Piotr Łuczuk, Ph. D.

From Propaganda to Trolling – a Plot Theory or a Prelude for Hybrid War?

As early as 1993, the American sociologist and futurologist, Alfin Toffler, in his famous book *War and Anti-War* in a very vivid way described the beginning of wars in cyberspace (2006, p. 170). He warned that making little of the threat can lead to the situation in which a group of able hackers shall be able to run the whole country to the verge of financial collapse and anarchy, which shall consequently spread onto the whole world. Toffler was also convinced that, together with technological growth, a terrorist from any point in the world shall be able to do much more damage using the keyboard of his computer than using a bomb or a machine gun. As one of the first scientists, Alvin Toffler already at the beginning of the nineties predicted the coming of a new kind of war and the appearance of a new kind of warriors. The chief role on this global battlefield was to be played exactly by information (*ibidem*, pp. 170 – 171).

Over the recent years, we could observe many cases proving beyond doubt that transferring war activities to cyberspace is no longer fiction. The methods of running a hybrid war base in a large measure on the activities of intelligence and counterintelligence. What is even more important than the possibility of destroying the informational infrastructure of the enemy, is the possibility of gaining data and, thanks to the data gained, of eliminating security systems. What matters most in intelligence service is gaining information. Regardless of its content it can prove useful in the least expected moment. That is why during the cold war, spies would endanger their own lives to know the rhythm of their "objects'" lives and to gather all the possible information about them. Now the spying games have moved to the internet, where their activities are partly propelled by the users themselves.

Robert D. Steele, an American intelligence expert quoted by Alvin Toffler, claims that it is intelligence that should be the peak of the infrastructure of knowledge (*ibidem*). In his opinion, agents and analysts should draw both from overt as well as secret sources and the effects of their work should be accessible to everyone. Yet, in the era of technological growth, Facebook and the revealing of archives, promoted by WikiLeaks, are we not becoming more and more like characters from Orwell's "1984" living under the watchful eye of the Big Brother?

Fight for information or information war?

There is no doubt that all kinds of social portals are true mines of knowledge for agents of intelligence of particular countries. It used to cost a lot of effort to gain this type of knowledge and it was also extremely risky. Presently, on our own wish, we place in the net the whole “operational knowledge” about ourselves. On the basis of several pieces of information and the geo-localising applications, so fashionable these days, it is possible within minutes to reconstruct the whole net of connections and acquaintances of a given person, as well as define the place they are at the moment with the accuracy of a couple of metres. To an able hacker, intercepting data, passwords or bank account numbers is practically no problem, because many users do not undertake even the most basic security measures while working on the computer. Special emphasis on this kind of threat is also put by the European Commission, describing the European approach to the abilities of using media in digital environment (2007).

Threats connected with the intensification of propaganda activities as well as the first signs of informational war directed against specific countries of the European Union were noticed by the European Parliament (2016) when they noticed that hostile propaganda against EU countries has in the last years assumed new forms and that it uses tools adjusted to the specific character of the particular member countries. One of the most often used activities is internet trolling as well as using fake news – prepared news whose purpose is to cause disinformation of societies, and consequently to deepen differences in the structures of the European Union and to instigate the breach of bonds connecting strategic partners on the lines EU – USA or within the Union itself.

Today the use of cyberspace and technologic novelties for propaganda purposes is not much of a secret. Apart from direct cyber-attacks at IT structures, servers or even news services, it is propaganda in the internet which is the main pillar of the new military doctrine – the doctrine of hybrid war. However one has been talking about internet trolling and propaganda for quite a long time, a true breakthrough in this area took place only a couple years ago. In 2015, a sensational piece of news went around the world. It was a discovery of a “troll factory” in Petersburg. Officially, the city was home to the Agency of Internet Research, directed by the oligarch Evgeniy Prigozhin – privately a close acquaintance of Vladimir Putin. In fact, the agency employed over 300 „bloggers” whose task was, over a single „working day” to publish even around 30 000 internet entries, praising Russian and Putin himself on Facebook, Twitter and also on news portals in Russia as well as abroad. Since that time nobody has any doubts that there must be much more of such places only in the area of Russia itself (Łuczuk, 2017, p. 58).

Trolls not just in fairy tales anymore

The intensification of Kremlin activity on the field of information war run against EU countries has been noticed also by the authors of European Parliament Resolution, which focuses on the issues of strategic communication for counteracting hostile propaganda of third parties (2016, p. 5-7). Kremlin has at their disposal many disinformation channels, starting from teams of advisors and foundations (e.g. Russkiy Mir), through special bodies (Rossotrudnichestvo), multilingual TV stations (e.g. RT), propagandist news agencies (e.g. Sputnik) up to armies of internet trolls (*ibidem*, p. 5).

