DOI: 10.53477/2668-2001-21-32

SOCIAL MEDIA IN INFORMATION WARFARE. ASSAULT WEAPON WITH HIGH RECOIL

Alin Preda[1]
ROU MOD Public Relations Directorate

Abstract

Beyond the benefits or risks of individual or institutional communication through social media, we must note that it is the perfect environment for fake news and propaganda because of the speed of information propagation, the unfriendly environment for checking sources, algorithms behind social networks and, last but not least, the extremely low cost. In other words, the Internet and web 2.0 have created the favorable framework for the conduct of the war "for minds and hearts", as it can be called the information war waged through social media. Beyond these considerations, the non-regulation of the online domain - the lack of rules, be they deontological, make social media a powerful weapon of attack in this type of war. At the same time, the use of this space by state actors should be done with caution because it involves risks that could result in the loss of the most important action capacity: credibility. This article aims to analyze social media as a tool in information warfare.

Keywords: social media; StratCom; narrative; strategic communication; propaganda; fake news; informational war; Russia.

INTRODUCTION

About social media and information warfare

Information warfare has become the most evolved form of conflict in recent years, due to low costs, low losses and maximum efficiency. The cyber warfare wage, or cyber warfare, is one of the main threats to national security.

As a natural consequence from a contextual point of view, social media is a very well-researched topic of late, and social media analysis is a priority for the commercial and political field in which very large amounts of money are invested.

Because social media encompasses a diverse range of communication styles, including multimedia and short messages, and connects a wide range of actors, it is a complex network. Analyzing the theory of complexity in terms of information systems, the networking world is a complex adaptable system with the potential for self-organization (Merali, Y. 2006, 216-228). Similarly, complexity can be seen in military systems, information warfare and riots (Schneider, J. J. 1997, 21-28) such as the Arab Spring, where a complex political system is thrown into chaos when it spontaneously reorganizes into a different state.

Information warfare is changing and spontaneously reorganizing due to the disruptive influence of another complex system: social media. The relationship between social media and information conflict has not yet reached its final state, which makes it difficult to predict the future with a certain degree of certainty. However, social media is an ideal tool for information-based conflicts. The use of social networks is not always successful in the complex system of policies and conflicts.

Some researchers warn that the role of social networks in riots such as the Arab Spring and in influence campaigns such as the one carried out by Islamic State between 2014-2016 should not be underestimated but nor overstated to prevent similar events. On the other hand, the government's attempts to block access to mitigate the riots have had varying degrees of success, which must also be assessed in relation to the context of the event.

[1] Corresponding author: alinpredapr@yahoo.com

Looking at these events we find that social media is not the main factor in triggering the uprising but the social context plays a very important role. Incitement to revolt would not be successful through social media if the political and social climate were not conducive to such events. Social media can therefore be considered a tool for triggering, supporting or facilitating information-based conflicts and perhaps not enough to create social upheavals on its own without a specific context.

Given its pervasive nature, social media is expected to become a redoubtable weapon in the information-based conflict, and its initial roles may become more significant due to the speed of information transmission, the difficulty of the source verification process and, last but not least, the algorithms behind social networks. However, we believe that, at least for the foreseeable future, social networks will remain a tool to facilitate a revolt rather than to become the primary factor of instigation.

In other ways, social media is one of the many variables in a complex system and has the ability to facilitate state changes within that system, rather than act as a catalyst for system change. In other words, social media is the main channel of communication, rapid transmission of information and environmental influence. Since the main purpose of social networks is to facilitate communication, its ability to serve as an improvised command and control network or mass communication platform for psychological operations will be an opportunity that alone will be exposed in contexts conducive to the outbreak of the uprising, as previously shown, using actions specific to information warfare.

Although information warfare is traditionally a military concept research has shown that it is relevant to the social, corporate and personal spheres (Cronin, B. & Crawford, H. 1999, 257-263), as well as the concept of strategy, or, more recently, that of strategic communication, to which it is often attached. Starting from this consideration we will address the role of social media in information warfare, considering information warfare as an application of military concepts, both in military and civilian environments.

In this context, starting from the definition of information warfare as "*actions taken to defend army-based processes, information systems and communications networks and to destroy, neutralize or exploit the similar capacity of the enemy in the physical, informational and cognitive fields* (Brazzoli, M. S. 2007, p.219)" is highlighted to us the defensive dimension and, therefore, that attacks allowed by social networks must be taken into account in determining countermeasures.

