ARI 92/2017
20 November 2017

The 'combination': an instrument in Russia's information war in Catalonia

Mira Milosevich-Juaristi | Senior Analyst at the Elcano Royal Institute and Associate Professor of the History of International Relations at the Instituto de Empresa (IE University) | @MiraMilosevich1

Theme

The 'combination' (*kombinaciya*) is an operation which integrates diverse instruments (cyber warfare, cyber-intelligence, disinformation, propaganda and collaboration with players hostile to the values of liberal democracy) in Russia's information war in Catalonia during and in the wake of its illegal referendum.

Summary

The principal objective of this paper (which serves to complement a previous work on 'disinformation')[1] is to: (1) analyse the facts of Russian interference in the illegal referendum in Catalonia, along with the motives and objectives which guided the actions of the current Russian regime; (2) show how Russian interference in Catalonia forms part of an information war, an asymmetric military method which Russia employs in the US and Europe; and (3) evaluate the response of the West (the US, the EU and NATO) and determine whether or not it has been up to the challenge of Russia's information war.

While Westerners tend to conflate 'disinformation' with 'information war' –while distinguishing between 'cyber warfare' and 'strategic communication'– the Kremlin uses 'disinformation' as one of the instruments of the 'combination', demonstrating in practice that 'cyber warfare' and 'information war' –while seemingly synonymous– are interdependent phenomena.

"Russian military doctrine defines as one of its principal objectives not to destroy the enemy but rather to influence him"

Russian military doctrine defines as one of its principal objectives not to destroy the enemy but rather to influence him –pursuing not the extinction of opponents but instead their internal decline–. This shifts warfare from the conventional battlefield to the sphere of information, and into the terrain of psychological warfare and the distortion of perceptions. Therefore, it is clear that war with Russia is not fundamentally a physical conflict but rather one between consciousnesses. In the final analysis, the objective is always the same: win the war in the hearts and minds of the enemy.

[1] See Mila Milosovic Juaristi (2017), 'El poder de la influencia rusa: la desinformación', ARI, nr 7/2017, Elcano Royal Institute, http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari7-2017-milosevichjuaristi-poder-influencia-rusa-desinformacion.

Analysis

Russia’s victory in Catalonia

In light of previous examples of Russian interference –in the Brexit referendum, in the Dutch referendum on the EU-Ukraine Association Agreement, in the US presidential elections and in the German and the French elections, not to mention the cyberattacks and disinformation campaigns undertaken by Russia against its neighbours– the 2,000% increase in Russian digital activity related to Catalonia registered during the month of September has been no surprise, and neither is it an anomaly. Rather, it reflects what has been one more Russian attempt (and probably not the last) to influence the internal political situation of another country, to sow confusion and to proclaim the decline of liberal democracy.

Various high-level Russian representatives –including Yuri Korchagin, the Ambassador of the Russian Federation in Spain, Serguei Lavrov, the Minister for Foreign Affairs, and President Vladimir Putin, among others– have officially expressed their ‘total support for the territorial integrity of Spain’. They claim that Russia has no interest in meddling in what is an ‘internal process’. Nevertheless, after conducting detailed analyses of pro-Russian websites and social network profiles (using, as in the case of *El Pais*, digital analytics), many Spanish and international news media have reported (along with many Russian communications media, including RT, the old Russia Today, Sputnik, Russia Beyond the Headlines and many state TV stations) that the Russian government has been applying the ‘combination’ of various instruments of information warfare. To this end, it has collaborated with players hostile to the West –Julian Assange, Edward Snowden and radical groups in the UK and the US supporting Brexit and Donald Trump– to intervene in the illegal referendum in Catalonia.

The contrast between the opinions of Russian diplomats and the attitudes of the Russian media should be no surprise. What George Kennan insisted on during the Cold War –that is, that one should not confuse Soviet foreign policy with Soviet external relations– is also still valid for Russia today. The external relations of Russia are –despite its violation of international law with the annexation of the Crimea– embedded within the institutional framework of the international community. Russian foreign policy is another matter altogether. The Russian foreign-policy objective is to revive Russia’s great-power status through the expansion of its zones of influence and by placing itself in competition with the US and the EU in different international scenarios. During the last three years, Russia has shown that it is capable of carrying out –and that it has the political will to do so– both military operations and information warfare at the same time. In the Ukrainian and Syrian wars, the Kremlin has combined the use of military force with the techniques of information warfare. In Western countries, where Russia’s principal objective is to gain influence, as opposed to territory, the conflict has taken the form of hybrid warfare with a special focus on the information war.

Russian activity related to the illegal referendum in Catalonia has concentrated on the transmission of both true and false messages via social networks (Facebook and Twitter) by trolls (online profiles created to disseminate pre-fabricated information), bots (dissemination of information by autonomic processes) and sockpuppets (online profiles

created with the objective of generating and transmitting false, or ‘fake’, news). It has also involved intense coverage of events in Catalonia by Russia media.

As on previous occasions, the successful combination of different instruments of information warfare has required the support of the Government of the autocratic regime, in addition to the close collaboration between intelligence services (which together define the principal weaknesses and internal problems of a target country), as well as the cyber intelligentsia: the ‘web brigade’ of all the hackers, trolls, bots and sockpuppets who steal digital information and then divulge it to the media. The pirated information on different social groups shapes the definition of potential targets –possible receptors of particular messages– in the social networks.

