SECURITY DIMENSIONS
ISSN 2353–7000
NO. 26; 2018 (144–159)
DOI 10.5604/01.3001.0012.7247

Digital Subversion

Ing. Milan HANKO
Armed Forces Academy of General Milan Rastislav Štefánik, SLOVAKIA

doc. Ing. Peter SPILÝ, Ph.D.
Armed Forces Academy of General Milan Rastislav Štefánik, SLOVAKIA

ABSTRACT

The aim of this article is to review and identify main attributes of a new form of subversion, so called digital subversion. Digital subversion is relatively new phenomena frequently used as vital part of nowadays resistance movement and hybrid warfare tactics. The article looks at subversion from the point of history through resistance movement and current use of hybrid warfare tactics where digital subversion can be considered as a vehicle for the deployment and achievement of other elements, tools and objectives of hybrid warfare. Within the digital subversion operating concept can be identified such elements and tools like online trolling, digital and social media, digital activism, digital media and marginally also cyber operations. Conclusion is focused on strategic and institutional perspective of how to counter digital subversion. An article expands today view on subversion as a vital element of resistance movement and hybrid warfare fused with cyberspace to a digital subversion.

ARTICLE INFO

Article history
Received: 02.05.2018 Accepted 27.05.2018

Key words
operating environment, resistance movement, social media, cyber operations, hybrid warfare

1. History of subversion

The history of wars, uprisings, coups, struggles for power, influence and freedom is full of subversion. While in the past subversion was primarily a means of the weaker against the stronger it has changed with the emergence of internet. Subversion sharply fused with cyberspace in the twenty first century, thus giving individuals and non-state actors a new tool to fight against state actors, both openly and clandestinely. Such campaigns may even abuse state actors´ economy, political system, form of government, security and defense mechanisms to wreak havoc on population. On the other hand, state actors have found themselves in a brand-new situation. They are forced to look for new security and defense approaches, build up and implement new capabilities in order to preserve their national security and promote their interests more than ever before. Today, subversion is different compared with what we had known and experienced ten or fifty years ago. By emergence of cyberspace traditional subversion was gradually enriched with the possibility of conducting digital subversion.

The history of subversion is closely related to the resistance movement which is "an organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability"[1]. There are many examples at hand, such as: The Afghan insurgency fight, or the World War II resistance movement where subversion played a vital role and enabled defeat and expelled the occupying force.

Knowledge acquisition from historical data shows us that subversion was very often a precondition or facilitator to the future political and power change and played an eminent role in coups, defeating occupying powers, or simply winning wars in general. What has changed, however, is the way how subversion is performed and uses its own means. Ancient subversion applied the same principles and had a very similar operating concept like subversion today. The change, however, is enshrined in a host of variables of subversion such as technology, security awareness, speed, and the way of dissemination of information in a global world. A real game changer here is the cyber domain. "Cyberspace is more than the internet, including not only hardware, software and information systems, but also people

[1] DOD, US ARMY, *Joint Publication 1–02 (JP 1–02) Dictionary of Military and Associated Terms*, Department of Defense (DOD) USA, Washington 2015, p. 212.

and social interaction within these networks"[2]. All these factors reshaped traditional subversion.

New era of modern subversion has begun with "a series of anti-government uprisings in various countries in North Africa and the Middle East, beginning in Tunisia in December 2010"[3] also known as the Arab Spring. A slightly different way of subversion has been present in Ukraine since 2014 and really aggressive subversion is performed by terrorists from Islamic State (IS). In all above-mentioned cases states and non-states actors heavily used online technologies and cyber operations as the means of subversion. Subversion has been known for centuries as a mix of tactics, threat and fight, whereas its present-day conjunction with cyberspace is a completely new phenomenon. Subversion in such a form can be regarded to be a simple means fight, but more often it is full part, or a component of power projection strategy. As NATO General Secretary Jens Stoltenberg declared „hybrid warfare combines different types of threats, including conventional, subversion and cyber threats"[4].

