UDC 004

«Reactional» information operations in cyberspace

V. M. Mishyn[1]

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Institute of Physics and Technology*

Abstract

The article investigates reaction-type information operations that can be used for misrepresentation, concealment or suppression of an information event in society and reviews an approach to their identification.

Keywords: Information operation, intelligent data analysis, unstructured text flows, web, social networks

Problem statement

Russian aggression in Ukraine exposed an important problem of being unprepared to oppose the Kremlin in the information realm. Media attacks can do even more harm to the country's defense than military operations by influencing public consciousness. They may be used to aggravate fear, cause panic or, on the contrary, to reassure and control the population. These operations usually target internal audience and aim to maintain the government's authority and preserve the illusion of stability. Not enough attention is paid to these information operations and approaches to their identification. This paper focuses on these types of operations as, in order to defeat an enemy, one must understand his methods and approaches that may in turn reveal his weaknesses. The aim of the article is to develop an approach to studying information operations for event concealment using intelligent analysis of unstructured text data.

Previous research

Most of the current research on specialized information operations in cyberspace aims to develop methods for timely identification of and counteraction against information attacks. The most common methods include search for recurrent patterns in previous attacks, identification of dependencies and use of acquired knowledge for the detection and neutralization of similar attacks at initial stages. Analysis is chiefly conducted to identify and protect against attacks that openly aim to exert negative influence on public attitudes and directly affect the national defense capability. Generally, a specialized information operation means a series of planned actions aimed at hostile, friendly or neutral groups of people with a view to inclining them to make decisions and take actions that would be beneficial for the subject of information influence [1]. The word «planned» should be emphasized in this respect since less scientific attention has been paid to the identification of spontaneous information operations that took place in response to an event.

Summary of core material

The development of approaches to intelligent text and data analysis as well as systems built on these approaches have become an effective tool for studying and identifying previously unavailable, non-trivial, practically useful and interpretable knowledge necessary for decision making in different domains of human activity. It is specialized systems of intelligent analysis of unstructured Internet text flows that are used for the identification of information operations. The current state of technical development allows automating this process almost completely using machine learning methods. However, the variety of approaches to specialized information operations may cause type I and type II errors. That is why such systems should be used under constant supervision of experts in this field for better identification of and timely reaction to a specialized information operation. These systems must in turn satisfy certain requirements. The major ones include speed of information collection from different sources and comprehensive coverage. Textual information on a given topic may appear very quickly in very different sources. These may be web resources, social networks, TV, press, and radio. Modern search engines are not capable of covering all sources, and indexation may take a long time in the case of web resources and social networks[2]. That is why large regional Internet news outlets are most often indexed for the users to see information that is most relevant to their queries. The existing approaches to the identification of specialized operations in cyberspace can be conditionally divided into two types:

1) Classical. Essence of the method: the number of negative tone messages within equal time spans is determined [3]. If their number exceeds a threshold value, it is concluded that an information operation is taking place. The main advantage of this method is the ability to detect the operation while it is in progress. However, this method has plenty of shortcomings. Typically, there are difficulties in performing Natural Language Processing (NLP) of Slavic languages. Therefore, the complex task

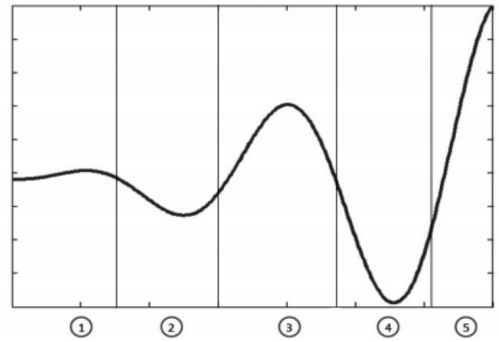

Fig. 1. dynamics of the number of messages on a given topic. It coincides with the dynamics of the information operation lifecycle

of determining a document's emotion in general and emotions of entities within it becomes even more complex. Information flows of text arrays with positive or negative topics may also be part of an information operation, so the determination of a threshold value based on expert evaluation may be false.

2) Based on temporary dynamics of information flows. Essence of the method: a graph of change in message frequency (number in a unit of time) is plotted and compared with a set pattern. If they coincide, a conclusion is made that an information operation is taking place [2],[3]. This approach has obvious advantages such as visualization of information flows which enables their comparison with patterns of information operations and prediction of action development dynamics, as well as convenience for experts.

