interaction*.[5] Geography, geopolitics and distances lost their meaning in a new world, dominated by virtual linkages. Networks, as Castells continues, *do not have fixed boundaries; they are open-ended and multi-edged, and their expansion or contraction depends on the compatibility or competition between the interests and values*[6] – in other words geopolitics do not matter in a world of *microelectronics-based, digitally processed information and communication technologies*.[7]

Such environment stimulated social developments which resulted in the creation of new form of the so-called 'network society'. The culture which surrounds it is based on the internet protocols which constitute new ethical codes. These sets of values create specific nature of new society models. The newly emerged social DNA is no longer framed on the shared identity – it is based on the value of sharing. Such architecture of the global information space accelerated significantly the speed of the human thought exchange. The ideas, reflections and interest are shared in the course of unbounded, everlasting digital debate. The human thought as it is emphasized by Castells, *is probably the most rapidly propagating and influential element of any social system*.[8]

Such scope of proliferation has been possible since it was supported by the *global, interactive communication system in real time*.[9] The existence of a multidimensional cyber space enabled human race to build a collective intelligence. The process of creation never ends and it is continuously fueled by thought being shared and circulated with the speed and range never experienced before. Despite numerous claims emphasizing that the core values of social interaction have not changed, some newly emerging ten-

5 M. Castells, *Communication Power*, Oxford 2013, p. 19.

6 Ibid., p. 19.

7 Ibid., p. 24.

8 Ibid., p. 29.

9 Ibid.

dencies have been identified within the network society. In addition, several existing theories became to be more relevant in new reality of virtual space. Collective intelligence built on the foundation of sharing protocols provides endorsement for line of thought represented by social constructivism. The theory, advocated by Soviet cognitivist Lev Vygotsky attributes the process of learning to the phenomena of the social interaction. Cognitive functions as he argued, *originate in, and must therefore be explained as products of social interactions*.[10] Vygotsky also declared that *learning was not simply the assimilation and accommodation of new knowledge by learners; it was the process by which learners were integrated into a knowledge community*.[11] Such theory explains precisely a human drive to associate around the communities of interest. Internet forums, subject oriented chat rooms and face book pages serve a good, practical example of the 'social constructivism' theory. Contemporary virtual platforms provide users with extraordinary tool for practical implementation of Vygotsky's concept. Social media allow two-way communication – they are specifically designed to support collective thinking. The prospect of the interaction or, as Anne Mintz calls it – 'participation', is *perhaps their most popular feature. Instead of being passive consumers of content, people can comment on each other's content and contribute their own text, audio and video*.[12] This particular capability, enabled by technical innovation, sparked a revolutionary change in a human interaction. It has also transformed the theory of 'social constructivism' into a globally exercised practice.

The architecture of the virtual exchange platforms, as it was stated earlier, is constantly occupied by 'thought' expressed in the form of endlessly circulating 'narratives'. The narrative serves as a carrier for a human ideas – it is often used by certain groups of interest to express their visions of the society. These concepts are spread, advertised, advocated, discussed, agreed and attacked. Network participants share their views in order to achieve a collective perception within selected groups. 'Strategic narratives' are utilized as a *means for political actors to construct a shared meaning of international politics and to shape the perceptions, beliefs, and behavior of domestic and international actors*.[13] Multidimensional cyber domain with its available, interactive tools, provides a perfect ground for debating over the strategic visions. Social media accessibility and the natural will of the people to rally around ideas, create a space for competition of ideologies. Interactive platforms enable to transfer and share countless perceptions, which often collide in the course of 'battles of narratives'. Number of interactions within this virtual domain makes some scholars think that instead of 'the battles', contemporary cyber space contains *enduring competition with no winners and losers*.[14]

---

10 "Social Constructivism", Berkeley Graduate Student Instructor Teaching & Resource Center, at <http://gsi.berkeley.edu/gsi-guide-contents/learning-theory-research/social-constructivism/>, 1 June 2017.

11 Ibid.

12 A.P. Mintz (ed.), *Web of Deceit. Misinformation and Manipulation in the Age of Social Media*, Medford 2012, p. 44.

13 T. Elkjer Nissen, *#TheWeaponizationofSocialMedia...*, p. 44.

14 Ibid., p. 45.

Social networks existing within this theater of the virtual contest have their own, sketchy structures. Their nodes assume certain functions, which are not entirely different from social functions in the traditional communities. Eric Larson, discussing some of these roles, underlines the essentiality of the 'opinion leaders'. He argues that *opinion leadership has been among the most important concepts related to the influence of key individuals within groups, networks, communities*.[15] The leaders – as on a regular front, assume key functions in the battles of narratives. They have the ability to shape, activate, connect or disintegrate networks. Manuel Castells further segregates the opinion leaders, basing on their potential for impact. He claims that the leadership in virtual networks has two levels of competence. At the first layer, the leaders have *the ability to constitute networks and to program/reprogram networks in terms of the goals assigned to the network*.[16] Such influential nodes of the system are called by Castells 'programmers'. 'The switchers', occupying the second layer of the leadership, maintain *the ability to connect and ensure the cooperation of different networks by sharing common goals and combining resources, while fending off competition from other networks by setting up strategic cooperation*.[17] Both leadership functions are the key for an existence and expansion of the networks. The 'programmers' possess visionary capabilities, while the social negotiation skill is attributed to 'the switchers'. Castells concludes, stating that the leaders – no matter which level of competence they represent, *hold network-making power, the paramount form of power in the network society*.[18]

The society built on the skeleton of the information technology utilizes several traditional mechanisms to maintain its structure and internal dynamic. Relative power of the nodes within the networks, is constructed on the foundation the principles including classic, informational, coercive, reward, legitimacy, expert, and referent models.[19] Despite of the existence of such traditional features, some scientists claim that the virtual human constellations are different from those based on personal linkages. As they emphasize, the essential difference between the traditional and virtual human networks, is the strength and nature of the relationship. Kirk A. Duncan brings to the attention two the most remarkable critiques of the network society phenomena. Evgeny Morozov, author of *The Net Delusion – the Dark Side of Internet Freedom*, criticizes the idea of the network society, stating that the cyber relationships offer more potential threats than benefits. The exposure of thoughts in the course of the open, virtual debate creates potential risks of being captured in the trap of the surveillance. Illusive freedom offered by a multidimensional cyber space, paradoxically increases chances for the regimes to control and manipulate populations. Michael Gladwell, a Canadian writer,

[15] E.V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*, p. 32, at <http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf>, 28 May 2017.

[16] M. Castells, *Communication...*, p. 45.

[17] Ibid.

[18] Ibid., p. 47.

[19] See E.V. Larson et al., *Foundations of...*, p. 8.

makes additional reservations to the value of the virtual networks. He bases his concern on the contrast between strong ties – characteristic for the personal relationship and weak ties – attributed to social media based bonds. According to Gladwell *successful social movements are centered on an individual's strong ties to one another*, he also highlights that *people join movements primarily because they have a close friend or relative who is already in the social movement*.[20] The weak ties – characteristic for the cyber relationship, even though fairly effective in marketing and thought exchange, *seldom lead to high risk activism*.[21] Such rhetoric expressed within some scientific circles, indicates the existence of disbelief in the social value of the virtual networks.