2. Subversion, resistance movement and hybrid warfare

One could ask if subversion does have something in common with resistance movement and hybrid warfare. The answer is yes they have a lot in common and they are often closely interlinked. Hybrid warfare by definition integrates the use of conventional and unconventional tactics, technics, procedures and means operated by state and non-state actors. And it consists of their components, which are usually interlinked and remain very unique. The list goes as follows: conventional operations, harmful propaganda, guerilla operations, resistance movements, cyber operations, harmful economy activities and others. When using this sort of understanding of hybrid warfare, subversion is a means enabling the application of hybrid warfare components. Other means could be information operations, sabotage, and guerilla fight. Therefore, subversion is to be seen

[2] CCDCOE, NATO, *Cyber Terms and Definitions*, [in:] *National cyber security framework manual* "CCDCOE", 2012, p. 8, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (accessed 10.08.2017).

[3] Effectiveness, *Oxford Dictionaries* 2015, http://www.oxforddictionaries.com/definition/english/effectiveness (accessed 9.05.2015).

[4] *NATO to counter hybrid warfare from Russia*, 14.05.2015, http://www.bbc.com/news/world-europe-32741688 (accessed 11.08.2017).

as a vehicle, or rather tactics through which various components of hybrid warfare could be applied, not as the ultimate goal of hybrid warfare itself.

Resistance movement as an organized effort of the civil population against its own government or against an occupying force could be either a component of hybrid warfare or a means through which the components of hybrid warfare are applied. The distinction between them what is a component, means and tool always depended from operating environment variables. In 2011, the course of the Arab Spring showed how quickly an effective resistance movement can emerge and what role subversion plays in it. An even more current example of Ukraine shows in what combination subversion, resistance movement and hybrid warfare interlocks. Very often they are interconnected vertically when subversion is used as a means, or tool of resistance movement and resistance movement is a component of hybrid warfare, or even more frequently subversion is directly a component of hybrid warfare.

3. Digital subversion

„More Europeans are concerned about the risk of Russia employing hybrid warfare than of it carrying out a conventional attack"[5]. Russia's blurred campaign against Ukraine had no official start and no formal end. Russia never admitted that it was in the conflict, which it fanned and fought. Ukraine never formally declared itself under attack, or to be in the war with Russia so it cannot formally admit its defeat.

Russia applies in the Ukraine crises a new type of warfare where information dominance is maintained together with asymmetric warfare which has coercive and subversive characteristics along with their hard power capabilities involving non-state actors and direct and indirect political, economic support of the separatist forces of the self-declared Donetsk and Luhansk People's republics. Consequences are destabilization and the escalation of political, ethnic and social tensions, destruction of economy, occupation of the Ukrainian territory and finally, the declining confidence of the population in the Ukrainian state. Furthermore, it aims to juggle the target, set partial or full-scale operating environment conditions, and/or get advantage

[5] S. Pezard, A. Radin, T. Szayna, *European Relations with Russia Threat Perceptions, Responses, and Strategies in the Wake of the Ukrainian Crisis*, p. 16, https://www.rand.org/content/ dam/rand/pubs/research_reports/RR1500/RR1579/RAND_RR1579.pdf (accessed 14.08.2017).

in the form of speed or momentum over third side´s reaction. Broad use of hybrid warfare tactics used by the Russians in Ukraine demonstrated the way subversion can be used in modern operating environments, as well as its relevance for the success of hybrid tactics.

From the historical perspective subversion for the Russians is not new. The Bolsheviks from the Russian Empire took benefit of and used almost a century ago what is known as „agent-operational measures aimed at exerting useful influence on aspects of the political life of a target country which are of interest, its foreign policy, the solution of international problems misleading the adversary, undermining and weakening his positions, the disruption of his hostile plans, and the achievement of other aims"[6]. They called it active measures. The KGB – often referred to as an old style agency – had a long history of employing active measures. The use of the measures was grounded in intelligence gathering and influence enforcement wherever it was needed. And subversion was a significant component of it.

The online world plays a crucial role in modern subversion. Especially its digital and social media make modern subversion proxy-driven. In the same vein, cyber operations are of increasing importance. The recent example is Russian government engagement and electoral interference during the 2016 U.S. presidential election „where Russian military intelligence executed a cyber-attack on at least one U.S. voting software supplier and sent spear-phishing emails to more than 100 local election officials just days before last November's presidential election"[7]. In a whole range of other operations in the same case „Russian General Staff Main Intelligence Directorate actors executed cyber espionage operations against U.S. in August 2016, evidently to obtain information on elections-related software and hardware solutions"[8].

