ieee.es
Instituto Español de Estudios Estratégicos

Opinion
Paper

Visit Web Receive Newsletter

45/2019 27 May 2019

*Samuel Morales**

Information warfare: feed information with disinformation

Information warfare: feed information with disinformation

Abstract:

After the Cold War, Russian elites were convinced that the attempts at expansion of the European Union and the Atlantic Alliance, as well as the impulse of democratic values in the Eastern European countries, were designed to isolate Russia. In response, Russia began promoting the ideology of traditionalism, the sovereignty of States, and national exclusivity.

The propaganda campaigns used led to an on-going information operations activity coming from Russia, irrespective of the existing relations with the countries concerned. These activities have led to the emergence of cognitive security to face a true "arms race" to influence and protect our societies.

Keywords:

Disinformation, Information, Internet, Propaganda.

How to quote:

MORALES, Samuel. *Information warfare: feed information with disinformation*. Documento de Opinión IEEE 45/2019. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

***NOTE:** The ideas contained in the Opinion Papers shall be responsibility of their authors, without necessarily reflecting the thinking of the IEEE or the Ministry of Defense

.

Introduction

Cédric Villani, celebrated mathematician and winner of the ‘Fields Medal’ in 2010 said in an interview with *El Mundo* that we should be afraid of what already exists: the Internet *bots* of fake news, adding that he feared more an app specialized in disseminating fake news, than a killer robot[1].

On the other hand, Jordi Costa, a regular reporter of ‘*El País*’, asserts that seduction attempts based on stories is an old treat that has to be managed in accordance with the ways in which they manifest themselves. At present, such manifestation takes place in a moment of a never-ending technological spree where we do not know if it is going to become the dominant channel to consume fiction[2].

With the development of technology and social networks, a series of biased, fragmented and even ephemeral narratives have begun to flourish everywhere. Henry Jenkins a famous media scholar, in an article in the MIT journal *‘Technological Review’* published in 2003, talked of what he defined as ‘transmedia storytelling’. A trend that has two characteristics: that history is narrated in many media and platforms, and that the public participates by disseminating it.

In addition, we cannot ignore the fact that the cross-sectional nature of social networks –or search engines on the Internet– has allowed their managers to position themselves as mere facilitators of data and opinions without having to take responsibility for the contents published therein by users; a deeply disruptive event.

The role of the public, the last link of the narrative chain, is the one that has undergone a more dramatic change thanks to technology, definitely breaking the borderline between spectators and creators. In just over a decade, the development of communications technology, and the emergence of social networks, has a turned citizenship not only into consumers of information, but also into distributors.

[1] Aitor Hernández “El genio matemático de Macron: Temo más a las fake news que a un robot asesino”. El Mundo (2018). Available in: https://www.elmundo.es/papel/historias/2018/12/29/5c266777fc6c8345148b468f.html

[2] Guillermo Arena “Nuevas narrativas. Los secretos de los cuentistas del siglo XXI” El País (2018). Available in: https://retina.elpais.com/retina/2018/11/19/tendencias/1542638174_916044.html

This new reality represents a change in the form of attacking what the Prussian strategist Carl von Clausewitz considered the center of gravity of the enemy; namely the mind and spirit of its population. Massive bombing or complicated propaganda campaigns are no longer required. The only thing needed is a smartphone and a few seconds of activity.

In this way, the influence on the cognitive space through Social Networks has dramatically changed the speed with which information is disseminated, the distance to which it travels and the ease of access. An influence that will increase as new forms of artificial intelligence are developed.

All this has transformed everything, from military planning to political campaigns and the information business, creating an environment characterized by a large amount of subject matter generated by a myriad of sources; a real challenge for modern societies.

Mobile technology and the Internet have provided state and non-state actors with a new tool of global proportions. This revolution compels governments, companies and citizens to understand the potential threats of the digital world and adapt their structures and strategies to confront them.

A new historical period: the era of Post-truth

History as an academic discipline was born as an opposition to war propaganda. In the first history book, *The Peloponnesian Wars,* Thucydides was careful enough to distinguish between the justifications given by the leaders of their own acts and the true reasons for their decisions. Today, as the surge of inequalities reinforces the role of political fiction, investigative journalism becomes increasingly important too[3].

But lies do indeed exist in politics. In *The Prince*, Machiavelli wrote that the breaking of promises, when those promises go against the idea of the ruler, was not only legitimate by virtue of its practicality, but also easy to undertake, since ‘men are so simple, and governed so absolutely by their present needs, that he who wishes to deceive will never fail in finding willing dupes’.

[3] Timothy Snyder “El camino hacia la no libertad” Galaxia Gutenberg. Barcelona (2018)

Diego Rubio has written that demagoguery and falsehood have always played an important role in politics. The truth has not lost importance; what happens is that it has multiplied. It is no longer one truth but many, apparently all equally valid. Thus, in today's world, does not compete against lies, but against other truths[4].