IT FACTOR

The parallel world contained in the cyber domain undoubtedly opens new opportunities for social development of the human race. Traditional models transferred to new spaces collide with each other, creating entirely new archetypes for the community interactions. The evolution would not have been possible without technological innovations. The first virtual application, enabling users to take advantage of interactive communication, appeared in 1979: *Tom Truscott and Jim Ellis had created the Usenet, a worldwide discussion system that allowed Internet users to post public messages*.[22] The real breakthrough, however, was initiated with the advent of an interactive Web2.0[23] tools (with the most popular ones: MySpace being introduced in 2003, and Facebook – launched in 2004). New platforms enabled active, 'many to many' interaction for users. Information, unlike in the classic 'one to one' or 'one to many' transmissions, can be delivered, commented, shared and exchanged with all in the network. There are several definitions of the Web2.0 architecture. NATO associates it with 'new media' category.[24] In accordance to the Alliance Directive AD 95-3, *social media are designed for dissemination through social interaction using internet- and web-based technologies, to transform broadcast media monologues (one-to-many) into social media dialogues (many-*

[20] K.A. Duncan, *Assessing the Use of Social Media in Revolutionary Environment*, Naval Postgraduate School thesis, Monterey, Calif. 2013, p. 8, at <http://calhoun.nps.edu/bitstream/handle/10945/34660/13Jun_Duncan_Kirk.pdf?sequence=1>, 28 May 2017.

[21] Ibid.

[22] A.M. Kaplan, M. Haenlein, "Users of the World, Unite! The Challenges and Opportunities of Social Media", *Business Horizons*, vol. 53, no. 1 (2010), p. 60, at <https://doi.org/10.1016/j.bushor.2009.09.003>.

[23] Web2.0 is defined as *a platform whereby content and applications are no longer created and published by individuals, but instead are continuously modified by all users in a participatory and collaborative fashion* – ibid.

[24] NATO Supreme Headquarters Allied Powers Europe, *Allied Command Operations Directive AD 95-3*, Mons 2013, p. 3: *new media is a generic term for many different forms of electronic communications that are made possible through the use of computer-based technologies*.

to-many).[25] European Union outlines the definition of the social media as *online technologies and practices to share content, opinions and information, promote discussion and build relationships*.[26] The same document further explains that, *social media services and tools involve a combination of technology, telecommunications and social interaction. They can use a variety of formats, including text, pictures, audio and video*.[27] Kenneth Laudon and Carol Traver define the Web2.0 tools as *a set of applications and technologies that allows users to create, edit, and distribute content; share preferences, bookmarks, and online personas; participate in virtual lives; and build online communities*.[28] Interactive media – to compile several definitions – constitute a set of hardware and software which enables an active communication of several users, through shared content. Some of the best known examples of such tools include applications like Facebook, Twitter, You Tube, interactive games and blogs. It is assessed that in the year of 2017, 37% of global population utilized social media for communication. Statistics also attribute 25% annual growth to the number of social media community.[29] Facebook currently associates the biggest group of users. The community as of 2017 includes 1,870 million participants. As an unquestionable leader, Facebook accumulates 18% of the global social media market. Average user accesses the platform 8 times per day, 75% of them operates application daily.[30]

Despite the big concentration of users around Facebook, social media market includes number of other platforms. They are further divided into the categories, depending on their specific nature and capabilities. Andreas M. Kaplan and Michael Heanlein these applications into six categories. In accordance with this typology social media include:

1. Collaborative projects, example: Wikipedia.
2. Blogs and micro-blogs blogs, example: sites like Twitter.
3. Content communities (Upload-sites), example: YouTube, Flickr, LiveLeak, Instagram.
4. Social networking sites, example: Facebook, Vkontakte or LinkedIn.
5. Virtual game worlds, example: World of Warcraft, Call of Duty or Grand Theft Auto.
6. Virtual social worlds, example: Second Life.[31]

A variety of platforms attracts numerous users, searching for an alternative form of

[25] Ibid.

[26] European Commission, *Social Media Guidelines for all Staff*, p. 1, at <http://ec.europa.eu/ipg/docs/guidelines_social_media_en.pdf>, 27 May 2017.

[27] Ibid.

[28] K.A. Duncan, *Assessing the Use...*, p. 18.

[29] See D. Chaffey, "Global Social Media Research Summary 2017", Smart Insights, 17 April 2017, at <http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/>, 27 May 2017.

[30] Ibid.

[31] A.M. Kaplan, M. Haenlein, "Users of the World...", p. 61.

the social interaction. The Second Life for example, as one of the first virtual worlds, accounted during its top popularity in 2008, *about 12.3 million registered users and about 50,000 visitors at any point in time on an average day*.[32] Early success of the game attracted banks, media and other entities to open their virtual offices in the cyber domain of the Second Life. The diversity of available social network platforms forced software providers to invest in their compatibility. Users desired to share content in a variety of ways – bringing and commenting it on more than one platform. The technical capability to enable such transfers is called 'cross-media communication'. It is defined as a capacity to distribute *an overall story, production, or event, using a coordinated inter-linked combination of platforms*.[33] Interoperability became to be one of the most essential features of the Web2.0 tools. Facebook as a leader in 'cross-media communication' offers its users two-way transfer gates to 90% of the available social media applications.[34] The 'multiplatform reach', as it is called, may be conducted in accordance with several protocols. Thomas Elkjer Nissen defines them as four approaches:

1. Push: to 'push' the same content with minor differences on all platforms.
2. Extra: to provide 'extra' content produced alongside a main production and delivered on different platforms.
3. Structure: to create and project a 'structured' story in order to drive the audience to continue to other platforms.
4. Hands-off: to distribute content across many platforms in a non-linear way in order to give the audience a possibility to create the story themselves.[35]

Popularity of the social media tools is also dependent on the capabilities of a hardware which brings the platforms to the users. Migration of the Web2.0 architecture to mobile devices represented a milestone in the process of an interactive communication evolution. The essentiality of this fact is based on a few factors – two of them seem to be the most vital. First and the most obvious is the aspect of accessibility. Users utilizing mobile devices are never off line. They actively participate in the networks – practically full time. Growing GSM coverage and increasing number of affordable smartphones influenced directly the size of the social media community. Secondly, since mobile devices are usually equipped with recording sensors, users expanded the amount of the photographic and video content. This particular factor contributed significantly to the popularization of so called 'citizens' journalism'.[36] The expansion of the video and photographic content has been further supported by already described cross media communication capability. The trend of bringing the Web2.0 platforms to the mobile devices will continue. It is assessed that 34% of global population currently uses social

[32] M. Castells, *Communication...*, p. 69.

[33] T. Elkjer Nissen, *#TheWeaponizationofSocialMedia*..., p. 41.

[34] See D. Chaffey, "Global Social Media...".

[35] T. Elkjer Nissen, *#TheWeaponizationofSocialMedia*..., p. 44.