Traditional concepts of subversion unfolded to much broader means, which could be much more easily used in order to resist, harm and damage, all in much safer manner. This is no doubt a daunting – if coura-

[6] V. Mitrokhin, *The Soviet Intelligence Officer's Handbook,* Abingdon, Oxon: Frank Cass 2004, p. 13.

[7] M. Cole, R. Esposito, S. Biddle, R. Grim, *TOP-SECRET NSA report details Russian hacking effort days before 2016 election,* 5.06.2017, https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ (accessed 23.10.2017).

[8] Ibidem.

geous – scenario for many. To conduct successful subversive IS activities on massive scale and of global impact we see today would be impossible in the past. The reason is simple, there was no online world, let alone about cyberspace. As Graham Harrison puts it, „cyberspace enables IS to intimidating to some of their distant enemies as the gunmen terrorizing people on the ground. The group's skill at manipulating social media, for recruitment and projection of power, has been acknowledged even by enemies and rivals, who have poured resources into trying to dismantle, defuse – or in the case of other jihadi groups, emulate – its online success"[9]. But can it be said that IS is really using digital subversion and not just propaganda with use of cyberspace? The case of US personnel data leakage occurred on August 2015 prove that it is not just propaganda. Spreadsheet, exposes names, email addresses, phone numbers and passwords of US security personnel were hacked and later published by IS on Twitter. In this particular case IS demonstrated an attempt to use proxy means of cyberspace to undermine the security and military, psychological, strength and morale of enemy authority without the need of having immediate population´s support within the assaulted target what definitely exceed definition of propaganda as process of persuasion or implanting the communicators` ideas in the minds of the receivers.

The way the IS uses cyberspace is an excellent example of successful and effective digital subversion.

To understand digital subversion some basic elements of subversion in- general have to be considered:

– leadership (to organize, or at least trigger required actions/engagements against the target, target group or object),
– intelligence (any information gathering process related to the object which could be used for planning and maneuvering purposes),
– communication (way of information sharing, and the process of dissemination and coordination thereof),
– maneuver (all type of actions – violent/non-violent, kinetic/non-kinetic – which help to achieve goals of subversion),
– protection (prevention of anything that could be divulged, misused, and threatened to perform subversion from harm).

[9] E. Graham-Harrison, *Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?*, 12.04.2015, http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race (accessed 14.08.2017).

Subversion usually adjusts, to unique operating environment. It requires preparation where subversion elements are evaluated and tailored from case to case. There is no generic paradigm how to prepare and execute subversion. What is suitable now could be utterly infective later. To correct, determine or refine subversion elements and adjust them to operating environment is a relatively long set of preconditions to successful subversion. But purpose of subversion remains always the same.

The Arab spring, Russia's and IS´s examples of current subversion which are often online-driven show us that such subversion is simply different from what it used to be when cyberspace had not existed. Therefore, the time is ripe for calling it „digital subversion, what soundly describes its content, possibilities and impact. Digital subversion may be defined as a set of actions using proxy means of cyberspace designed to undermine the military, economic, psychological, or political strength or morale of a governing authority without the need of having immediate population´s support within the assaulted target (object) or physical presence in it"[10]. It does not mean, however, that subversion cannot be performed without the use of cyberspace anymore, quite to the opposite – of course it can, but there is a difference whether we speak about digital (cyber) subversion or subversion in general. Such expectations are not correct.

4. Purpose, aim and means of digital subversion

Analysis of Russia's subversion in Ukraine can help us to explain the aim and means of digital subversion. Let's assume that Russian essential strategic aim in the present-day conflict in Ukraine is to achieve political might, and influence over the country in order to make it impossible to join EU and possibly NATO and bring Ukraine back to Eurasian Economic Union. This generates for Russians implied tasks to undermine Ukraine sovereignty, territorial integrity and political control over the territory and economy in order to support its higher strategy, or its particular national interests. This constitutes difference with respect to traditionally known subversion (e.g. from World War II). The opposing sides in this conflict are states not domestic population and its own government. This indicates the fact, that Russians cannot straightforwardly rely on Ukrainian popular discontent with the local government. They have to either create at least some ambiguity and boost uncertainty within civil envi-

[10] Authors' own definition.

ronment, as well as paralyze the ability of the opponent (Ukraine government) to react effectively to the extent possible. To use digital subversion at a distance with its online driven acts using digital and social media as a platform appears as an effective means to be use for such case.