In the times in which we live, the truth is not found, but built. The real problem is that ‘Modern Man’, as Federico Aznar Montesinos says, does not think, he informs himself. The cycle of information is 24 hours, maximum 48. There is no way to contrast the huge number of news that flow through the networks every day[5].

The variability of the current world has contributed to the emergence of a new concept. The Oxford dictionary defines ‘post-truth’ as ‘relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief’. This concept explains the current circumstances and, although powerful people have always wanted to manipulate public opinion, what is certainly new is that the influence of these emotional lies has penetrated very deeply in a generation which is supposedly the best informed and educated in history.

According to the Annual Report on ‘*Trends in Reputation and Management of Intangibles*’, issued by *Corporate Excellence* (Center for Reputation Leadership) and *Canvas Sustainable Strategies*, more than 71% of the global population does not trust its institutions, and 63% is unable to distinguish between real news and rumors[6].

The post-truth era also arises from the wariness of rational arguments, and the disqualification of those who transmit them. As journalist Matthew D'Ancona has pointed out in a study focused on brexit and Donald Trump, ‘the collapse of trust is the basis of the post-truth era: everything flows from this single poisonous source. All developed societies rely on a high degree of honesty to preserve order, to respect the law, to hold the powerful accountable, and to generate prosperity’.

[4] Diego Rubio “La política de la posverdad”. Política Exterior, March/April Madrid (2017)

[5] Federico Aznar Fernández-Montesinos “La posverdad y la seguridad nacional” Claves de razón práctica, Nº 260. Madrid (2018)

[6] Corporate Excellence “Informe anual sobre tendencias en reputación y gestión de intangibles” Madrid (2018). Available in: https://www.corporateexcellence.org/recurso/approaching-the-future-2018/010cd1e0-243f-3213-adc1-

However, according to Felipe Fernández-Armesto, the elites are unable to offer comfort and security to a public easily frightened by uncontrollable changes and inexplicable problems. When people access to the Web looking for answers, what matters is not the truth or the scientific evidence of the information, but —purely and basically— that it is simple and intelligible[7].

One of the features of the world in which we live is the tendency towards distrust and skepticism. There is, however, a great paradox: at the same time that trust in governments is minimal, our credibility with certain messages from the Internet is complete. This is what Moisés Naím considers the paradox of trust. We do not believe in the government or the experts, but in anonymous messages that appear in *Facebook*, *Twitter* or *WhatsApp*.

People trust what sounds good, but trust allows manipulation. This paves the way for the rise of disinformation campaigns, which are not randomly generated, but are consistent with identified vulnerabilities detected by the trails we leave on the Internet. A variant of these campaigns may occur when people are led towards an increasingly intense annoyance at something they already fear or hate from the beginning.

Federico Aznar says that post-truth poses an important risk to national security by putting pressure on society and the apparatus in which it is sustained. Citizens have been overexposed through social networks to the influence of actors with particular interests, who try to influence the existing rules and the moral conscience of society[8].

A tool used not only by State actors

From the very beginning, and according to Sebastián Sánchez Castillo, the terrorist organization *Al Qaeda* has been deeply aware of the critical role communication could play to its own advantage. Thus, in a letter addressed to the spiritual leader in Afghanistan, Mullah Omar, Bin Laden acknowledged that ‘it is obvious that in this century

[7] Felipe Fernández-Armesto “La era de las noticias falsas” El Mundo (2018). Available in: https://www.elmundo.es/opinion/2018/12/20/5c1a4702fdddffb5798b45f6.html

[8] Federico Aznar Fernández Montesino (2018). Op. Cit.

media wars are one of the most powerful methods. Its influence can, in fact, represent 90% of the total planning of battles'[9].

This concern for the dissemination of information led Abu Musab al Zarqawi to affirm that 'we are conscientiously preparing material for the media that will reveal the facts, reaffirm our intentions, enhance our determination and become the fighting arena for a Jihad where sword and pen look at each other firmly in the eye'.

However, and despite the importance given to communication within Al Qaeda, the Saudi organization would need years to reach the intended communication skills.

The emergence of ISIS in Syria and Iraq represented a new qualitative leap in the management of communication within the world of jihadist-type terrorist organizations. According to Fernando Reinares and Carlota García-Calvo, with this insurgency propaganda, ISIS tried to give an image of success, offering to individuals of European societies going through an identity crisis, a much sought-after 'sense of belonging' and becoming part of a new jihadist society. This referred mainly to second and third generations of immigrants from predominantly Muslim countries[10].

A much more unknown dimension is presented by Colonel Gómez de Ágreda who upholds that the former sense of balance whereby States attacked States, companies competed with other companies and individuals harassed other individuals, is no longer valid. The adversary is now a concept, a way of performing, rather than a specific sector or field[11].

Moreover, Juan A. de Castro and Aurora Ferrer, when talking about the use of destabilization tactics by governments, underline that a well-organized handling of information is 'a must' if those campaigns are to work properly. Success is hardly possible if there is no prior media control[12].