[36] *The collection, dissemination, and analysis of news and information by the general public, especially by means of the Internet* – "citizen journalism", in *Oxford Living Dictionaries*, at <https://en.oxforddictionaries.com/definition/citizen_journalism>, 26 May 2017.

media via mobile devices. The statistics also attribute 30% annual growth to this particular section of the Web2.0 community.[37] The internet communication, whether it is wire or wireless, requires a technical infrastructure to support fast and stable data transfer. This is particularly important within the mobile realm of the internet. Throughout the last decade a substantial investment has been made to improve the reach of the enhanced broadband transmission. Wireless networking has also been significantly developed, bringing the affordable and reliable coverage of almost global range.

Social and technical characteristics of the interactive media, indicate a mass nature of the virtual, 'many to many' communication. The scale of the Web2.0 utilization will most likely continue to grow. The expansion of the cyber domains, however, was not accompanied with the implementation of regulatory measures. Thus the realm of the social media remains, and with high probability will remain rather poorly controlled. The capabilities, range, popularity and lack of rules invite the state and non-state actors to exploit potential opportunities, which social media offer to the policy makers. The Web2.0 network opens a wide space for an employment of different influence methods. Referring to such techniques, social psychologist Robert B. Cialdini created a model based on six 'weapons of influence'. They include: reciprocation, commitment, social proof, authority, and scarcity.[38] These mechanisms of manipulation, skillfully smuggled into the narrative applied through the Web2.0, may act as an effective stand-off, non- kinetic weapon. The predominant goal of its application is described as *political concessions*, extracted through *manipulation and exerting influence on decision-making processes*.[39] The term 'influence' suggests a direct association of the social media military operations (SMMO) with psychological operations. Such connotation, despite of being obvious, generates an incomplete picture. A number of the other doctrinally recognized areas of operational activities which may include the Web2.0 utilization, makes such correlation defective. Elkjer Nissen claims that, the platforms may be *utilized for a series of military activities, whether by state or non-state actors (even down to the individual level), such as Intelligence Collection, Targeting, Psychological Warfare, Cyber-Operations and Command and Control*.[40] These operational activities can be accommodated within a wider scope of campaigns, which are usually dominated by specific type of warfare. Some obvious linkage of the social media utilization may be tracked to the 'cyber warfare', which is defined as *an armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyber-*

37 D. Chaffey, "Global Social Media...".

38 E.V. Larson et al., *Foundations of...*, p. 30: Cialdini's Influence Model. Social psychologist Robert B. Cialdini (2000, 2006) identified what he described as six 'weapons of influence': (1) reciprocation, the tendency for people to return a favor; (2) commitment, the tendency for people to honor a commitment; (3) social proof, the tendency for people to behave as they observe others behaving; (4) authority, the tendency to obey authority figures; (5) likeability, i.e., people are more easily persuaded by those whom they like; and (6) scarcity, perceptions of scarcity generate demand.

39 T. Elkjer Nissen, *#TheWeaponizationof SocialMedia...*, p. 29.

40 Ibid., p. 62.

space systems and weapons in a conflict.[41] Offensive function of the cyber warfare: Computer Network Attack (CNA) as well as intelligence collection, defined as Computer Network Exploitation (CNE), may be potentially executed within the social media sphere. Such operational employment may have a form of hacking, blocking accounts, denying access to the networks and other modes of technical interruptions. More generally, the military operations, which offensively exploit computer networks, are classified as 'cyber-attacks'. These offensive efforts are further defined as *activities that are carried out over information networks ranging from hacking and defacing of webpages to large-scale destruction of the military or civilian computer-based systems, networks or infrastructure*.[42] Broad capacity of this definition covers numerous activities referring to the SMMO.

SMMO: DOCTRINAL CONTEXT

Thomas Elkjer Nissen sheds different light on the nature of cyber-attacks, by bringing them close to the realm of the special operations. He underlines that these activities *mostly in the form of hacking, aimed at social network media accounts*, are often based on *tactical actions with strategic aims*.[43] The correlation of the tactical task with the strategic goal, constitutes the most recognizable attribute of the special operations. In accordance with the NATO doctrines, such operations utilize range of unconventional tactical activities with the aim to *deliver strategic or operational-level results* in areas where *significant political risk exists*.[44] The CNE, as mentioned in the previous paragraph, also accommodates some of the social media related military functions. Number of users and the density of the network create a fertile ground for information gathering. This opportunity is exploited to a very large extent by numerous state and non-state actors. The value which the Web2.0 represents for the collection efforts, inspired some authors to recognize a 'social media intelligence' (SOCMINT), as a separate branch of the military, analytic community. Intelligence gathering within the social media domain is conducted mainly with the utilization of five standard techniques. They are defined as: *open source collection, client/customer/visitor (CCV) tracking, remote monitoring, communications intercepts, and data requests and seizures*.[45] The SOCMINT, as a rapidly surfacing, new analytic discipline, offers opportunities for advanced modelling and predictive analysis. The specific intelligence products are formulated basing on techniques such as:

---

41 US Armed Forces Joint Staff, *Joint Terminology for Cyberspace Operations*, p. 8, at <http://www.nsciva.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf>, 25 May 2017.

42 T. Elkjer Nissen, *#TheWeaponizationofSocialMedia*..., p. 28.

43 Ibid., p. 88.

44 NATO Standarization Agency, *Allied Joint Publication 3.5: Special Operations*, Mons 2013, p. 1-1.

45 K.A. Duncan, *Assessing the Use*..., p. 33.

– Trend analysis.
– Network analysis.
– Sentiment analysis.
– Geo-analysis.
– Content analysis.
– Behavioral analysis.
– Target Audience analysis.[46]

The SOCMINT, as a relatively new intelligence branch, is beginning to be a very dynamically developing discipline. The reason for that is twofold: first – it offers practically unlimited space to exploit, second – it is a very low risk and low cost type of the activity.

The cyber space accumulates a bulk of information to be exploited, it is however also a strategic key terrain which offers a favorable position in a battle for the influence. Numerous scholars and practitioners agree that *influencing through social network media is probably one of the central issues when it comes to their weaponization*.[47] In accordance with Russian academic Igor Panarin, struggle for dominance in this particular area of warfare, is composed of: *social control (influencing society); social maneuvering (intentional control of the public aimed at gaining certain benefits); information manipulation (using authentic information in a way that gives rise to false implications); disinformation (spreading manipulated or fabricated information or a combination thereof); the fabrication of information(creating false information and lobbying)*.[48] Western doctrines recognize the *influence activities*, as *the capability or perceived capability to affect the understanding and thus the character or behavior of an individual, group or organization*.[49] This particular military function is mostly associated with 'information operations' (IO). They are defined by western doctrines, as *the integrated employment, during military operations, of information related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries*.[50] The 'information activity' seems to be another term, existing in the NATO lexicon and corresponding to the nature of the SMMO. The doctrine describes it, as means to *undermine adversary's moral power base, separating leadership from supporters, political, military and public, thus weakening their desire to continue and affecting their actions*.[51] NATO categorizes potential effects of an integrated application of the information ac-

46 T. Elkjer Nissen, *#TheWeaponizationofSocialMedia*..., p. 61.

47 Ibid., p. 85.

48 J. Darczewska, *The Anatomy*..., p. 15.

49 NATO Standarization Agency, *Allied Joint Publication 01: Allied Joint Doctrine (2010)*, p. 123, at <https://www.gov.uk/government/publications/ajp-01-d-allied-joint-doctrine>, 24 May 2017.