At the same time, both methods have characteristic drawbacks — low precision, late detection of operations and possible expert errors. The approach to the identification of specialized information operations based on temporal dynamics uses patterns of typical operations.

The dynamics presented in Figure 1 characterizes an information attack model consisting of the following stages:

1) Background publications
2) Calm
3) Fire preparation
4) Calm before the attack
5) Attack

Theoretically, if similar dynamics is identified at stage 3 or 4, the attack can be countered or predicted and a response can be prepared. This model usually suits and characterizes the cases of web resource monitoring and analysis [4]. In most cases, however, attacks have a more complicated nature, distribution by types of sources, stages and speed of progression.

There are other types of information operations in cyberspace that suggest a reaction to an unexpected event, so they obviously do not have the preparation stage. They are conducted as promptly as possible. Their aim, just like in the case of prepared operations, is manipulation of collective consciousness. They may be used both as a rapid attack and as quick defense. The trigger of this operation is usually a newsworthy event that must be presented to the audience (society) in such a light that it will be beneficial for the subject of manipulation. There are numerous examples of such information attacks in the context of war against Russia. Sometimes they are so grotesque that the failed propaganda is mocked at. Such operations include stories about the «crucified boy» or the story about the skirmish by Sloviansk hyped up by LifeNews, the Russian propaganda machine: after an armed encounter a business card of Dmytro Yarosh, the leader of the Pravyi Sector, was allegedly found at the scene as well as the following items: machine gun (German, dating back to World War II), night vision device, maps, American dollars and weapons [5]. However, one should keep in mind that the Russian propaganda aims to simultaneously influence both the Ukrainian and Russian populations. Such actions on the part of the Russian state mass media in the context of information war are intended to stir up hatred and maintain the degree of hostility towards Ukraine. When information needs to be concealed for the manipulation of public opinion, the Kremlin mass media effectively diverts attention to other topics. Suppression means concealment of selected topics and information related to them. A much more frequent method is partial coverage and differentiated presentation of material. It is the way of information presentation that is the main tool to frame content in a way that is advantageous for the manipulator. For example, the situation with dead troopers from Pskov in Eastern Ukraine in summer 2014. Federal mass media did not mention this information on their websites, front pages or in TV programs. Liberal mass media were forced to remove news and photos of burial sites. Military men guarded these sites to prevent photographing and information leakage [6]. Chief Military Prosecutor's Office of Russia officially acknowledged that the circumstances of death of Pskov troopers are a state secret. It follows from the official reply that the troopers did not die at the permanent station of their military units. Criminal proceedings must be initiated automatically following servicemen's death unless it was an accident[6].

However, no cases were opened in this respect, relatives received compensation and the situation was not publicly disclosed. The information operation was successful. A definitive factor of its success was that people were ready for this development; an algorithm was created for military men and media representatives in case of such situations.

Another thing is when an unpredicted force majeure situation is taking place that shall not be made public. The spread of information must be suppressed as soon as possible. It is quite simple in case of traditional mass media: total ignoring of information or categorical denial of any facts, labeling of foreign publications highlighting the event as fake news. However, it is much more difficult to prevent the spreading of information in the web and in social networks. The subject of manipulation adopts various approaches in order to solve this problem. They include simultaneous artificial development and promotion of other topics using