[9] Luis Veres y Germán Llorca (coord.) "Comunicación y terrorismo" Tirant humanidades. Valencia (2016)

[10] Fernando Reinares y Carola García-Calvo "Siria, Irak y la movilización terrorista en España: reactivación de redes latentes y eclosión del yihadismo homegrown" Real Instituto Elcano, ARI 50/2014, (2014)

[11] Gonzalo Araluce "Coronel Gómez de Ágreda: Ha habido injerencias extranjeras para desestabilizar Cataluña". El Español (2019). Available in: https://www.elespanol.com/espana/20190308/coronel-perez-agreda-documentadas-injerencias-desestabilizar-cataluna/381462864_0.html

[12] Juan A. de Castro y Aurora Ferrer "Soros. Rompiendo España" Bibliotheca Homolegens. Madrid (2018)

They added that, although disinformation was a recurring mechanism for certain leaders and a means to fight non-friendly States in wartime, the practice has been extended to anyone holding a minimum of power, no matter whether they are sharks, wild lobbies, terrorist organizations, pressure groups or hackers looking for a minute of glory.

It has traditionally been said that whoever has the information has the power, but the truth is that power is held by those who control the dissemination of news. The struggle, therefore, will always orbit around communication.

Operationalization of a strategy

From 2006 to 2017 the Massachusetts Institute of Technology conducted a study of 126,000 rumors and fake news published on *Twitter*. They were messages reaching 3 million users 4.5 million times. The conclusions published in '*Science'* and entitled *The spread of true and false news online*, were alarming[13].

Taking as a sample a group of 1,500 users, they found that a false piece of news arrived six times faster than a true one. This happens in all fields: finance, science and technology, but especially in the world of politics. 'False/Fake news about politics spread faster and more widely, reach more people, and become more viral than any other piece of false information'.

According to the aforementioned report, political disinformation reaches a group of, say, 20,000 people three times faster than it takes real information to reach only 10,000. This means that disinformation travels faster than real news. From this analysis, the authors draw the conclusion that a lie is usually shared in social networks 70% more often than a real fact.

An interesting conclusion extracted from that report is that, contrary to what is normally believed, robots disseminated true and fake news at the same rate indistinctively. This implies that fake news spread more extensively than truths because people, not robots, are more likely to disseminate them. Therefore, it is clearly inferred that implementation

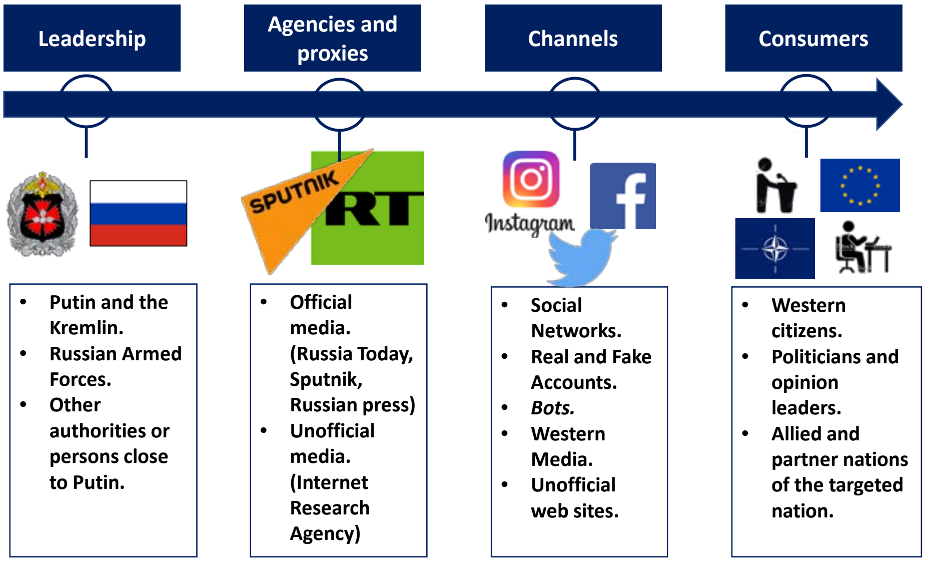
[13] Soroush Vosoughi, Deb Roy y Sinan Aral "The spread of true and false news online" Science Magazine (2018). Available in: https://science.sciencemag.org/content/359/6380/1146

of disinformation containment policies should focus on behavior rather than on restricting ‘bots’.

The main problem of disinformation is, then, its very existence as a weapon to destabilize democratic processes and institutions. A large part of fake news are designed with a political aim and reproduced in digital platforms taking advantage of the architecture of their algorithms. In other words, *bot* networks, so difficult to identify and locate geographically, are part —but only a part— of the problem[14].

However, a study published on the eve of the last US elections warned that *bots* could jeopardize the accuracy of the presidential election. Three fundamental problems were pinned down: ‘In the first place, the ability to influence with malicious purposes can be shared between different suspicious accounts; secondly, political conversations can become even more polarized; and third, the dissemination of false and unverified information may increase’.