Internet trolling is a mean which enables to conduct or support an action designed to undermine the political strength or morale of a governing authority and population. The goal of internet trolling is usually to impact population and its opinions. To shape them and to create specific themes, objections, attitudes and issues that are puzzled in higher, more complex, hybrid or fully military strategy. Internet trolling is not the most effective means for change opinions and attitudes in the target object. But in conjunction with other means of digital subversion it does work. „In 2014 Russia's campaign to shape international opinion around its invasion of Ukraine has extended to recruiting and training a new cadre of online trolls that have been deployed to spread the Kremlin's message on the comments section of top American websites"[11]. According to the assessment of the same source at this particular time, the ratio of supporters and opponents of Russia were about 20/80 in the foreign internet community respectively. Despite qualified estimations, most of the comments were within the pro-Kremlin scope of attitudes. The Guardian noticed, just after the annexation of Crimea in 2014, that „in fairness there is no conclusive evidence about who is behind the trolling, although Guardian moderators, who deal with 4 000 pro-Kremlin comments a day, believe there is an orchestrated campaign"[12]. Some sources like the novayagazeta.ru (Гармажапова 2013) provided a description of the so called troll farm or troll army already in 2013. What was only a suspicion in 2013 is a confirmed fact in 2017 when several sources began to publish large amount of evidence about the Russian troll army activities. „Facebook says a Russian group posted more than 80,000 times on its service during and after the 2016 election, potentially reaching as many as 126 million users"[13].

[11] M. Sedon, *Documents Show How Russia's Troll Army Hit America*, 2.06.2014, http://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america#.emraX56mA (accessed 16.08.2017).

[12] Ch. Elliott, *The readers' editor on… pro-Russia trolling below the line on Ukraine stories*, 4.05.2014, http://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online (accessed 5.05.2015).

[13] *126 Million People May Have Seen Russia-Linked Facebook Posts,* 30.10.2017, http://time.com/5003363/facebook-russia-posts/ (accessed 31.10.2017).

Extent of this paper doesn't allow detailed evaluation of all the operating environment variables and classifying their parameters necessary to set up successful digital subversion. But at least one of them need to be mentioned. It's social networking which has spread around the world with remarkable speed and goes hand in hand with digital and social media expansion which help to strengthen the freedom of speech, reduce distance between communities in a way that makes life more dynamic. Social media, highly interactive platforms through which individuals and communities share, co – create, discuss, and modify user-generated content both in peacetime and wartime. In the case of social media, we are talking about a group of „2.56 billion global mobile social media users in 2017"[14], which is a shocking number itself.

Another means of digital subversion is propaganda. Past and current Ukraine´s experience from the conflict with Russia shows how vital role can play propaganda spread through digital media and how can be successfully use as an effective means of digital subversion, or hybrid warfare. The most influential one for foreign recipients is a satellite news network called Russia Today (RT). „RT serves today as an excellent tool for propaganda (the network claims in 2014 a worldwide audience of 700 million"[15].

RT was used as propaganda means of digital subversion many times in the past and it continues to these very days. Examples of the intensive and often self-fabricated RT topics which have been used to spread propaganda are crisis in Ukraine, the European migration crisis, the American presidential elections 2016. In other words, RT is use by Russians as a means of digital subversion. However, as propaganda can be conducted separately, so more often it is use as a vital and accompanying means of digital subversion uses the same a strategic narratives that underpins digital subversion.

Successful and effective digital subversion does not rely on single means only. „The contemporary Russian model for propaganda has two of its distinctive features: high numbers of channels and messages and a shame-

[14] S. Kemp, *Special reports digital in 2011: Global overview*, 24.01.2017, https://weareso cial.com/special-reports/digital-in-2017-global-overview (accessed 16.08.2017).