controllable mass media and corrupt opinion leaders in social networks in order to divert attention from the main event. This approach may shift the focus of attention, but it cannot prevent the diffusion of unwanted information. Unexpectedly, a propagandist manipulator can take advantage of the algorithms of web sources indexation by present-day web search engines. Several search systems can be considered for the Russian Internet segment. The leaders include Google with 49% of users, Yandex with 46% and Mail.ru with 2.5% [7]. The others can be disregarded as very few people use them for searching information. It is inappropriate to run the analysis with respect to Yandex and Mail.ru since they are loyal to the Russian government and can display search results in a biased fashion. So we will focus our attention on the mechanism of the Google indexation tool. Google web crawler has a User Agent — Googlebot, which is the main crawler for scanning pages and adding them to the search index. Additionally, there are several other crawlers for the indexation of images, mobile apps, and ad profiles. Google uses the PageRank ranking algorithm [8]. This algorithm is one of the key factors for the ranking of sites in search results. The essence of the method is as follows: the more links to pages the more important the site is and the higher it is ranked in search results. Google search engine attempts to solve the problem of relevance — the ability of information displayed in search results to satisfy the user's needs (queries). It takes into account users' personal data to generate only those results that they need. This process also has shortcomings: for example, if a user always goes to a certain set of websites, search results will display these websites at the top even if there are more relevant pages on other resources. Assuming that someone criticizes Ukraine in social networks, a search query about the public opinion in Ukraine will only generate results with a negative presentation of events. Generally, whatever the query, the user will get information that does not contradict his/her opinion. This algorithm execution shapes an impression in the user's mind that an absolute majority of the population share his/her opinion, so it rejects the possibility of unbiased event coverage. It should be noted that it is now possible to turn off the personalized search feature in Google, but this function is as rarely used as users go to the second or third page of search results. Therefore, in order to block information flow to users, the manipulator's objective is to fill the search engine with information that will be relevant or similar to the user's query about the event but will redirect to websites with absolutely different topics.

As an example of reaction-type specialized information operation, let us consider one of the key events of the war in Syria that is still in progress, namely the battle of Khasham that took place at night on 8 February (when the forces of the Wagner Group that also took part in the war in Donbass were defeated), and the reaction of the mass media to this event. During the armed clash, the U.S. military carried out an air strike destroying Russian and Assad's armored task force [9]. The strike was carried out in response to the attempt of the Russian and Assad's troops to use the cover of darkness to set off to the Conoco natural gas factory near Khasham, where Syrian-Kurdish democratic forces were stationed and the headquarters of American counsellors was situated. On 7 February 2018 at 10 p.m. local time, two battalion task groups each consisting of three companies of Wagner Group contractors disguised as Syrian soldiers formed a marched column and went to the Conoco gas field near the town of Al Tabiyeh. The attack at Kurdish and American positions was carried out from the base on the left bank of the Euphrates previously seized by the Russians (approximately 80 km south-west from Deir ez-Zor in the territory which, as was agreed by the parties, was supposed to remain under the control of Kurdish military formations). A preparation fire preceded the attack. The Russian headquarters traditionally replied to the propositions of the American party to stop moving towards American and Kurdish position at the stage of deployment of Russian forces that there was «nothing happening» at their end and «they were not there». The counterattack of the U.S. artillery and air force lasted for more than 7 hours. The American high-precision missile artillery was the first to attack the Russian column, followed by military air forces. Both Wagner battalions were crushed as a result of the battle. Company 5 was destroyed almost completely[9]. A Russian artillery support group, logistic base and the Russian-Syrian headquarters deep in Assad's territory that was controlling the attack at Kurdish positions were also annihilated. The battle was over at 5:30 a.m. 8 February 2018. The official headquarters of the Russian command in Syria requested an armistice from Kurds and Americans over the radio in order to evacuate the dead and the injured from the battlefield. The Russian side did not provide any official data or information on casualties. On 15 February, a week after the event, Maria Zakharova (Director of the Information and Press Department of the Ministry of Foreign Affairs of the Russian Federation) informed that 5 Russian citizens that were not Russian servicemen might have died in the battle. She called messages about hundreds of dead Russians «false information» [10]. In the material dated 15 February, Reuters announced data on Russian casualties — around 80 – 100 people died, and another 200 were injured [11],[12].

It is worth analyzing what was happening in the Russian Internet mass media with regard to this event. Semantrum analytical system for intelligent analysis of unstructured text flows was used for this purpose. The Semantrum system was developed at the LIGA information company (promo.semantrum.net). It collects, processes and generalizes news from over 14 thousand domestic and foreign web sources. The Semantrum system is designed to find relevant topic-based news in the Internet, promptly generate search results, grant users access to online information search on multiple websites, perform semantic processing and, consequently, minimize users' effort to filter out duplicate information and information noise. Thus, if an average Russian citizen read in social networks or heard about the confrontation of Wagner Group contractors and American