As a complement to the study published in *Science* in January 2018, *Twitter* admitted, at the request of the United States Congress, that during the 2016 presidential election campaign it had detected 50,528 automatic profiles that were located in, or related to, Russia. At least 677,775 real tweeters followed at least one of those profiles, or interacted with their publications, sharing news or ‘*liking’* them.


Leadership
Agencies and proxies
Channels
Consumers
SPUTNIK
RT
Instagram
Putin and the Kremlin.
Russian Armed Forces.
Other authorities or persons close to Putin.
Official media. (Russia Today, Sputnik, Russian press)
Unofficial media. (Internet Research Agency)
Social Networks.
Real and Fake Accounts.
Bots.
Western Media.
Unofficial web sites.
Western citizens.
Politicians and opinion leaders.
Allied and partner nations of the targeted nation.

[14] David Alandate “Fake News: la nueva arma de destrucción masiva” Ediciones Deusto. Barcelona (2019)

At the same time, a group of researchers from the City University of London examined 10 million *Twitter* messages about the brexit campaign and found 13,493 false or automatic generated profiles related to Russia because of their location or the type of content they disseminated before the referendum.

The brexit referendum is perhaps the best example of the authentic and harmful effects that disinformation can have on society. David Alandete sustains that those who opposed the exit of the United Kingdom from the European Union, including David Cameron's own Government, were convinced that such a move was impossible and did not take protective measures against fake news[15].

Despite those signs, most US or UK voters were probably subject to propaganda generated from Russia during 2016. It is therefore significant that *Facebook* closed 5.8 million false accounts before the elections in November 2016. These accounts had been used to disseminate political messages. In that year, around one million *Facebook* pages used a tool that allowed them to artificially generate tens of millions of '*likes*' and, in this way spread certain stories, often lies, into the unsuspicious American information channels.

One of the most obvious intrusions from Russia were the 470 *Facebook* pages created by the Internet Research Agency supposedly belonging to organizations or political movements in the United States. The campaign from Russia also included a minimum of 129 event pages, which reached at least 336,300 people.

Furthermore, just before the election, 3,000 *Facebook* ads were sent from Russian territory promoted as '*memes'* in at least 180 *Instagram* accounts. This was done without including any legal notice about who had paid for the advertisements, so that the Americans were possibly left with the impression that foreign propaganda was a national debate.

Measuring the real impact of all these activities is a huge and complicated task, but it goes without saying that there were clear influences in the 2016 U.S. presidential election campaign.

[15] Ibid.

David Alandete asserts that in 2016, Russia denied the opportunity to freely choose a candidate of the Democratic Party by hacking accounts of members of the National Democratic Committee on the one hand, and the Clinton campaign on the other, just before the convention was held[16].

The leaked messages were carefully chosen to ensure disagreements between Clinton supporters and those of his nomination rival, Bernie Sanders, and created division at the time when the campaign should have converged. The information made public from Russia referred to real people who were playing important roles in the democratic process in the United States. Such publications may have affected their psychological state and political competence during the election procedure.

Also significant was the fact that those who were trying to organize the National Democratic Convention, whose telephone numbers had been made public through social networks, received death threats on their mobile phones. Besides, many private citizens who had made donations to the Democratic Party were harassed and threatened after their private data had been circulated.

The European Union has set up a High-Level Panel to study the influence of fake news and disinformation campaigns through the Internet, as a direct consequence of the alarm created by the incidents occurred in the United States and Great Britain. The report presented to the European Commission highlighted the role of Internet platforms in magnifying this type of contents[17]. Thus, and according to the Panel report, there is clearly a magnification of disinformation through social networks and other online media.

In addition, the document published by the European Commission identified the innermost structure used for the proliferation of disinformation:

[16] Ibid.

[17] European Commission "A multi-dimensional approach to disinformation" Bruselas (2018). Available in: https://blog.wan-ifra.org/sites/default/files/field_blog_entry_file/HLEGReportonFakeNewsandOnlineDisinformation.pdf

1. Use of algorithms: algorithms focus on the visualization of information encouraged by the business model of those platforms and also on the fact that these algorithms favor a personalized and sensationalist content, which is normally more likely to attract attention and be shared among users. By encouraging the exchange of personalized content among like-minded users, the algorithms indirectly increase polarization and strengthen the effects of disinformation.
2. Advertising-based strategy: the current model of digital advertising is usually based on user 'clicks', which favors sensationalist and viral content. These advertising networks are operated by agencies that ensure that those ads on websites disseminate sensationalist content –including disinformation– that appeals to the emotions of users.
3. Technological facilitation: online technologies such as automated services artificially amplify the dissemination of disinformation. This technological mechanism —sometimes orchestrated on a massive scale— is based on simulated profiles, behind which there are no real users.

On the other hand, and after the alleged interference of Russia in the *Brexit* referendum, the United Kingdom created a Committee to analyze the causes and the possible solutions to face these types of threats.

The published report sustains that people can accept and give credit to information that reinforces their viewpoints, no matter how distorted or inaccurate, while they discard (as fake news) the information they do not agree with. This trend has a potential polarizing effect and reduces the possibility of a coherent and well-structured debate based on objective facts[18].