In this perspective, social media is used to create accounts and develop groups that, collaborated with the algorithms behind social networks and other programming mechanisms developed using artificial intelligence such as bot networks or the construction of non-existent human profiles, ensure their transmission and support of messages, which, if necessary, can be used in the command and control of information warfare.

The Internet and web 2.0 platforms first showed their potential in political and military unrest in 1994 when Mexico's Zapatist movement, though defeated militarily, continued its online fight in an effective campaign dubbed by researchers as "social war" (Ronfeldt, D. & Arquilla, J. 1998, 2-7).

Subsequently, social networks played a significant role in a number of large-scale civil unrest. These social disorders initiated through social networks are a form of psychological influence operations, in which instigators try to influence the perception of the general population and to urge physical action to protest (revolts) against the government. This type of unrest is increasingly common globally since the 2016 US elections, continuing with Brexit, then the elections in France, Austria, Germany and the recent US elections, validated earlier this year and which were recently given in the public space the first official conclusions on attempts to influence (National Intelligence Council 2021).

From a military point of view, the contemporary operational environment dominated by technological developments, which have increased the speed of information movement, has created new challenges, both in terms of decision-making within the Coalition and in terms of interaction with the population in the areas of operation.

Due to the ubiquitous nature of social networks, it is inevitable that military operations will not be affected by this technology. To do this, we will address both the benefits and vulnerabilities and

risks, the use of social networks in the military environment, and the implications they may have as a precursor to the use of social networks in an information war scenario.

As Prier Jarred specifies in his article “Commanding the Trend: Social Media as Information Warfare”, *“the combination of social network, propaganda and dependence on unverifiable, or hard-to-verify, online news sources introduce the possibility of completely falsified news entering the mainstream of public consciousness. This phenomenon is commonly referred to as* ***fake news*** *and has generated a significant wave of criticism of social media. Fake news is a special form of propaganda composed of a false story disguised as news”* (Jarred Prier 2017, 50). On social media, this becomes particularly dangerous because of the viral spread of sensationalized fake news. This fake news comes from several categories. There is fake news that consists of wrongly chosen titles, buried leads or stories with weak sources (Merriam-ebster Dictionary Online, s.v. “lede”).

For example, during the 2016 US presidential election, one of the most streamed fake news on social media came as a source for an American, supposedly a patriot, who posted on his blog a news that the Pope had blessed Donald Trump for the presidency who received over a million reactions on Facebook alone, without taking into account the reactions on Twitter (Tess Townsend, 2016). This news generated more reactions on that site at the end of 2016 than traditional news sources received (Craig Silverman 2016, 12-16).

ABOUT PROPAGANDA AND FAKE NEWS IN SOCIAL MEDIA

Russia's involvement in information warfare is already a certainty long before the existence of social media. According to a 1987 US State Department report on the Soviet information war, *"active measures are distinct, both from espionage and counterintelligence, as well as from traditional diplomatic and informational activities. The purpose of active measures is to influence the opinions and/or actions of individuals, governments and/or the public"* (United States Department of State, 1986-87). This report highlights that Soviet agents were trying to forge a propaganda narrative to penetrate the countries or individual candidates where they were interested in stinking. The active measures were designed, as the retired KGB General, Oleg Kalugin, explained, *"to produce short circuits in the alliances of all Western communities, especially NATO, to sow discord among the Allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America, and thus to prepare the ground where the war really takes place”* (Jarred Prier 2017, 77).

If messages designed to influence behavior have existed for centuries, it is also a certainty that methods of mass communication have allowed a wider dissemination of propaganda. Noting the rise of the media and its presence in everyday life, the French philosopher Jacques Ellul noted the simplicity of propaganda in 1965. According to Ellul, "*propaganda ceases where the dialogue begins*" (Jacques Ellul 1965, p.6).

For the propaganda to work, it needs a previously existing narrative on which to rely, as well as a network of fans who already believe the theme of the narrative, the "propagandist". While social media involves dialogue – and this should inspire us to identify and use it in combat – social media helps the propagandist spread the message through an established network.

The mechanism used is a logical one, a person is inclined to believe the information on social networks, because people are psychologically tempted to choose to pursue things that fit their beliefs and things recommended by people to ask for them. This person, in turn, is likely to share the information of others in his network (bubble), who are similar in beliefs and therefore prone to appreciate the message and who in turn will share the information further by propagating the message in turn in their own network. Consequently, in this network propaganda is certain that it has achieved its purpose. However, it is not considered dangerous because it remains located (Jarred Prier, 2017, 58) within this fan network.