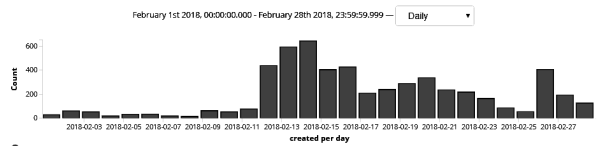

Fig. 2. General dynamics of messages as a result of «wagner» query in Russian Internet publications

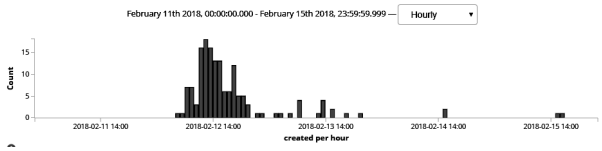

Fig. 3. Dynamics of messages concerning the figure skater Wagner in Russian Internet publications

forces in Syria, he/she want to find information about this event using a search engine in order to disprove or confirm this information. Queries may be quite different, but they will all have the head word «wagner» in common. Examples of such search queries may include the following Russian phrases:

- вагнер (wagner)
- чвк вагнер (chvk wagner)
- вагнер сирия (wagner syria)
- вагнер сша (wagner usa)
- вагнер америка россия (wagner america russia)
- противостояние вагнер сша (opposition wagner usa)
- что произошло с вагнер (what happened to wagner)
- and others

In order to block these information requests and prevent the user from accessing information related to the military conflict per se, Russian Kremlin Internet mass media had to unwind a completely different topic with similar key words in major sources. Using the Semantrum analytical system, 5568 documents were identified in Russian Internet publications dated between 01 and 28 February 2018 based on the general «вагнер» («wagner») query. The general dynamics is presented in Figure 2.

We are especially interested in the period of most frequent publications from 12 to 16 February and will not consider the subsequent fading information background of the following days. Though the military conflict took place on 8 February, related information started appearing in the Internet several days later. It was a weekend. Internet news outlets typically reduce the number of publications on days off. It should be noted that the subject was first brought up on Sunday 11 February in Ukrainian sources. This day was probably used by the Russian system to prepare the reaction of information protection. On Monday 12 February, the Russian media segment started developing a topic that would overlap with the users' queries and redirect to completely different information. Thus, on Monday a large number of publications were issued concerning the exaggerated conflict between the American figure skater Ashley Wagner and the Russian figure skater Alina Zagitova. The dynamics of these publications is shown in Figure 3. The publications often included the following phrases and sentences:

- Wagner vs Zagitova: the American attacks the Russian star
- Critical statements of the American figure skater Ashley Wagner against Russian Alina Zagitova was the subject of hot discussions in the net

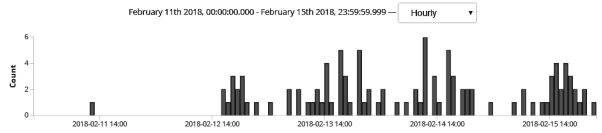

Fig. 4. Dynamics of messages concerning the military conflict in the publications of large Russian Internet sources

- The Federation of Figure Skating of Russia (FFSR) explained Ashley Wagner's criticism towards Alina Zagitova by the fact that the American cannot skate as well as the 15-year-old Russian

The use of sentences with key words that are cognate with queries concerning the military conflict cause respective pages to be indexed as such that match both queries. Extra weight to this pages is added by the use of words «Wagner», «America», «Russia», «conflict», «attack» next to each other in the text.

Before midday 12 February, a considerable number of articles were published in large news outlets in order to block the display of information in response to the «wagner» query. Large Internet news outlets basically ignored the topic of military conflict. The dynamics of messages concerning PMC (private military company) Wagner in the publications of large-scale news outlets is shown in Figure 4.

Naturally, Ukrainian Internet news outlets completely ignored the topic of exaggerated conflict between figure skaters. Publications appeared only in knowingly pro-Russian Komsomolskaya Pravda in Ukraine and ru-informer.com online media outlet, which is recognized as Ukrainian since it is situated in the Crimea. There were no anomalous peaks in English-language publications either. Although the famous American is mentioned there, the topic was only brought up in the English versions of the Russian propaganda outlets such as Russia Today and Lifenews. Thus, if the abovementioned average Russian citizen quickly searched the Internet, he/she would first see references to publications that have nothing to do with the military conflict. The specialized information operation in cyberspace was successful. The dynamics shown in Figure 5 characterizes the model of the reactional information operation.