Moreover, the aforementioned report provides detailed definition of what can be considered 'fake news' in an information environment influenced by disinformation:

[18] UK House of Commons "Disinformation and 'fake news': Final Report". United Kingdom (2019). Available in: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

1. Made-up information: completely fake news.
2. Manipulated information: distortion of information or real images. For example, a sensationalist headline ending up becoming popular with more ‘clicks’.
3. Information from false sources: impersonation of sources by impostors. For example using corporate images of news agencies.
4. Misinformation or ill-intentioned information: misuse of information. For example, disguising an opinion as a fact.
5. False contexts or connections: real information shared with false contextual information. For example, when the headline of an article does not reflect its content.
6. Satire and parody: funny information is presented as if it were true. Although not usually considered fake news, this category can deceive readers intentionally.

Given all this evidence we can conclude that, for the information activity being part of the harassment exercised in what is known as the ‘Grey Zone’, the information itself has to become a *weapon*, which is not really possible if it is only a staging of reality. In order to use the information as a *weapon*, this must be transformed and modified taking into account the objectives of the conflict.

As a result of these interferences, when the information is inaccurate, incomplete, decontextualized, based on rumors, or the result of disinformation campaigns, impulsive reactions can be triggered and emotional decisions made, even stopping an action that is in progress. A duel of stories appears then, in which the contenders are the ‘who’ and ‘how’ the narration of events is established.

Information operations in the Russian military doctrine

Throughout this document, repeated reference has been made to several authors who accuse Russia of being allegedly responsible for the use of disinformation campaigns. And while it is necessary to reiterate that this type of operations can be carried out by state and non-state actors, the fact is that Russia has raised information operations to a new level. However, their origins are not to be found in the nonexistent *Gerasimov* doctrine, but constitute a structural characteristic of the way in which they achieve their political objectives since the Russian Revolution of 1917.

Russian President Vladimir Putin has revived the Russian philosopher and ideologist of the Russian Military Union, Ivan Alexandrovich Ilyin (1883 - 1954)[19]. Ilyin, and other Russian nationalists after him, had defined the Western World, as a spiritual threat whose very existence gave rise to realities that could be harmful or confusing to the Russians.

According to this logic, the preventive cybernetic war against Europe and the United States is justified insofar as it is technically feasible. And Russia, after political disagreements with the West, is interested in a weak Europe, a knocked-out United States and a paralyzed NATO. In order to achieve its strategic objectives, it uses disinformation campaigns as a tool to create confusion and enhance existing problems, not to favor one over the other.

Disinformation endeavors intended to influence the European Union seem to have taken different forms: recruitment of European leaders and political parties wishing to disintegrate Europe; use of digital tools and television to sow the seed of distrust in the Union; and support all kinds of separatist movements[20].

Some Russian media are following the strategy of magnifying any protest that may harm European authorities, trying to spread a message of chaos and hate, not because of a specific reason, but because the conditions are favorable. Its activities therefore are aimed at creating problematic situations and uncertainty.

Internally, the fear of instability campaigns by the West led to the creation of a huge network of digital news media with two main features: the news themselves and technology, that is to say: the content and the channels to disseminate it in a massive way.

In 2013, Margarita Simonián, editor-in-chief of the English-language version of *Russia Today*, spoke about information using war terms and highlighting its importance in critical moments: ‘This information weapon is used at critical moments, and war is always a critical moment. It is about war. It is a weapon like any other. And why do we need it? It's

[19] Timothy Snyder “El camino hacia la no libertad” Op. Cit

[20] Agencia EFE “Snyder: Es claro que Rusia está detrás del "brexit" y del separatismo catalán” OK Diario (2919). Available in: https://www.eldiario.es/cultura/Snyder-Rusia-detras-separatismo-catalan_0_842366405.html

almost the same thing as saying: Why do we need the Ministry of Defense if there is no war?'[21].

The use of information as a weapon obviously requires a loss of objectivity. Alekséi Volin, vice-minister of communications, described the professional future awaiting the workers of state television networks in the following way: 'They will work for Man, and Man will tell them what to write, what not to write and how to write this or that. Man has the right to do it because He is the one who pays them'[22].

This loss of objectivity coincides with the description of the world made by Vladislav Surkov, first deputy head of the Russian Presidential Administration from 1999 to 2011. At that time he was considered one of the greatest political ideologists of Russia and suggested and implemented the concept of sovereign democracy in Russia. According to Surkov, nobody ever says the truth; perhaps the truth does not even exist[23].

In his work '*Close to Zero'*, Surkov states that facts only provide facts, but uncertainty gives hope. So let's just repeat the things we like to hear and obey those who say them. If the only truth is the absence of truth, the liars would be honest servants of Russia.

Also in 2013, Dimitri Kiselyov, director of the '*Rossiya Segodnia'* conglomerate (*Russia Today)*, intended to water down the informative work of the Russian state media with a new assignment: drafting useful fiction. Kiselyov greeted his newly formed team with the following words: 'Objectivity is a myth' and set the foundation stone of the new editorial line: '*Love for Russia*.'