The most effective propaganda campaigns are not limited to those prone to appreciating the message. Essentially, propaganda permeates everyday experiences and the individual targeted by an aggressive campaign in the media will never fully understand that the ideas he has are not entirely his own. In other words, propaganda is easier to understand if everyone around a person seems to share the same emotions on a particular subject (Thomas Rid 2013,132).

Even a general discussion among the crowd can provide the illusion that propaganda is information (Thomas Rid 2013, 85). In other words, propaganda creates the impression of the individual that he discovers the information himself, and the ideas he finds online become his own, that he learns by discovering his own information, a way in which the mind simplifies solving problems through trust in quickly accessible data. The process of learning through discovery is influenced more by the amount and frequency of information on the same topic online, and less by its accuracy or provenance (source). Essentially, the mind creates a shortcut based on the latest available information, simply because it can be easily remembered.

The Internet makes it possible to flood the daily consumption of the person's usual information, which helps to spread propaganda.

One of the main principles of propaganda is that the message must resonate with the target. Therefore, when we are presented with information that is in the structure of our faith, our bias is confirmed, and we accept propaganda.

If it's outside our network, we can initially reject the story, but the volume of information can create a heuristic availability in our minds. Over time, propaganda normalizes - and becomes even credible. It is confirmed when a fake news story is reported by the media, which has become dependent on social media for spreading and receiving news.

Social networks like Twitter and Facebook use an algorithm to analyze words, phrases, or hash tags aimed at creating a list of topics sorted in order of popularity. This "trend list" is a quick way to review the most discussed topics at a time. (Jarred Prier 2017, 58)

According to a 2011 study on social media, a viral topic "*will capture the attention of a large audience for a short period of time*" and thus "*contributes to the mechanisms for setting the goal to be achieved*."

Using existing social networks with "bots" accounts, *"foreign agents can insert propaganda into a social media platform, create a trend, and disseminate a message faster and cheaper than through any other method or information medium*" (Jarred Prier 2017).

According to the American researcher Jarred Prier, author of *Commanding the Trend: Social Media as Information Warfare*, social media facilitates the spread of a story, of an event outside the fan group, of people who believe strongly in that thing, by forming a trend. He argues that in warfare there are four factors on which the success of the formation of a trend depends.

1. the message is found in an existing story, even if it may not yet be very well known - on the basis of which the narrative can develop,
2. identifying a group of fans, people who already believe in that message and who will pass it on,
3. a relatively small team of agents (trolls) or hackers, programmers, cyber fighters
4. a network of bot-type, automated accounts.

For this mechanism to work any form of propaganda must match that narrative, a narrative that is already supported by individuals who believe in it, to penetrate the message more easily into the fan network. Typically, the cyber team (trolls, hackers, programmers, cyber fighters) is responsible for developing the specific message for dissemination. Then the team produces fake videos, memes or videos, often in collaboration with those individuals who truly believe, fans. To achieve the effective spread of propaganda, true believers, the cyber team and the bot network combine their efforts to take command of the trend (Jarred Prier 2017, 58) [18].

Through case studies conducted by the American researcher show that this model was successfully used by both Russia in the annexation of Crimea and subsequently by other state and non-state actors who have successfully managed to influence publicly through social media(Jarred Prier 2017 77) [19]. Constraint and conviction remain decisive factors in information warfare, all the more so as more and more countries turn to such techniques and try to influence public opinion through social networks.

On the other hand, even if the mechanism proposed by the American researcher will be improved with the help of artificial intelligence, I believe that the best way to counter fake news and

propaganda is still social. Also offers the antidote through active information, education and use of network users in the role of truth-spreading elves...

"Trolls against elves"

A topic addressed in the studies of the NATO StratCom Center, Riga can be translated not by achieving a rival capability to Russian trolls – which would be a big mistake of the Alliance as it could seriously shake its credibility by altering one of the main narratives - of justice and the legality of its actions - but by using them to identify fake news and counteract them by supporting the institutional message and spreading the truth.

CONCLUSION

In order to have an overview of social media, in addition to the fact that these technologies are centered on the concept of user-generated content, online collaboration, information sharing and collective intelligence (Davidson, M. A., & Yoran, E. 2007, 117–119)[20] we must keep in mind that these technologies are centered on the concept of social network, a concept that has integrated users and made possible the generation and exchange of content, producing collective intelligence and, by implication, the emergence of Web 2.0. Therefore, social media and web 2.0 are new concepts based on a concept recognized for its characteristics, developed with the help of technological evolution and the emergence of the Internet.

Basically, if the social network makes the difference from "one-to-one" or "door to door" communication to "from three to infinite plus" communication to mass communication, virtual space, the Internet and web 2.0 make the switch to ***virtual social networks*** in which it is preserved and even amplifies the intention to communicate with the transmission of the desire and intention to influence.