50 US Armed Forces Joint Staff, *Joint Publication 3-13: Information Operations*, p. IX, at <http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf>, 24 May 2017.

51 NATO Standarization Agency, *Allied Joint Publication 3.10: Information Operations (2009)*, pp. 1-4, at <https://info.publicintelligence.net/NATO-IO.pdf>, 20 May 2017.

tivities within the social media sphere, as *to deny, degrade, disrupt and manipulate the information available to a decision maker*.[52]

Information activities conducted by the military actors within the range of the SMMO are very close in their nature to the information campaigns exercised by a competitive business and politics. Both military and non-military players are embedding to the substantial extent, their IO efforts within the Web2.0 domain. The difference between such efforts employed by the military and non-military actors is *the purpose of application*.[53] In other words, the SMMO is based on the use of the commercially available tools, utilized to achieve military goals. Such combination represents a lucrative opportunity for any actor willing to struggle for the influence without being identified as a source of the hostile activity. This particular peculiarity of the social media, makes them an extremely attractive tool to be used in a hybrid warfare,[54] which by its nature relies heavily on the success of the clandestine, shaping operations – conducted before the outbreak of hostilities.

Operations conducted in the Web2.0 sphere – either to influence the adversary, or to collect the intelligence, may be conducted in an overt,[55] covert[56] or clandestine[57] mode. Covert application of the social media includes utilization of 'nongovernmental IP addresses'[58] or hardware which does not leave a virtual footprint, attributable to the sponsoring agency. Clandestine activities are conducted with the employment of false virtual identities, created in order to produce a fake accounts. Low profile modes of the SMMO represent a particularly feasible option to support an 'unconventional' warfare campaigns. They are doctrinally defined *as activities conducted to enable a resistance movement or insurgency to coerce, disrupt or overthrow a government or occupying power by operating through or with an underground, auxiliary or guerrilla force in a denied area*.[59]

---

[52] Ibid.

[53] G.J. David, T.R. McKeldin, *Ideas as Weapons. Influence and Perception in Modern Warfare*, Washington 2009, p. 113.

[54] Defined as: *the use of asymmetrical tactics to probe for and exploit domestic weaknesses via non-military means, backed by the threat of conventional military means* – J.M. Calha, "Hybrid Warfare: NATO's New Strategic Challenge?", NATO Defense and Security Committee Report, p. 3, at <http://www.nato-pa.int/default.asp?SHORTCUT=3778>, 20 May 2017.

[55] Defined as: *an operation conducted openly, without concealment* – NATO Standarization Agency, *Allied Publication AAP6: NATO Glossary of Terms and Definitions (2014)*, p. 296, at <http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf>, 12 May 2017.

[56] Defined as: *an operation that is planned and conducted so as to conceal the identity or permit plausible deniability of the executor* – NATO Standarization Agency, *Allied Joint Publication 3.5...*, p. LEX-4.

[57] Defined as: *an operation planned or conducted in such a way as to assure its secrecy or concealment* – NATO Standarization Agency, *Allied Publication AAP6...*, p. 89.

[58] Global Justice Information Sharing Initiative, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities. Guidance and Recommendations*, February 2013, p. 14, at <https://it.ojp.gov/documents/d/Developing%20a%20Policy%20on%20the%20Use%20of%20Social%20Media%20in%20Intelligence%20and%20Inves.....pdf>, 20 May 2017.

[59] "Irregular Warfare: a SOF Perspective", *Center for Army Lessons Learned Newsletter*, no. 11-34 (June 2011), p. 20.

Nearly global reach of the internet provides a frame for social media to be used specifically in the 'denied areas'. Military experts emphasize that the successful influence operations require *effective communication using the local information systems*.[60] Since the Web2.0, as it was described earlier, dynamically expands, it is reasonable to assume that its regional clusters will replace local media very soon. Such perspective indicates that the planners of unconventional campaigns should pay special attention to social media related aspects.

The SMMO corresponds very well with asymmetric approaches to the warfare. The theory of operational asymmetry emphasizes the value of *acting, organizing, and thinking differently than opponents in order to maximize one's own advantages, exploit an opponent's weaknesses, attain the initiative, or gain greater freedom of action*.[61] Employment of the social media to attain military goals became a characteristic feature of an asymmetric strategies used by non-state actors, who attempt to compensate for the conventional superiority of their adversaries. Such application of the Web2.0 platforms is also characteristic for 'irregular warfare', which is defined as *a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations*. Mass perception – which is a central theme of the irregular warfare strategies, may be, with high expectation of success, shaped by the implementation of the SMMO tactics.

SMMO BY STATE ACTORS

The confrontation of doctrines and Web2.0-offered military opportunities might be concluded within the conceptual frames of functionally oriented typology. Doctrinally, as it was described above, the SMMO primarily supports unconventional, irregular, hybrid and asymmetric warfare scenarios. These strategies might be supported by passive and/or active employment of the SMMO. The first category includes intelligence collection, the second covers a range of the influence operations. Passive and active functions are conducted in overt, covert or clandestine modes. Subsequent section of the article provides an account of several case studies for selected combinations included in the above typology.

Clandestine, active utilization of the social media in influence operations, offers a perfect option for actors waging asymmetric and hybrid warfare. Elements of such strategies, as pointed out by Russian political scientist Aleksandr Dugin, are employed in a cultural struggle between 'Euroasian' and 'Atlantic' regional clusters. Capabilities of the Web2.0 platforms to support this contest are highly appreciated in Russia. The Kremlin is believed to be *modifying and perfecting its propaganda techniques, taking into account new media tools and introducing innovations, such as activity in social network-*

[60] Ibid., p. 29.

[61] S. Metz, D.V. Johnson II, *Asymmetry and US Military Strategy: Definition, Background and Strategic Concepts*, Collingdale 2001, p. 5.

ing services.[62] Dugin concludes that the information warfare in support of the cultural struggle is so vital, that it should be centrally controlled and conducted by *special group consisting of senior officials, the best 'mission-oriented' (Russian пассионарные) staff from the Russian secret services, intellectuals, scientists, political scientists and the corps of patriotically-oriented journalists and culture activists*.[63] Being inspired by such approaches, Russian authorities employ a range of active functions, offered by the social media. Coordinated activities, conducted by so called 'trolls', offer a tangible example of the 'active, clandestine' utilization of the Web2.0. Urban Dictionary defines a 'troll', as a person with usually false virtual identity, which *posts a deliberately provocative message to a newsgroup or message board with the intention of causing maximum disruption and argument*.[64] Analysts associate 'trolling' with disruptive comments made at social platforms for no other purpose but an ignition of conflict and confusion. Report by the NATO Strategic Communication (STRATCOM) Center of Excellence identifies the difference between the classic and politically motivated trolls. In accordance with the publication *a classic troll acts with no apparent instrumental purpose, whereas purported hybrid trolls (hired, pro-Russian trolls), communicate a particular ideology and, most importantly, operate under the direction and orders of a particular state or state institution*.[65] Active, clandestine function of such trolls is conducted in line with the hybrid warfare principles – the operations are executed within the limits of plausible deniability. As a result it is difficult, if not impossible, to recognize and associate such on-line activity, with specific sponsor. In case of Russia there are numerous reports by an investigative media, indicating the existence of 'troll farms' – groups of government- sponsored personnel, tasked to *spread disinformation, rumors, or falsified facts, enter into discussions and flood topic-related web spaces with their own messages or abuse*.[66] Hybrid trolls are reported to operate simultaneously on several Web2.0 platforms. Each of them posts and comments from number of false accounts. Analysts estimate, that *on an average working day, the Russians are to post on news articles 50 times. Each blogger is to maintain six Facebook accounts publishing at least three posts a day and discussing the news in groups at least twice a day. By the end of the first month, they are expected to have won 500 subscribers and get at least five posts on each item a day. On Twitter, the bloggers are expected to manage 10 accounts with up to 2 000 followers and tweet 50 times a day*.[67] Their efforts are centrally coordinated and dedicated to support Kremlin's 'information struggle' campaigns. Several Russian-sponsored concentrated troll attacks have been reported