The following year Kiselyov defined his work in military terms: 'It is clear that Russia wants to be a competitive player in the international media arena because nowadays information wars have become a customary and predominant practice. In the case of Syria, for example, the Americans lost the information war. In the case of Crimea they did too. In the past, massive artillery attacks were launched prior to the combat itself. Now, we are talking of media attacks'[24].

[21] David Alandate "Fake News: la nueva arma de destrucción masiva" Op. Cit

[22] Ibid.

[23] Timothy Snyder "El camino hacia la no libertad" Op. Cit

[24] Kiselyov, D. 2014. Дмитрий Киселёв представил международный проект "Спутник". YouTube. Available in: https://www.youtube.com/watch?v=WR6qEi8I-IE

According to David Alandete information warfare was —for Kiselyov— the most important type of war. On the other side of the coin, the president of the Democratic Party wrote that there was 'a war, no doubt, but this war is fought in another type of battlefield'. The term should be taken literally[25].

Carl von Clausewitz defined war as '*an act of force to compel our enemy to do our will'.* What if —as suggested by the Russian military doctrine of the 2010s— technology allows us to seize the will of the enemy without the need for violence? It should be possible, as Valery Gerasimov suggested in 2013, to rally 'the potential for protest of the population'[26] against their own interests or, as the *Izborsk Club* advocated in 2014: to generate a '*paranoid and destructive reflection'* in the United States[27].

The *Izborsk Club* is arguably the most influential intellectual group of Russia and specializes in the study of foreign and domestic policies. Among its main objectives are the making and presentation of analyses aimed at creating a patriotic state policy in all areas of national life. This *think-tank* is responsible, to a larger extent, for the strategies that President Putin is implementing. In December 2014, it published a series of articles about a new *Cold War* directed against the United States: a war of information. He anticipated 'feeding information with disinformation'. The objective was plainly 'the destruction of several of the main pillars of Western society'[28].

The management of information offering alternative realities bears a resemblance to the 'plausible deniability'. The idea of plausible deniability created in the United States in the 1980s, consisted in making statements vague enough to avoid accusations of racism.

After the plausible deniability, the second propaganda strategy more commonly used by certain Russian sources is the proclamation of innocence. During the recent invasion of Crimea, Russian propaganda presented the events not as a stronger country attacking a

[25] David Alandate (2019). Op. Cit.

[26] Valery Gerasimov "Мир на гранях войны. Мало учитывать сегодняшние вызовы, надо прогнозировать будущие" (La paz al borde de la guerra. No es suficiente tener en cuenta los retos de hoy, es necesario predecir el futuro), VPK, No 38/2017 (702) March, 2017. Available in: http://vpk-news.ru/articles/35591

[27] Timothy Snyder "Russia is Winning the Information War. The Invasion of Ukraine was a Practice Run for the 2016 American Election" Literary Hub (2018). Available in: https://lithub.com/russia-is-winning-the-information-war/

[28] Ibid.

weaker neighbor at a time of extreme vulnerability, but as the legitimate rebellion of an oppressed society against a global conspiracy.

With a more specific viewpoint from inside the Russian armed forces, it was clear that, having apparently used their cybernetic capabilities in Estonia (2007) and Georgia (2008), they still needed to develop the information element since, in spite of its military achievements in the war, Russia had lost the information and propaganda aspects of these operations given the subsequent international uproar. Consequently, the Chief of Staff General Valeri Gerasimov, described the information operations as crucial.

In an article published in February 2013, General Gerasimov called for the adaptation of military strategies to the digital environment. His reasoning was based on the importance that social networks had had in the ensuing success of the so-called *Arab Spring* and the revolutions against regimes aligned with Moscow in Eastern Europe[29].

In that article Gerasimov wrote: 'The rules of war have changed. The role of non-military elements to achieve political and strategic goals has increased and, in many cases, has proven to be much more effective than the use of actual weapons'.

The General warned of the need to weaken the enemy by feeding 'the internal opposition and opening up a permanent frontline in the whole territory of the enemy State'. On these measures, Gerasimov continued saying that 'the new information spaces open asymmetric possibilities to reduce the enemy's fighting potential. In North Africa we have already seen the use of these technologies to influence the different State structures and the population, with the help of information networks'.

Although modest in military terms, the Russian military operation in southern and southeastern Ukraine included the most advanced propaganda campaign so far in the history of warfare. Propaganda acted on two levels: first, as a direct attack on the objective facts by denying the obvious, even war itself; secondly, as an unconditional proclamation of innocence underlining that Russia could not be responsible for any wrongdoing. There was no war but, if there was one, it was totally justified.

[29] Valery Gerasimov "Мир на гранях войны. Мало учитывать сегодняшние вызовы, надо прогнозировать будущие" Op. Cit.

In this way, one of the most important elements of the Russian operation in Ukraine in 2014 was the information warfare, designed to undermine the truth and insist on innocence. These operations were transferred to the United States and the European Union with more complexity and more impressive results, causing the information warfare against Russia to be lost because the West did not fully understand what was happening.