On considering the broad range of propaganda activities undertaken via internet, one should pay special attention to the differentiation of two basic groups of so-called internet trolls. The first group are **internet users who perform their duties on commission, paid for their job.** Among their duties there is, for example, writing entries and commentaries which are supposed to portray the "commissioner" in positive light, basing mainly on facts – only that the facts are suitably chosen and manipulated before. The other group are **internet users defined as so-called "useful idiots".** Their duties encompass registering profiles in social media and running blogs in which there appears properly prepared information. To this group belong also all those people, who, unaware of the whole operational game, share the information they read, believing in its authenticity and this way contributing to their credibility in the eyes of public opinion.

The CERT.GOV.PL has been warning that the social media as well as Internet as a whole are easily used to support conventional military and intelligence activities, as well as employed for propaganda purposes. Analysing cases of this type, the administrators of social media and of the greatest informational portals in the country noticed that in many cases the entries showing up on the internet are almost calques of those appearing in other services. All were published almost at the same time. Initially they were characterized by very poor Polish language, broadly ridiculed by other internet users, but gradually their quality in linguistic respect improved greatly. The CERT.GOV.PL team alarmed that the growth of acts of this kind has long since exceeded the level close to natural and poses an increasingly serious threat in the information war (2014, p. 48-49).

What was a real sensation was the revealing of the functioning of "troll factory" in Petersburg. The exact mechanism of action of the internet trolls paid by Kremlin was quite simple: officially employed people, as bloggers, were supposed to open fictitious accounts on social portals. Then, they opened their activity on the internet using numerous fictitious identities. This way they generated and published hundreds of entries and commentaries, amplifying the informational noise around a chosen issue. What is very important, the trolls usually connect to the internet through a net of proxy servers. This is to guarantee their anonymousness or in the worst case, to efficiently wipe away any traces and to confuse anyone trying to track the information to the source. Using proxies is supposed to create the impression that the entries are published by people having no relation with Russia and not staying in the territory of that country. From the point of view of an ordinary user, unaware of the whole propaganda machine, everything looked as if the internet users were really situated in the country at which the propaganda activities are aimed. Thriving like some vibrantly active marketing companies, the “troll factories” were able practically day and night to flood the internet with commentaries of smaller or bigger pro-Russian character. Often, to make all the action more credible, particular trolls would even enter mutual polemics. What else was typical, is group accusations of alleged abuse addressed to administrators of social portals, demanding blocking or removal of entries diverging from the propaganda line (Łuczuk, as quoted above, p. 59).

Unfortunately, in the course of time it became more and more difficult to distinguish the entries written by internet trolls writing on commission from those spread only by naïve internet users. It was thus hard to find unbeatable proofs for the use of elements of information war and manipulation in the Polish internet. A reliable evaluation of this phenomenon was undertaken by Andrzej Gołoś, a sociologist from the marketing agency ARC Rynek and Opinia (ARC Market and Opinion), who decided to treat the whole problem from the scientific side (2014).

Gołoś started his research from an attempt at measuring the real presence of the Russian influence in the Polish internet. He also analysed a range of discussions going on there and went through hundreds of commentaries. This way he managed to find certain patterns. It turned out that the pro-Russian entries were 39% and in 10 of the most popular articles on the Ukrainian-Russian subject there were already as much as 71%. Out of all the analysed entries, those pro-Ukrainian constituted 32, and in 10 most popular articles there were as few as 17%. The same schema could be observed during discussions run in social media. The moment any pro-Ukrainian entries appeared, immediately there came an avalanche growth of pro-Russian voices. After several hours, the attack subsided and situation came back to normal (*ibidem*, p. 9 – 15).

Similar observations were made also after an analysis of entries appearing under texts concerning Russia on CNN and BBC pages. Such a mechanism of action means that many forces were thrown into cyberspace, forces aiming to prepare ground for the possible subsequent stages of the hybrid war. It would be naïve to claim that so coordinated actions are only the effects of chance.

An Oxford researcher, Robert Gorwa, in his work describes the mechanism of creating artificial identities in the internet in order to perpetrate propaganda on a large scale (2017). Gorwa calls upon information gained from a Polish communication and marketing specialist, who for obvious reasons reserves his right of anonymousness. As an employee of a company which has for years been creating false accounts and whole identities on the internet, he has some incredibly precious knowledge as concerns using this type of mechanism in various branches of marketing – from trade to political marketing. It turns out that just this company was able within 10 years to create almost 40 000 false identities. It is worth mentioning in this point that every such false internet user had his own unique features, a story and a group of accounts in social media. The false users were also given unique IP addresses so that their activities on the internet do not arouse suspicions and were amazingly similar to standard activity in the net (*ibidem*, p. 16).