[15] J. O'Sullivan, *Russia Today is Putin's weapon of mass deception. Will it work in Britain?*, 6.12.2014,http://www.spectator.co.uk/features/9390782/the-truth-about-russia-today-is-that-it-is-putins-mouthpiece/ (accessed 17.08.2017).

less willingness to disseminate partial truths or outright fictions"[16]. Dissemination of narratives and information through RT is the only means from a large spectrum used by the Russians for digital subversion. Another principle of successful digital subversion is an act aiming to oversaturate the object with orchestrated information following the same narratives. „In the words of one observer, Russian propaganda entertains, confuses and overwhelms the audience"[17].

There is an example at hand. Lisa F., a 13-year-old Russian-German girl was reported missing for over a day in Berlin in January 2016 and, after returning, she first claimed that she had been kidnapped and raped by three strangers, most probably migrants. The allegedly criminal case has been promptly used by Russian officials and media to accuse Germany of tolerating and covering up child abuse which in turn provoked demonstrations of Russian Germans in several cities in Germany. The kidnapping story has been shortly after proven to be false by police using a mobile phone analysis and Lisa admitted she went into hiding voluntarily and wasn't raped. An originator of this alleged news tried to create uncertainty and mistrust over the security forces of the state and political power in dealing with major socio-political issues. This time migration in Germany. This case showed how swift and effective can be well orchestrated digital subversion.

Another powerful digital media means is mobile phone. Traditional mobile phones are widespread in almost every family all over the world. In some regions of the world it is the main communication medium between authorities and citizens. Such being the case it seems to be quite remunerative to use mobile phones for digital subversion. As lessons from the crisis in Ukraine show mobile phones are a perfect medium for digital subversion. „Text messages (SMS) sowing fear, hate, and panic are being sent to residents in Western Ukraine. And they're being sent from Russian servers. The messages contain false information about the losses in the Ukrainian army which is fighting against Kremlin-backed insurgents in the east of the country"[18]. Mobile phones are and remain a valu-

[16] P. Christopher, M. Matthews, *The Russian Firehose of Falsehood Propaganda Model: Why It Might Work and Options to Counter It*, 2016, p. 1, https://www.rand.org/pubs/perspectives/PE198.html (accessed 16.08.2017).

[17] Ibidem.

[18] *Ukrainians receive fake SMS messages sent from Russian servers,* 25.08.2014, https://www.kyivpost.com/multimedia/video-2/ukraine-today-ukrainians-receive-fake-sms-messages-sent-from-russian-servers-361934.html?flavour=full (accessed 16.05.2015).

able medium for digital subversion, that's because it covers more people than internet given its accessibility limitations.

Let´s focus on another example. „We are trying to change reality. Reality has indeed begun to change as a result of the appearance of our information in public"[19]. One way to do this is to use social media like Facebook, Twitter, YouTube and many others. They can serve as perfect means of digital subversion. Their most striking feature is that they represent a direct cross link to social networking within the population. Social media are similar to digital media when it comes to subversion. They both use similar patterns following the use of same narratives with respect to the target audience.

The use of social media in digital subversion requires a specific approach with more stratified information adapted to the target audience. Information need to be shattered on smaller bits and pieces in comparison with information given through digital media like a TV, or website. Moreover, the use of social media in digital subversion requires a more organized and synchronized effort for it is more resource intensive and it increases operating risk with possible disclosure. Social media influence showed „reaction of Ukraine on Russian's attempts to silence pro-Ukrainian voices on Facebook when the president of Ukraine himself addressed the Facebook: We have to use all available channels to get reaction from global companies"[20]. The situation in this field has already evolved. Today „experts consider the threat level high for these platforms to be used by foreign governments or other entities seeking to influence millions because of their extensive reach and ability to disseminate both malignant links and propaganda"[21].

Some other cases of the use of social media are within the scope of terrorists from IS. „IS like no other terrorist organization before, has used Twitter and other social media channels to broadcast its message, inspire followers, and recruit new fighters"[22]. For IS digital

[19] M. Sedon, *Documents…*

[20] V. Shevchenko, *Ukrainians petition Facebook against Russian trolls,* 13.05.2015, http://www.bbc.com/news/world-europe-32720965 (accessed 17.08.2017).

[21] A. Breland, *Social media fights back against fake news,* 27.05.2017, http://thehill.com/policy/technology/335370-social-media-platforms-take-steps-to-protect-users-from-fake-news (accessed 18.08.2017).