This evolution of Russian military doctrine has become increasingly clear. Thus, as of 2016, senior Russian officials have mentioned the propaganda warfare as part of their military strategy. On February 21st 2017 the Minister of Defense, Sergei Shoigu, appeared before the State *Duma* (Lower House of Parliament) to detail a series of measures that involved a considerable increase in military spending. The minister admitted for the first time the creation of a Division in charge of undertaking informative actions. According to Shoigu, 'propaganda must be smart, shrewd and efficient'[30].

On the other hand, the retired General Vladimir Shamanov, who chaired the Defense Committee in the *Duma*, also admitted in that session the existence of that newly established Division, just mentioning its objectives: '*protect the interests of national defense and undertake information warfare operations'*, including cyber-attacks[31].

In addition, the *RIA Novosti* news agency quoted retired Colonel Leonid Ivashov, who had been in charge of the Department of International Cooperation of the Ministry of Defense: 'We must stop offering excuses and force the West to put itself on the defensive with operations intended to surface their lies'[32].

Counter-disinformation strategy

In March 2018, the European Security Commissioner, Julian King, asked Mariya Gabriel, Commissioner of Economy and Digital Society, to put forward a series of mandatory measures to confront the serious threat to democracy posed by disinformation. In that request, King stated that it was becoming increasingly clear that the threat of

[30] Agencia "Ministro de Defensa ruso ataca las revoluciones de color y a la OTAN" La RouchePac (2017). Available in: https://spanish.larouchepac.com/es/20170224

[31] Agencia "Las tropas informativas, al servicio de la Defensa de Rusia" Sputnik (2017). Available in: https://mundo.sputniknews.com/defensa/201702231067162979-rusia-tropas-informativas/

[32] Ibid.

cybersecurity was changing its goals from a systems-centered approach, to one that used cybernetic methods to manipulate behaviors, deepening social divisions, subverting our democratic systems and questioning our institutions.

Commissioner Gabriel ignored the request, but an accurate description of the problem was included in a public communiqué. She defined disinformation as 'verifiably false or misleading information that is created, presented and disseminated to profit from or deliberately deceive the population causing public mischief. Public mischief includes threats against democratic political and policy making processes, as well as against public goods or the security of European Union citizens'[33].

It is clear that to face this 'trend' it is essential to understand the environment in which we find ourselves. Freely quoting the Spanish philosopher and essayist Ortega y Gasset, we could say that *we are our circumstances and us*. As has already been said, we cannot ignore that these operations are used to create confusion and aggravate existing problems.

Therefore, we cannot think of 'empty spaces' placing ideas away from reality, influenced only by the circumstances fancied by our reasoning or preferences. The degree to which an event, idea, or question affects us, is therefore conditioned not so much by what really happens, but by the way in which we interpret that event.

Context is of the essence to counteract disinformation campaigns. We must then learn to recognize it, to observe beyond what we do and expand the viewpoint further away. To make decisions as accurate as possible it is necessary to analyze the contexts, especially one's own.

Victoria Clarke, a communications expert from the United States who held several posts in the private sector and in three Republican Presidential administrations, notably as Assistant Secretary of Defense for Public Affairs with Donald Rumsfeld, published a document entitled '*Against Disinformation'* in which she asked herself: 'How can we do a better job against disinformation in general terms, and against terrorism in particular?' Faced with this dilemma, Victoria Clarke's main strategy was to build credibility through the validation of third parties[34].

[33] European Commission (2018). Op. Cit.

[34] Alfonso Bauluz "Prensa y manipulación. El Pentágono y las Operaciones de Información" Editorial

At home, the National Cryptologic Center (CCN in its Spanish initials) published in February 2019, an interesting guide entitled '*Disinformation in Cyberspace*'[35] in which a part of the problem was addressed; namely the cyberattacks intended to erode public opinion in a given State which —if successful— could cause damages not limited to economic or material losses, but to the nature and raison d'être of liberal and democratic governments.

In that guide, the National Cryptologic Center points to a fivefold challenge to counteract and stop disinformation campaigns:

1. To detect and stop illegitimate influence attempts on specific issues of social and political polarization.
2. To analyze these illegitimate attempts and differentiate them from processes of political and social influence carried out by legitimate actors.
3. To adequately put into context the attributions of the actors' intentions and abilities with disinformation goals in order to define the small or large dimension of those actors in the global network of mass communication which is already taking place in any democratic process.
4. To arrange information campaigns about disinformation, its intentions and scope. Underline the fact that the attempts of some actors are intended to fool public opinion saying they can exert 'total manipulation', when they have neither the resources nor such ambitious intentions in most cases.
5. To introduce good practices in academic circles or through the press, describing attempts at disinformation campaigns in social networks, so as to adequately assess the scope that these campaigns and how they share space with legitimate information which, by and large, is the one that reaches the people in terms of both, quantity and quality.