Manipulation scenario

In the context of real possibilities and results of running propaganda activities on a broad scale, what is especially noteworthy is the model of public opinion manipulation created by Trend Micro – an international company specializing in the safety of the IT sector (2017, p. 62-64). It consists of eight basic stages:

Stage 1 – reconnaissance

It assumes gathering information on the subject of the planned action as well as an analysis of the target audience. In the frames of those activities, information is gathered on persons potentially interested in the subject of those activities, their loyalty and their knowledge in a given area.

Stage 2 – armament

It assumes preparing the key history and one's own version of the facts which are then to be passed on to the target audience. This stage also assumes preparing additional fake news supporting the key history and creating various "alternative versions" of a given event. It leads to creating informational noise around a given subject and literal flooding of the internet with the manipulated message

Stage 3 – delivery

It assumes spreading the previously prepared materials and fake news via specific communication channels, e.g. social media, or traditional media. Besides, the activities at that stage assume also the possibility of using all the possible channels of spreading fake news, above all, manipulation and disinformation by the use of a net of bots and farms of internet trolls.

Stage 4 – exploitation

It assumes regular heating up of the subject in social media and strengthening the credibility of the fake news by instigating the moods of specific social groups and the fans and activists already identifying with the promoted idea.

Stage 5 – stabilizing

One of the key steps aiming at increasing the credibility of the whole propaganda action. It assumes reaching the largest possible target audience, including people of critical attitude. The main goal at this stage is enforcing interaction and the so-called viral effect from the users. The more people write/speak on a given subject, the bigger number of people shall read and hear about it, and this way the number of potential supporters of the idea, or the group of people who simply believe the fake news shall grow drastically. Often one uses the impression of an argument on a given subject, preparing both positive and negative entries, so as to raise the rank of the fake news and attract the attention of people of initially critical attitude.

Stage 6 – keeping up the involvement

It assumes bringing into the game „supporting stories", which had been prepared at the earlier stages, and instigating activity on possibly the highest level.

Stage 7 – from words to deeds

It assumes the realisations of activities mentioned at the beginning of the action. It can result in additional motivation of the target reader and lead for example to the realization of the activities assumed by the initiators of the action: organizing a rally, a manifestation, an appeal of support, an open letter.

Stage 8 – obliterating the traces

It assumes possibly the quickest aversion of the public opinion from the given problem and transferring it, suitable channelling, onto a completely different subject. In extreme cases this stage involves even a complete negation of, and wiping away, the memory of all the previous activities in order to calm down social moods. Such a way of action ensures full control over the situation and gives a possibility to efficiently "switch" the attention of public opinion onto other tracks, with the reservation of the possibility for re-activation of the original target group, if such need should arise in the future.

Conclusions

The realisation of subsequent points of this scenario means that the information war directed against European countries is already in progress. There is also no doubt that the social media have a very strong impact on reality, and what happens in virtual space more and more often really influences whole societies. Facts are increasingly losing importance in the situation where instead of objective information there circulates the prepared, fabricated information, based on the emotions of the users. It is the connection of internet and the theory of public opinion manipulation that brings those terrifying effects, especially if it all begins to rub sides with the world of politics.

Dr Piotr Łuczuk

Journalist and theologian. A lecturer in the Faculty of Internet and Digital Communication of the Institute of Medial Education and Journalism of the Cardinal Stefan Wyszyński University. Author of works on cyber-safety, informational war as well as the influence of modern technologies on social communication.

Bibliography:

CERT.GOV.PL, A report on the state of safety of the Republic of Poland’s cyberspace in 2014 (Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku), to be found on the web page: http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html.

Gorwa, R.: Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere, to be found on the web page: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Poland.pdf

Gu, L., Kropotov, V., Yarochkin , F.: The Fake News Machine. How Propagandists Abuse the Internet and Manipulate the Public, to be found on the web page: https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf?_ga=2.58817832.485134583.1503746972-1268436894.1503494608

Commission of European Communities (2007): *European approach to the ability of Rusing media in digital environment*, to be found on the web page: http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52007DC0833&from=PL.

Łuczuk, P.: Nie karmić trolla! Kulisy wojny w internecie. (Don’t feed the troll! What is behind the internet war) in: Wpis 7-8 (81-82 2017), s. 57-60.

European Parliament (2016): *The Resolution of the European Parliament from 23 October 2016 concerning union communication for the purpose of counteracting hostile propaganda of third parties*, to be found on the web page: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0441&language=PL.

Toffler A., *War and Antiwar*
Toffler A., Wojna i antywojna, Poznań 2006.