[62] J. Darczewska, *The Anatomy*..., p. 8.

[63] Ibid., p. 18

[64] "Troll", in *Urban Dictionary*, at <http://www.urbandictionary.com/define.php?term=troll>, 23 May 2017.

[65] "Internet Trolling as a Tool...", p. 10.

[66] Ibid., p. 3.

[67] P. Pomerantsev, M. Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, Institute of Modern Russia, p. 17, at <http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf>, 3 June 2017.

so far. Active, clandestine use of the social media which followed the downing of the Malaysian Boeing 777 on the flight MH17 over the Ukraine may serve as the most illustrative example of the hybrid trolling. The comments and posts used during the campaign were used to propagate conspiration theories and to devaluate the expert opinions. Shortly after the shot down, the volume of trolling strongly intensified. The Guardian news page for instance, *was flooded by approximately 40 000 comments per day in a troll attack that is considered to have been ordered by the Kremlin*.[68] In contrast to the attacks, designed to manipulate public perception of certain event, trolls may be used as an effective tools for prolonged information campaigns. Russia, in accordance to the NATO STRATCOM Center of Excellence, wages such remote campaigns in several countries. The Alliance made a particular investment to investigate the hybrid trolls' activities in Latvia. Group of the STRATCOM analysts developed a set of criteria used to identify trolls in the flood of virtual communication. These measures included following features of the user:

1. Must have posted more than 15 comments during the period under investigation.
2. Must be consistently pro-Russian.
3. Must either post links to pro-Russian websites or large chunks of copy-pasted information from such sites.
4. Must generally not engage in conversations with other users.
5. Must not comment on mundane and non-political topics unless such comments are political and pro-Russian.
6. Must be repetitive, reposting the same message multiple times.[69]

Using the above criteria, researchers analyzed comments made for 207,707 information items. In the course of the selection, 48 unique IP addresses have been identified, as a trace of potential trolls. 1.45% of overall analyzed content has been labelled as an effect of hybrid trolling.[70]

Active, clandestine employment of the SMMO is utilized for the strategic purposes by numerous actors operating in the global security space. Techniques being used differ to some extent. The 'sock-puppet' is a term which describes an account used to manipulate information in social platform. An exact definition classifies it as *a user account controlled by an individual who has at least one other account. In other words, if an individual controls multiple user accounts, each account is a sock-puppet*.[71] The user who controls sock-puppets is labelled as 'the puppet master' and the activity which he conducts is referred to 'sock-puppetry'. Slight difference between puppet masters and trolls, bases on the fact, that the former ones are not necessarily involved in the disruptive and provocative narrative, the latter ones on the other hand, do not always use more than one virtual identity. The sock-puppetry has been employed by the United States military

[68] "Internet Trolling as a Tool...", p. 16.

[69] Ibid., p. 33.

[70] Ibid., p. 37.

[71] S. Kumar et al., *An Army of Me: Sockpuppets in Online Discussion Communities*, p. 2, at <https://cs.stanford.edu/people/jure/pubs/sockpuppets-www17.pdf>, 20 May 2017.

in order to challenge Islamic radical narration distributed in virtual space. This particular case of active, clandestine use of the Web2.0, has been initiated as a part of the program call signed "Operation Earnest Voice" (OEV). The purpose of the operation, according to General James Mattis,[72] was *to disrupt recruitment and training of suicide bombers; deny safe havens for adversaries; and counter extremist ideology and propaganda*.[73] The OEV has been initially applied as a part of the psychological operations targeting al-Qaida members in Iraq. As a result of satisfactory effects, the operation *expanded into a $200m program*,[74] covering Pakistan, Afghanistan and the Middle East. In order to build further capacity for the SMMO, the US administration contracted a civilian company with the task to prepare dedicated software. Ntrepid, the contractor selected in 2011, is a well-known brand in military cyber branch. In 2016, it was nominated as a winner of the NATO-sponsored Defense Innovation Challenge. The company is heavily involved in the research on an unconventional technology – in accordance with the Ntrepid motto, they *invest heartily in new ideas where they see disruptive potential*. A contract worth $2.76 million, signed with the US Central Command (CENTCOM), resulted in creation of the software package, so-called 'MetalGear'. The product, as it is defined in a disclosed section of the contract, *allows users to control '10 personas* [...] *replete with background , history, supporting details, and cyber presences that are technically, culturally and geographically consistent*.[75] It is also designed to enable creation of the online personas with the data indicating their origin from any part of the world. Wide range of the potential MetalGear employment stimulated the debate on legal grounds of its application. Since the US military is not authorized to target US citizens, following the US CENTCOM spokesman: *none of the interventions would be in English, as it would be unlawful to address US audiences* [...]. *The languages in which the interventions are conducted include Arabic, Farsi, Urdu and Pashto*.[76] The technical capability offered by the Ntrepid to the US military enables to exercise unlimited, active, clandestine use of the social media to pursue strategic goals. Sock puppetry may also be used effectively for a passive utilization of the social media. Once 'the masters' penetrate the networks, they may collect high value intelligence. Operational practice demonstrates that the information sometimes has more value than the effect produced by an active engagement.

---

72 General James N. Mattis, currently Secretary of Defense of the United States, formerly US Central Command Commander (2011/2013).

73 N. Fielding, I. Cobain, "Revealed: US Spy Operation that Manipulates Social Media", *The Guardian*, 17 March 2011, at <https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks>, 20 May 2017.

74 Ibid.

75 L. Bazley, "Combating Jihadists and Free Speech: How the U.S. Military Is Using Fake Online Profiles to Spread Propaganda", *Daily Mail*, 18 March 2011, at <http://www.dailymail.co.uk/news/article-1367535/U-S-military-using-fake-online-profiles-spread-propaganda.html>, 20 May 2017 .