At stage 0, an event takes place, and information about it begins spreading in the Internet mass media. Shortly, at stage 1, the subject of manipulation decides on the suppression of the information wave and the commencement of a reaction-type information operation — spreading of a parallel topic that is relevant to the main query. At stage 2, the dynamics of diffusion of the distractor topic becomes more intensive or comparable to the main one at its peak. It is the main period of

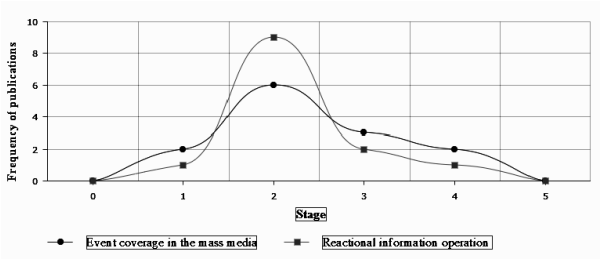

Fig. 5. Dynamics of event coverage and reaction of suppression

the topic propagation lifecycle when the manipulation target's attention is diverted. It is followed by gradual fading to complete silence.

Conclusion

The paper analyzes the existing approaches to the identification of specialized information operations in cyberspace. An emphasis is put on the fact that modern research does not pay enough attention to operations that are reactions to an event. They are used by the manipulator to conceal events and divert the attention of the manipulation target, i.e. society.

An approach is examined and a model is proposed to identify such operations using cutting-edge systems for the content analysis of unstructured text documents in the Internet using temporal series of relevant publications, their subsequent analysis and filtering for the identification of anomalous surges.

References

[1] V.M. Petryk, M.M. Prysjazhnjuk, L.F. Kompanceva, *Suggestive technologies of manipulative influence.* Kyiv, Ukraine: VITOL, 2011, pp. 31-37.

[2] D.V. Lande, «Dynamics of information flows and information operations», *Informacionnyie tekhnologii dlya menedzhmenta,* № 10, pp. 22-27, 2010.

[3] A.G. Dodonov, D.V. Lande, «Method of analytical research of dynamics of events on the basis of monitoring of web resources of the Internet», *ITV-2014. Institute of information registration problems of NASU,* Kyiv, Ukraine, 2014, pp. 3-17.

[4] D.V. Lande, *Search of knowledge on the Internet,* Kyiv, Ukraine: Dialektika, 2005, pp. 158-199.

[5] Dmitry Yarosh: "The first offensive of the war took place on April 20, 2014 - volunteers attacked the checkpoint under the Slavic". Available: https://censor.net.ua/resonance/385673. Accessed on: April 22, 2016.

[6] The graves of the Pskov paratroopers are guarded by the military, Available: https://nv.ua/ukraine/mogily-pskovskih-desantnikov-ohranyayut-voennye-9755.html. Accessed on: August 31, 2017.

[7] Search Engine Ranking, Available: http://gs.seo-auditor.com.ru/sep/. Accessed on: March 05, 2018.

[8] The Anatomy of a Large-Scale Hypertextual Web Search Engine Computer Science Department, Stanford University, Stanford, CA., Available: http://infolab.stanford.edu/backrub/google.html. Accessed on: March 12, 2018.

[9] In Syria, Russian bad faith turns fatal, Washington Post, Available: https://www.washingtonpost.com/blogs/post-partisan/wp/2018/02/09/in-syria-russian-bad-faith-turns-fatal. Accessed on: February 15, 2018.

[10] Briefing by Russian MFA Spokesman M. Zakharova, Available: http://www.mid.ru/press_service/spokesman/briefings/-/asset_publisher/D2wHaWMCU6Od/content/id/3077521. Accessed on: April 05, 2018.

[11] Russians killed in clash with U.S.-led forces in Syria, Available: https://www.reuters.com/article/us-mideast-crisis-syria-russia/russians-killed-in-clash-with-u-s-led-forces-in-syria-say-associates-idUSKBN1FW2DC. Accessed on: March 15, 2018.

[12] Russian toll in Syria battle was 300 killed and wounded, Available: https://www.reuters.com/article/us-mideast-crisis-syria-russia-casualtie/russian-toll-in-syria-battle-was-300-killed-and-wounded-sources-idUSKCN1FZ2DZ. Accessed on: March 17, 2018.