As Jacques Ellul explains, *"in this context, as a conclusion to the conclusion, to counter fake news and propaganda through social media is necessary an analysis and an integrated response in the same environment is necessary. In other words, a multidisciplinary analysis team and a prompt and committed reaction to social media are required. First of all because this is the channel on which the fake news was posted and propagated and naturally the reaction must reach those infected with fake news, exposed to propaganda and, secondly, because the speed of the spread of information as well as the interaction specific to social networks favors both the time and the volume/number of users exposed to information, power and rhythm on the penetration of information using the principle that* "p*ropaganda ceases where the dialogue begins*" (Jacques Ellul 1965,6).

Just as propaganda needs to function by a "bubble" of users who believe in the narrative that dresses the propaganda, so counterpropaganda needs a "bubble" of users to identify it as propaganda and help spread this message. Because, as I previously mentioned, the individual is inclined to believe the information on social networks, because people choose to pursue things that fit their beliefs. This individual, in turn, is likely to share the information of others in his network, who are similar in beliefs and therefore predisposed to appreciate and promote the message in turn. Basically, applying the same principle of "bubble", as there are followers to promote fake news there is also to counter it. The difference, in applying this principle, can be made from my point of view by the sensational information.

At the same time, I believe that to successfully apply this counter-terrorism principle and turn users into combatants in countering propaganda and fake news, they must be educated both to detect them and to understand the special role they can play in this process.

It is obvious that social media has become a ubiquitous source of communication that poses security threats and plays an important role in information conflict. These threats, especially vulnerabilities, malicious codes and social engineering, illustrate that social media is a tool that can be used offensively in information warfare. For the defense against such attacks, it is recommended that vulnerable individuals and organizations implement a multi-technical layered defense to minimize the likelihood of a security incident occurring. Social networks may continue to be a tool in information conflict, but they are unlikely to be the main incitement factor. Its use as an information warfare tool may eventually decline, but it will still be useful for mass influence operations.

REFERENCES

Argenti, Paul A. 2009. Corporate Communication, McGraw Hill Higher Education.

Aristotle. 2007. *Metaphysics, About Interpretation*, translation Andrei Cornea, Bucharest. Humanitas Publishing House.

Aristotle. *Rhetoric*, bilingual edition, translation, introductory studies and index by Maria Cristina Andries, notes and comments Stefan Sebastian Matei, Iri Publishing House, Cogito collection.

Brazzoli, M. S. 2007. *Future prospects of information warfare and particularly psychological operations*. In L. le Roux (Ed.), South African army vision 2020. Pretoria, South Africa: Institute for Security Studies.

Christakis, Nicholas A. Dr., and Dr. James H. Fowler. 2009. *Connected*, Ed. Curtea Veche.

Cronin, B., & Crawford, H. 1999. *Information warfare: Its application in military and civilian contexts*. Information Society, 15 (4).

Davidson, M. A., & Yoran, E. 2007. *Enterprise security for Web 2.0. Computer*, 40 (11)

Ellul, Jacques. 1965. *Propaganda: The Formation of Men's Attitudes*, New York: Knopf.

Fry, Hannah. 2018. *Hello world! Computer Revolution and the Future of Humanity*, Corinth Future.

Merali, Y. 2006. *Complexity and information systems: The emergent domain*. Journal of Information Technology, 21 (4).

National Intelligence Council, 10th of March 2021, *Foreign Threats to the 2020 US Federal Elections, Intelligence Community Assessment*, Declassified by DNI Haines on 15th of March 2021.

NATO ACO Directive (AD) 95-2 Strategic Communications, 21st of May 2012, Ronfeldt, D., & Arquilla, J. 1998. *The Zapatista social netwar in Mexico*. Santa Monica, CA: RAND Corporation.

O'Reilly, T. 2005. *What is Web 2.0?* Online: http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1, accessed on 19th December of 2020.

Potter, L. R. 1998. *The Ten-Step Strategic Communication Plan*, 1999 Yearbook of Global Communication, Madrid, Spain, October.

Prier, Jarred LTC. USAF. Commanding Trend: Social Media as Information Warfare.

RAND Europe. 2010. *NATO's Strategic Communication Concept and its Relevance to France*.

Silverman, Craig. 2016. *This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook*.

Townsend, Tess. *The Bizarre Truth behind the Biggest Pro-Trump Facebook Hoaxes*.

United States Department of State, report. 1987. *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-87*. Washington, DC: Bureau of Public Affairs.