76 N. Fielding, I. Cobain, "Revealed...".

SMMO BY NON-STATE ACTORS

The covert, active employment of the Web2.0 based military techniques is characteristic for non- state actors, pursuing propaganda and recruitment related objectives. Well-crafted social media campaign of the so-called Islamic State (IS) serves as a good example of such practice. Covert techniques are used when the user intends to hide his location and at the same time to maintain the consistence of his cyber and real identity. In other words, the method enables to inform, motivate and recruit the others in a virtual space, while being undetected in a real world. Information operations play an essential role in the IS strategy. Skillfully crafted campaign is based on the decentralized approach to the messaging, which is enabled by the Web2.0 technical capabilities. The Twitter, which is the most widely utilized platform, *serves the same essential purposes for terrorist organization (IS) that bookstore and Internet forums played in the past: the proselytizing and recruitment of followers, firming up the resolve of believers by engaging them in the distribution of propaganda and educating them in dogma*.[77] The Web2.0 platforms have been utilized by the IS to build entirely new type of the information campaign. Their active, covert use of the social media is based on a highly decentralized system – such organizational solution ensures high level of the operation security, redundancy of the network and what's probably the most important – massive participation in the propagation of the narrative. According to the Danish-born political scientist, Jytte Klausen, *broad audiences can be reached directly and amplified by the echo chamber of lateral duplication across multiple platforms at low cost. A handful of hyperactive online activists can quickly and at low cost distribute massive amounts of material*.[78] Decentralized system of the 'individual jihad' has been successfully established, as a result of inspirations provided by theoreticians such asal-Suri. In accordance with his concepts, extremists' organizations should abandon the 'traditional pyramid' structures for the sake of *decentralized system which seeks to enable individual and small cell operations*. Such decentralization, paired by the *empowerment and education of operatives*,[79] builds foundation of the IS social media strategy. Functions of such highly distributed information campaign have been perfectly enabled by the Web2.0. Al-Suri's concept has been operationalized by numerous IS top thinkers. Anwar al-Awlaki, labeled as a 'small-caliber bin Laden,'[80] crafted the design of the social communication with non-Arabic jihad followers. His efforts resulted in the perfection of the global range distribution methods. Through translations and visualization he also made radical Islamic concepts

[77] J. Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq", *Studies in Conflict & Terrorism*, vol. 38, no. 1 (2015), p. 20, at <https://doi.org/10.1080/1057610X.2014.974948>.

[78] Ibid.

[79] L.J. West, "#jihad: Understanding Social Media as a Weapon", *Security Challenges*, vol. 12, no. 2 (2016), p. 14.

[80] A. Madhani, "Cleric al-Awlaki Dubbed 'bin Laden of the Internet'", *USA Today*, 25 August 2010, at <https://usatoday30.usatoday.com/news/nation/2010-08-25-1A_Awlaki25_CV_N.htm>, 20 May 2017.

accessible to those who lacked Arabic language skills or a sophisticated understanding of Islamic theology.[81]

Structurally – despite the mass and spontaneous appearance – the IS social media campaign is a well-controlled mission with *a high degree of content control*.[82] Not everyone in the organization is authorized to upload information. Fresh recruits have to give their communication devices away. 'Tweeting' or creating the messages in a virtual world is a right reserved to the most experienced and trusted fighters. The narrative of the IS members' content is carefully shaped by centrally defined and imposed guidelines. The overall master message, carried preferably in a form of pictures and short video uploads, evolves in accordance with the engagement models, specifically designed for a particular target audience. The visual content tone ranges from coercive pictures of mutinied enemy corpses, glorifying videos of heroic IS warriors to charming images of the fighters' comradeship. The narrative, shaped by the strategic leadership and created by trusted fighters is disseminated worldwide with the purpose *to build a transnational community of violent extremism*.[83] The distributive function of the network has been also very carefully designed. The IS understood both: the vital importance of this capability and the risks of compromise, associated with on-line distribution. The 'disseminators' are defined as *unaffiliated individuals who are broadly sympathetic with the jihadist*.[84] Their role is to transfer the content to the accounts, which work as hubs between extremists' sub-networks. This function is conducted primarily by females (so-called 'umms') – usually wives or mothers of the insurgents.

Extensive size of the network causes significant security risks. The covert, active nature of the IS campaign assumes a high degree of personal security for key network members. There are several measures employed by the organization to protect identity of its members and supporters. General policy of the IS communication, as described by James P. Harwell, *tries to protect the identity and location of its leadership by minimizing electronic communications among top cadres and using couriers to deliver command-and-control messages by hand. Social media is reserved for propaganda*.[85] In order to reduce the risks, network members are additionally educated in the field of the cyber security. The training is conducted by the distribution of materials such as 34-page 'counter-surveillance manual'. The publication, originally created for the political activists in the Gaza Strip, *offers a handy compilation of advice on how to keep communications and location data private, as well as links to dozens of privacy and security applications and services*.[86] Reportedly the IS has also initiated to utilize an enhanced encryption

[81] L.J. West, "#jihad...", p. 22.

[82] J. Klausen, "Tweeting the Jihad...", p. 19.

[83] Ibid., p. 18.

[84] Ibid., p. 14.

[85] J.P. Farwell, "The Media Strategy of ISIS", *Survival – Global Politics and Strategy*, vol. 56, no. 6 (2014), p. 52, at <https://doi.org/10.1080/00396338.2014.985436>.

[86] K. Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits", Wired, 19 November 2015, at <https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/>, 19 May 2017.

software. In accordance with the BBC study, *the organization has shifted its propaganda distribution to the secure mobile messaging app Telegram*.[87]

The Islamic State's information campaign is a perfect example of the covert, active SMMO conducted by a non-state actor. Propaganda serves as a key enabler for the organization's success and is almost entirely based on the Web2.0 platforms. The network capability not only allows to motivate fighters and bring new recruits – thanks to the skillful use and global reach, the campaign initiated a fearful trend of 'individual jihad', resulting in several deadly attacks conducted in Europe by radicalized Web2.0 users.

SOCMINT EFFORTS BY STATE AND NON-STATE ACTORS

With the growing signature of the extremists' narrative in the social media, the SOCMINT becomes to be one of the leading disciplines of counterterrorism intelligence. It is widely employed by state and non-state agencies, practicing passive forms of the SMMO. One of such actors, the Simon Wiesenthal Center conducts a program "Digital Terrorism and Hate Project". The research constitutes a good example of the overt, passive penetration of the Web2.0 architecture. The purpose of the program is to study *how the Internet has become a virtual university for terrorism and has emerged as the nerve center for training, recruitment, and terrorist activities around the world*.[88] The effects of the social media monitoring are published by the Center in form of an on-line reports.[89] The publication exposes the sites and users who are creating and distributing extremist narratives with use of the Web2.0 platforms. The project is oriented on a wide scope of radicalism. Despite religious extremism it also tracks racism, radical left and right wing ideology supporters. A comprehensive report is prepared on annual basis. The authors present overall strategies of the Web2.0 based propaganda, they outline a global range of examples, with actors and programs being exposed in a detailed manner. The Center's research team conducts an annual assessment of the specific social media platforms in order to evaluate their utility for the distribution of violent propaganda.

The SOCMINT offers several opportunities with the range expanding far beyond the narrative analysis. As a branch of intelligence, it supports heavily numerous agencies in their network analysis efforts. This particular discipline enables to understand, track and predict the development of the relations within the social structures. Their investigative activities are usually conducted as a covert or clandestine and passive utilization of the social media platforms. In order to retain the low profile nature, the intelligence

[87] Source: Video *Islamic State prioritise Telegram app to spread propaganda*, BBC, 9 October 2015, at <http://www.bbc.com/news/av/world-middle-east-34478695/islamic-state-prioritise-telegram-app-to-spread-propaganda>, 20 May 2017.