[22] E. Bodine-Baron, *Examining ISIS Support and Opposition Networks on Twitter,* October 2016, https://www.rand.org/pubs/research_reports/RR1328.html (accessed 18.08.2017).

subversion with its use of social media is very convenient. It enables it to disturb all its enemies across the globe without being physically present as jihadists enemy´s soil Posted and tweeted videos, images, messages of IS barbaric psychopathic violence with ultimate destruction of towns, villages and humiliation of its population were acts of digital subversion that were designed to undermine the military, economic, psychological, or political strength or morale (excerpt of subversion definition). But it is necessary to keep in mind that IS´s social media usage is not a decisive platform for their operations. Most of the time, it is only a supplement to their kinetic activities.

The last means of digital subversion which deserves particular attention are cyber operations. It is necessary to recognize at the very beginning that digital subversion could be executed within the current operating environment and without such operations. Cyber operations could be complex and very efficient, but on the other hand they require time and are resource consuming. The term cyber operations may sound as an exclusively military term. It is not true, though, as chief of the NSA noted, „the source of a cyberattack can easily be disguised, and the capability does significant damage is possessed not only by nation states but by criminal groups and individuals"[23]. Therefore, cyber operations have to be taken into consideration as a means of digital subversion. The use of cyber operations for the purpose of digital subversion is more probable for the states actor, but it is increasingly becoming available to non-state actors, as well. With no further exhaustive details needed, cyber operations used in digital subversion could be broken down according to their intended or already achieved effect on its objective. We also talk about kinetic and non-kinetic effects when dealing with cyber operations.

„On 23th December 2015, the Ukrainian Kyivoblenergo, a regional electricity distribution company, reported service outages to customers. The outages were due to a third party's illegal entry into the company's computer and SCADA systems. Seven 110 kV and 23 35 kV substations were disconnected for three hours. Later statements indicated that the cyber-attack impacted additional portions of the distribution grid

[23] M. Rogers, *China, 'one or two' other countries can mount cyberattack shutting down US power grid: NSA director*, 20.11.2014, http://www.nydailynews.com/news/politics/china-capable-cyberattack-shut-power-grid-nsa-article-1.2018316,2014 (accessed 14.08.2017).

and forced operators to switch to manual mode. The event was elaborated on by the Ukrainian news media, which conducted interviews and determined that a foreign attacker remotely controlled the SCADA distribution management system. The outages were originally thought to have affected approximately 80,000 customers. However, later it was revealed that three different distribution energy company were attacked, resulting in several outages that caused approximately 225 000 customers to lose power across various areas of Ukraine. Shortly after the attack, Ukrainian government officials claimed the outages were caused by a cyber-attack"[24].

The damage caused by the attack was both kinetic and non-kinetic. If we admit that in 2015 Russia used hybrid warfare tactics against Ukraine, then cyber operations against the Ukrainian Electricity Company was a perfect means of digital subversion and fell in a broader Russian hybrid strategy against Ukraine. Cyber operations will therefore be the fastest unfolding means of digital subversion in the upcoming future.

5. Countering digital subversion

Any detailed elaboration of countering digital subversion would deserve much more space. From the strategic and institutional perspective, it is more difficult to defend and counter digital subversion than to conduct and act with its characteristics. It is also far easier to counter digital subversion in authoritarian states, than in liberal democracies. Democratic states often find themselves reacting lately, insufficiently, or not at all. Examples how does it works in authoritarians states occurred in Egypt and Libya in 2011. At that time both regimes demonstrated how relatively easy is to disconnect the Internet in order to deny the enemy from digital subversion. Both conducted controlled nationwide Internet blackout which would be almost impossible to do in the technical and social environment of liberal democracy. To counter digital subversion in liberal democracies requires more complex solution and does not focus on counter-intelligence operations only. To counter digital subversion requires wide overarching counter actions of all elements of power, be it the executive, legislative or judicial, on both strategic and tactical level. We need to rethink our security and understand that internal vulnerabilities come

[24] E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 18.03.2016, p. 4, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf (accessed 22.08.2017).

to the fore front as a major concern. This calls for more inter-agency collaboration at home and inter-institutional cooperation globally.