Fragua. Madrid (2018)

[35] Centro Criptológico Nacional "Desinformación en el espacio" CCN-CERT BP/13. Madrid (2019). Available in: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3552-ccn-cert-bp-13-desinformacion-en-el-ciberespacio-1/file.html

These endeavors, in our opinion, go beyond the mere defense of the cyberspace and require ample solutions by any government, with collaborative support from the highest authorities of the National Security System and not only from some of its departments.

Conclusions

The way in which some actors use information warfare has caused considerable alarm in the International Community. The way to exercise national power and achieve strategic objectives seems to have bypassed conventional military procedures, undermining the traditional concept of military deterrence.

Reactions to Russia's intervention in Ukraine, or to the alleged actions in the United States and the United Kingdom in 2016 were slow, hardly effective and based on obsolete criteria. In general terms, no one has clearly assessed the sophistication, intensity, scope and impact of the Russian information warfare campaign.

The Greek historian and general Thucydides wrote in his '*Peloponnesian Wars'* after the Athenians had been defeated in battle, that Nicias encouraged them with these reasoning: '*men are the city and not the walls, let alone the ships without names'*[36]. In that same work Thucydides reminded us that Sparta had no walls because it had its citizens.

In an interview with *El País,* the famous world chess champion Garry Kasparov provided one of the most important hints to tackle the trend of disinformation campaigns: the formation of critical and well-informed societies. It is a process that inevitably implies investing more in education[37].

Most researchers on the topic of disinformation in modern societies agree that the best tool to fight against it is to strengthen the education and critical thinking of the people. Diego Rubio concludes that ignorance and oblivion are the compost where lies in politics grow.[38] Hence, education is called upon to play a key role in facing the post-truth era.

[36] Tucídides "Las guerras del Peloponeso" Ediciones Orbis S.A. Barcelona (1986)

[37] Ben Gordon y Azahara Mígel "Garry Kasparov explains how fake news work". El País (2019) Available in: https://elfuturoesapasionante.elpais.com/garry-kasparov-explica-como-funcionan-las-fake-news/

[38] Diego Rubio (2017). Op. Cit.

Nowadays, however, a humanist education that helps identify lies, is not always accessible to the vast majority of people. José Carlos Ruiz, in his book '*The Art of Thinking*', affirms that reflection has been replaced by the dictatorship of action and urges to revive critical thoughts. He continued adding that learning to think is the same as to trigger correctly two mechanisms that work quite well together when analyzing an issue or making a decision: reason and feeling.[39]

The endeavor will have to be lasting in time, since changing perceptions, attitudes and, ultimately, behavior is the effort of a generation. Only then the battlefield of information can be leveled to subsequently win the battle of ideas.

But history teaches us that Sparta needed its walls. If information harassment or disinformation turns information into a new weapon, that is to say into an instrument used to attack or defend, and if such disinformation is intrinsically intentional, we could be facing activities that may pose a real threat to national security, putting at risk goods and rights that should be legally protected.

Perhaps the time has come to open a serene and calm debate to assess the need to provide a legal framework for the issue of disinformation, as it has become one of the problems that generates more uncertainty. To do this, it is necessary to judge whether legally protected assets are being jeopardized and, if necessary, set limits to prevent States from falling into the hands of powerful tycoons, ruthless terrorists or other criminal groups.

At national level, the Director of the National Intelligence Center said some time ago before the Joint Congress-Senate Committee of National Security, that Spain was ready to counter any cyber-attack during the election process, although we were never exempt from fake news or any other type of harmful external influence. In that same appearance he explained that in a short period of time the National Cybersecurity Operations Center would be fully operational[40].

[39] José Carlos Ruiz "El arte de pensar. Como los grandes filósofos pueden estimular nuestro pensamiento crítico" Editorial Almuzara. Córdoba (2018)

[40] Diario de Sesiones de las Cortes Generales (*Official Journal*). Joint Congress-Senate Committee of National Security held on February 14 2019. Available in: http://www.congreso.es/public_oficiales/L12/CORT/DS/CM/DSCG-12-CM-131.PDF

The creation of this center, as part of the National Security System, probably responds to the recommendations issued by the European Union to fight disinformation. However, addressing disinformation operations from a cybersecurity perspective could prove to be a limited response.

A report published by the ‘*Rand Corporation’* recommends adopting holistic, comprehensive and interconnected responses and avoiding fragmentary and incomplete efforts. According to this report, most of the solutions provided by the States are developed in an uncoordinated way, and in some cases even without any kind of connection between the different organizations concerned. These solutions will never be really effective when it comes to tackling this trend.[41]

Contrary to what one might think, we are not confronted by an insuperable situation. Both Germany and France have dealt with these information operations with effective responses based on a precise understanding of the environment and the threat. For these countries, it is an essential condition to flee from partial solutions that, by definition, will be slow or ineffective responses based on models from bygone times.

*Samuel Morales****
Lt-Col Marine Corps (Joint Staff Course)

[41] Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin y Elina Treyger “Countering Russian Social Media Influence” Santa Monica, CA: RAND Corporation (2018). Available in: https://www.rand.org/pubs/research_reports/RR2740.html