[88] Source: Simon Wiesenthal Center, "Understand Simon Wiesenthal Center's Mission", at <http://www.wiesenthal.com/site/pp.asp?c=lsKWLbPJLnF&b=4441471>, 20 May 2017.

[89] Simon Wiesenthal Center, "Digital Terrorism and Hate Project Report 2016", at <http://digitalhate.net/inicio.php>, 20 May 2017.

analysts employ several techniques, one of them being utilization of nongovernmental IP addresses to monitor the network. Such tactic enables to avoid compromise resulting from bloggers' use of *an analytical tool to track both hits to the blog and IP addresses of computers that access the blog, which could potentially identify law enforcement personnel*.[90] Clandestine, passive exploitation of the social media is characteristic for state sponsored agencies, which can afford to acquire and implement sophisticated technologies designed for collection and analysis of the data. The classified nature of such programs results in a very few case studies being available for an open source research. Voss Bristol in his article "Government Shop for Latest Internet Weapons" describes the purchase of specialized targeting software by Russian authorities. The package is designed to *monitor of the blogosphere and social networks in order to single out the centers where the information is created and the ways by which it is spread among the virtual society*.[91] Such tool, married with sophisticated hardware and trained personnel, without doubt serves the purpose of the passive, clandestine Web2.0 network penetration. Similar technique, with the use of unknown software is also conducted by the U.S. Central Intelligence Agency. Its "Open Source Center" reportedly employs *full time staff that include translators, researchers, and analysts*. According to the data collected in 2011, it was capable for monitoring over *five million updates, tweets, and the like, every single day*.[92] For numerous organizations the SOCMINT becomes either a main source of information, or a primary verifier of other intelligence collection sources.

CONCLUSION

As Manuell Castells points out, *for millions of Internet users, online communities have become a fundamental dimension of everyday life*.[93] Indeed, on-line interaction also became a vital communication artery, for those communities and actors, who challenge global security. The Web2.0 network created an entirely new dimension for military activities. One can say without hesitation, that it added to the air-land-maritime triad, one more battlespace domain. Since nothing seems to disturb the tendency of conflicts being about the influence rather than the defeat, the importance of newly introduced dimension will constantly grow. Rapid evolution of the technology results in the creation of new spaces for an interactive communication, example being an 'augmented reality' or the '3D virtual worlds'. As a consequence, the cognitive center of gravity of the human race constantly drifts towards systematically more attractive cyber domain. Such trend puts an immediate demand for the security community to better under-

[90] Global Justice Information Sharing Initiative, *Developing a Policy*..., p. 14.

[91] B. Voss, "Governments Shop for the Latest Internet Weapons", Minyaville, 28 August 2012, at <http://www.minyanville.com/business-news/politics-and-regulation/articles/internet-weapons-cyberspace-social-media/8/28/2012/id/43548?page=full>, 19 May 2017.

[92] K.A. Duncan, *Assessing the Use*..., p. 64.

[93] M. Castells, *Communication*..., p. 68.

stand the social media architecture. Military planners must recognize and appreciate the essentiality of the social aspects of cyber space. They need to have the knowledge and tools adequate to challenges, posed by new engagement space geometry. Such requirement inspires contemporary researchers to claim that military organizations of tomorrow *do not only need to have a presence in the social network, they need to have (strategies) doctrine, organization and capability enabling them to operate in the part of the cyber-domain to which social network media belong*.[94]

Some efforts related to the above statement were made by segregation of the SMMO employment techniques into the passive and active ones. Their further division into covert, overt and clandestine enabled to define some reoccurring characteristics of the Web2.0 embedded military engagements. The issue of the network exploitation is, however, extremely broad and it clearly calls for some further, solid intellectual investment. Social media can be effectively utilized as a 'sensor and an effector'[95] in support of irregular and unconventional campaigns. They can also be used as a vital tool of influence in recently so relevant hybrid warfare. The question whether the social media based military operations deserve their own space within the world of doctrine or should they just contribute to already defined forms of warfare remains open. Growing number of available case studies will surely offer new research areas for analysts struggling to find an answer. The 'strategic high ground' so far has been unquestionably occupied by actors challenging peace and stability. Virtual operations of the IS, outlined in this article, may serve as the best validation for such thesis. Global security seems to rely extensively on the success or failure achieved in a virtual world of social interactions. Facing such reality the security community should dedicate resources and energy to exploit opportunities and limit risks associated with the Web2.0 utilization. Despite of some initiatives specified in the publication, the Euro-Atlantic military community *still looks at war in a classical manner and therefore fails to grasp the new realities of contemporary war and the nature of its goals*.[96] Understanding the specific nature of the virtual 'many-to-many' communication, may transpire to be a major aspect, enabling to refine currently inadequate optics. To repeat the Ntrepid corporate motto, the investment should be made 'in new ideas' where one can sense 'the disruptive potential'.[97]

BIBLIOGRAPHY

Bazley L., "Combating Jihadists and Free Speech: How the U.S. Military Is Using Fake Online Profiles to Spread Propaganda", *Daily Mail*, 18 March 2011, at <http://www.dailymail.co.uk/news/article-1367535/U-S-military-using-fake-online-profiles-spread-propaganda.html>.

94 T. Elkjer Nissen, *#TheWeaponizationofSocialMedia*..., p. 55.

95 Ibid.

96 Ibid., p. 8.

97 Ntrepid, at <https://ntrepidcorp.com/>, 28 May 2017.

Burnore N., *Social Media Applications for Unconventional Warfare*, U.S. Army Command and General Staff College thesis, Fort Leavenworth 2013.

Calha J.M., "Hybrid Warfare: NATO's New Strategic Challenge?", NATO Defense and Security Committee Report, at <http://www.nato-pa.int/default.asp?SHORTCUT=3778>.

Castells M., *Communication Power*, Oxford 2013.

Chaffey D., "Global Social Media Research Summary 2017", Smart Insights, 17 April 2017, at <http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/>.

Darczewska J., *The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study*, at <https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf>.

David G.J., McKeldin T.R., *Ideas as Weapons. Influence and Perception in Modern Warfare*, Washington 2009.

De Cuia Ch., *IS (Islamic State) and the West: The Role of Social Media*, at <http://tesi.eprints.luiss.it/15151/1/070502.pdf>.

Duncan K.A., *Assessing the Use of Social Media in Revolutionary Environment*, Naval Postgraduate School thesis, Monterey, Calif. 2013, at <http://calhoun.nps.edu/bitstream/handle/10945/34660/13Jun_Duncan_Kirk.pdf?sequence=1>.

Elkjer Nissen T., "Social Media, Strategic Narratives and Stratcom", *The Three Swords Magazine*, no. 28 (2005), at <http://www.jwc.nato.int/images/stories/threeswords/SOCIAL_MEDIA_STRATCOM.pdf>.

Elkjer Nissen T., *#TheWeaponizationofSocialMedia. @Characteristics_of_Contemporary_Conflicts*, Copenhagen 2016.