Conclusion

Digital subversion is a fact. It is a concept here and now, far from being something theoretical and will only boost its presence in the future. It is intensively used all over the globe. But again, it is necessary to emphasize it does not mean that subversion cannot be performed without the use of cyberspace. It could. Digital subversion may occur separately or could be a vehicle for other components of hybrid warfare. Successful digital subversion does not rely on just one means. Usually it is simultaneously orchestrated and based on the ground of many other means, be it internet or others. Such being the case, an orchestrated digital subversion act creates desired results in the minds of the audience undermining the military, economic, psychological, or political strength or morale of a governing authority.

References

1. *126 Million People May Have Seen Russia-Linked Facebook Posts,* 30.10.2017, http://time.com/5003363/facebook-russia-posts/.
2. Bodine-Baron E., *Examining ISIS Support and Opposition Networks on Twitter,* October 2016, https://www.rand.org/pubs/research_reports/RR1328.html.
3. Breland A., *Social media fights back against fake news,* 27.05.2017, http://thehill.com/policy/technology/335370-social-media-platforms-take-steps-to-protect-users-from-fake-news.
4. CCDCOE, NATO, *Cyber Terms and Definitions*, [in:] *National cyber security framework manual* "CCDCOE", 2012, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.
5. Christopher P., Matthews M., *The Russian Firehose of Falsehood Propaganda Model: Why It Might Work and Options to Counter It*, 2016, https://www.rand.org/pubs/perspectives/PE198.html.
6. Cole M., Esposito R., Biddle S., Grim R., *TOP-SECRET NSA report details Russian hacking effort days before 2016 election,* 5.06.2017, https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

7. DOD, US ARMY, *Joint Publication 1–02 (JP 1–02) Dictionary of Military and Associated Terms*, Department of Defense (DOD) USA, Washington 2015.
8. Effectiveness, *Oxford Dictionaries* 2015, http://www.oxforddictionaries.com/definition/english/effectiveness.
9. E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, 18.03.2016, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
10. Elliott Ch., *The readers' editor on… pro-Russia trolling below the line on Ukraine stories*, 4.05.2014, http://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online.
11. Graham-Harrison E., *Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?*, 12.04.2015, http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race.
12. Kemp S., *Special reports digital in 2011: Global overview*, 24.01.2017, https://wearesocial.com/special-reports/digital-in-2017-global-overview.
13. Mitrokhin V., *The Soviet Intelligence Officer's Handbook,* Abingdon, Oxon: Frank Cass 2004.
14. *NATO to counter hybrid warfare from Russia*, 14.05.2015, http://www.bbc.com/news/world-europe-32741688.
15. O'Sullivan J., *Russia Today is Putin's weapon of mass deception. Will it work in Britain?*, 6.12.2014, http://www.spectator.co.uk/features/9390782/the-truth-about-russia-today-is-that-it-is-putins-mouthpiece/.
16. Pezard S., Radin A., Szayna T., *European Relations with Russia Threat Perceptions, Responses, and Strategies in the Wake of the Ukrainian Crisis*, https://www.rand.org/content/ dam/rand/pubs/research_reports/RR1500/RR1579/RAND_RR1579.pdf.
17. Rogers M., *China, 'one or two' other countries can mount cyberattack shutting down US power grid: NSA director*, 20.11.2014, http://www.nydailynews.com/news/politics/china-capable-cyberattack-shut-power-grid-nsa-article-1.2018316,2014.
18. Sedon M., *Documents Show How Russia's Troll Army Hit America*, 2.06.2014, http://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america#.emraX56mA.
19. Shevchenko V., *Ukrainians petition Facebook against Russian trolls,* 13.05.2015, http://www.bbc.com/news/world-europe-32720965.

20. *Ukrainians receive fake SMS messages sent from Russian servers*, 25.08.2014, https://www.kyivpost.com/multimedia/video-2/ukraine-today-ukrainians-receive-fake-sms-messages-sent-from-russian-servers-361934.html?flavour=full.

Authors

Milan Hanko – External doctoral student at Security and Defence Department on Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 06 Liptovský Mikuláš 6.

Peter Spilý – Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 06 Liptovský Mikuláš 6.

Cite this article as:

M. Hanko, P. Spilý, *Digital Subversion*, "Security Dimensions", 2018, no 26, p. 144–159, DOI 10.5604/01.3001.0012.7247.