European Commission, *Social Media Guidelines for all Staff*, at <http://ec.europa.eu/ipg/docs/guidelines_social_media_en.pdf>.

Farwell J.P., "The Media Strategy of ISIS", *Survival – Global Politics and Strategy*, vol. 56, no. 6 (2014), at <https://doi.org/10.1080/00396338.2014.985436>.

Fielding N., Cobain I., "Revealed: US Spy Operation that Manipulates Social Media", *The Guardian*, 17 March 2011, at <https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks>.

Geers K. (ed.), *Cyber War in Perspective. Russian Aggression against Ukraine*, Tallinn 2015.

Gladding R.S., McQuade S.P., *Cyber-Enabled Unconventional Warfare: The Convergence of Cyberspace, Social Mobilization, and Special Warfare*, Naval Postgraduate School thesis, Monterey, Calif. 2015, at <http://calhoun.nps.edu/bitstream/handle/10945/47951/15Dec_Gladding_McQuade.pdf?sequence=1&isAllowed=y>.

Global Justice Information Sharing Initiative, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities. Guidance and Recommendations*, February 2013, at <https://it.ojp.gov/documents/d/Developing%20a%20Policy%20on%20the%20Use%20of%20Social%20Media%20in%20Intelligence%20and%20Inves.....pdf>.

Handel M.I., *Clausewitz and Modern Strategy*, Abingdon 2004.

"Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia", NATO Strategic Communications Centre of Excellence, at <http://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0>.

"Irregular Warfare: a SOF Perspective", *Center for Army Lessons Learned Newsletter*, no. 11-34 (June 2011).

Kaplan A.M., Haenlein M., "Users of the World, Unite! The Challenges and Opportunities of Social Media", *Business Horizons*, vol. 53, no. 1 (2010), at <https://doi.org/10.1016/j.bushor.2009.09.003>.

Klausen J., "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq", *Studies in Conflict & Terrorism*, vol. 38, no. 1 (2015), at <https://doi.org/10.1080/1057610X.2014.974948>.

Kumar S. et al., *An Army of Me: Sockpuppets in Online Discussion Communities*, at <https://cs.stanford.edu/people/jure/pubs/sockpuppets-www17.pdf>.

Larson E.V. et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*, at <http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf>.

Lewis J.A., "Cyber War: Definitions, Deterrence and Foreign Policy (2015)", Center for Strategic and International Studies, 30 September 2017, at <https://www.csis.org/analysis/cyber-war-definitions-deterrence-and-foreign-policy>.

Lucas E., Pomeranzev P., "Information War Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe", CEPA, 2 August 2016, at <http://cepa.org/reports/winning-the-Information-War>.

Madhani A., "Cleric al-Awlaki Dubbed 'bin Laden of the Internet'", *USA Today*, 25 August 2010, at <https://usatoday30.usatoday.com/news/nation/2010-08-25-1A_Awlaki25_CV_N.htm>.

Maxwell D.S., "Do We Really Understand Unconventional Warfare", *Small Wars Journal*, 23 October 2014, at <http://smallwarsjournal.com/jrnl/art/do-we-really-understand-unconventional-warfare>.

Metz S., Johnson II D.V., *Asymmetry and US Military Strategy: Definition, Background and Strategic Concepts*, Collingdale 2001.

Mintz A.P. (ed.), *Web of Deceit. Misinformation and Manipulation in the Age of Social Media*, Medford 2012.

NATO Standarization Agency, *Allied Joint Publication 01: Allied Joint Doctrine (2010)*, at <https://www.gov.uk/government/publications/ajp-01-d-allied-joint-doctrine>.

NATO Standarization Agency, *Allied Joint Publication 3.10: Information Operations (2009)*, at <https://info.publicintelligence.net/NATO-IO.pdf>.

NATO Standarization Agency, *Allied Joint Publication 3.5: Special Operations*, Mons 2013.

NATO Standarization Agency, *Allied Publication AAP6: NATO Glossary of Terms and Definitions (2014)*, at <http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf>.

NATO Supreme Headquarters Allied Powers Europe, *Allied Command Operations Directive AD 95-3*, Mons 2013.

Niekerk B. van, Maharaj M., "Social Media and Information Conflict", *International Journal of Communication*, vol. 7 (2013).

Pomerantsev P., Weiss M., *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, Institute of Modern Russia, at <http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf>.

Porshe III I.R. et al., *Redefining Information Warfare Boundaries for an Army in a Wireless World*, Santa Monica 2013.

Seddon M., "Documents Show How Russia's Troll Army Hit America", BuzzFeed, 2 June 2014, at <https://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america?utm_term=.gsJl9nKJy#.guPKP1jlr>.

Shaheen J., "Social Media Warfare: Findings from a Daesh Analysis, Network Simulation, and Future Direction", APAN Community, 20 December 2016, at <https://community.apan.org/wg/oekn/m/mediagallery/179849>.

Simon Wiesenthal Center, "Digital Terrorism and Hate Project Report 2016", at <http://digitalhate.net/inicio.php>.

Simon Wiesenthal Center, "Understand Simon Wiesenthal Center's Mission", at <http://www.wiesenthal.com/site/pp.asp?c=lsKWLbPJLnF&b=4441471>.

"Social Constructivism", Berkeley Graduate Student Instructor Teaching & Resource Center, at <http://gsi.berkeley.edu/gsi-guide-contents/learning-theory-research/social-constructivism/>.

Svetoka S., Reynolds A., Curika L., *Social Media as a Tool of Hybrid Warfare*, Riga 2016.

US Air Force LeMay Center for Doctrine, *Air Force Doctrine Document 3-2: Irregular Warfare*, at <https://fas.org/irp/doddir/usaf/afdd3-2.pdf>.

US Armed Forces Joint Staff, *Joint Publication 3-13: Information Operations*, at <http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf>.

US Armed Forces Joint Staff, *Joint Terminology for Cyberspace Operations*, at <http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf>.

US Department of the Army, *Field Manual 3-05: Army Special Operations Forces Unconventional Operations*, at <https://fas.org/irp/doddir/army/fm3-05-130.pdf>.

Voss B., "Governments Shop for the Latest Internet Weapons", Minyaville, 28 August 2012, at <http://www.minyanville.com/business-news/politics-and-regulation/articles/internet-weapons-cyberspace-social-media/8/28/2012/id/43548?page=full>.

Weiman G., *New Terrorism and New Media*, Wilson Center, at <https://www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F.pdf>.

West L.J., "#jihad: Understanding Social Media as a Weapon", *Security Challenges*, vol. 12, no. 2 (2016).

Winterfled S., Andress J., *The Basics of Cyber Warfare. Understanding the Fundamentals of Cyber Warfare in Theory and Practice*, Waltham 2013.

Zetter K., "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits", Wired, 19 November 2015, at <https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/>.

Marcin SZYMAŃSKI – Polish Special Operations Forces officer, veteran of operations in Afghanistan and Iraq. Lecturer at the Institute of Political Science and International Affairs of the Jagiellonian University. Guest lecturer at the NATO School in Oberammergau (Germany). Graduate of the US Navy Post Graduate School.