The most significant content of the messages

The most significant information divulged by Twitter and Facebook came from Julian Assange and Edward Snowden. They defined Spain as a ‘banana republic’, arguing that Spain was on the verge of a civil war and insisting that Spain had used violent police force to block the democratic right to vote. This was retweeted and shared on Facebook by trolls and bots.

The Russian media publishing in English and Spanish –*Sputnik* and RT– and the Russian state television channels[2] (the only source of information for most Russians) offered an ‘alternative point of view’ on the events, highlighting the supposed weaknesses of a Spain in crisis. The most significant content of these messages can be summarised as follows:

- The use of force by the police consisted of deliberate violence that was not employed in the legitimate defence of the security of the State, but rather as a Francoist practice unworthy of a democratic State.
- The EU would recognise the independence of Catalonia after a process of accession.
- The EU had ordered Spain to undertake “repressive action” to stop the referendum, in an attempt to avoid another *Brexit*.
- The referendum is another ‘colour revolution’, but this time within the EU, representing the first phase of the EU’s own disintegration.
- Europeans are ‘hypocrites’ to condemn the use of force in the Ukraine by Victor Yanukovich but not that used by the Spanish police in Catalonia.

[2] To analyse the messages about the illegal Catalan referendum broadcast on Russian TV channels I have used the outstanding analysis of the portal EU vs DisinfoRussian, ‘TV’s view on Catalonia referendum: Europe falling apart and Spain compared to Ukraine’, https://euvsdisinfo.eu/russian-tvs-view-on-catalonia-referendum-europe-falling-apart-and-spain-compared-to-ukraine/.

- Spain is in the same situation as the Ukraine, and Catalonia is on the verge of a civil war like that in Donbas.

- The referendum in Catalonia is like the referendum in the Crimea.

- The West is responsible for the Catalan desire to become independent of Spain: it created the prior conditions for the separatists when it supported and recognised the independence of Kosovo.

The objectives and motives of the ‘combination’ in the illegal referendum in Catalonia

The fundamental objectives of employing the ‘combination’ is the same as that of disinformation: to deceive and disorient an opponent, to influence his decisions and to undermine his political, economic and military efficacy. The difference between disinformation and the ‘combination’ lies in the fact that the ‘combination’ uses a larger number of instruments (including disinformation). The principal objectives of the ‘combination’ in Catalonia are:

1. To discredit Spanish democracy, foment division among Spanish citizens and create a divide between Spain and its EU and NATO partners.

2. To discredit European institutions, pointing to their inefficacy and to the failure of the European project, and to sow confusion.

3. To discredit the liberal order created and maintained by the US.

4. To distract the attention of Russian citizens away from internal problems (including the separatism of the North Caucasus region) and to insulate them from information from foreign communications media.

The strategic motives of the Kremlin which underlie these practices are the following:

1. To achieve the lifting of the economic sanctions imposed on Moscow for the annexation of the Crimea and the economic and military support provided to the pro-Russian rebels in south-eastern Ukraine, deepening internal division within the EU.

2. To present liberal democracy as a failed model, lacking any credibility to offer moral lessons to Moscow, and not one desirable for Russia, as it only creates chaos and disorder.

3. To foment ‘anti-Westernism’, one of the supporting pillars of the Russian regime, which maintains a deeply-rooted attitude of resentment and grievance towards the West. Russia is not only a very proud country but also a resentful and alienated one. A large part of this alienation is based on a fundamental difference in the Russian and Western points of view on Europe, the US and NATO.

The information war: origin and development

To obtain military, social, political and economic advantages through cyber intelligence and cyberattacks is part of a strategy that is not exclusive to the Kremlin (as the well-

known cases of China, North Korea and the radical US groups supported the Trump candidacy amply demonstrate). Not even presenting fake news as real and authentic is an exclusively Russian practice. Respected media such as *The New York Times*, the BBC and *The Guardian* (to mention only a few) have published, intentionally or not, articles on Catalonia with much erroneous information. Nevertheless, what distinguishes Russia from other ‘cyber actors’ and disseminators of lies is the use of information warfare as a military strategy defined by and integrated into the most recent Military Doctrine of the Russian Federation, official since 2014.

As a concept, information warfare has its roots in pre-revolutionary Russia and the Bolshevik tradition, and its evolution has been shaped by: (1) the Kremlin’s mimicry of what it considers the US attitude with respect to Russian behaviour in the ‘colour revolutions’ (as interferences in the internal affairs of other countries with any eye to changing their regimes); (2) the observation of the workings of social networks during the Arab Spring; (3) by the trial and error pattern of the Kremlin’s behaviour in the Chechen War of 1999, the Georgian War of 2008, the mass protests against Putin’s government for fraud in the legislative elections of 2011, the annexation of the Crimea and the war in the Ukraine (2014); and, finally, (4) the extraordinary capacity of the Russian intelligence services to adapt to the principles of subversion relevant in the age of the Internet. The fact that since 2014 information warfare has formed part of the Military Doctrine reveals that the Kremlin considers Russia to be involved in a large-scale information war.

The perfecting of the current information war began with the second Chechen War (1999-2009), when the Federal Secret Service (FSB) concluded (based on information that citizens had disseminated about the war on social networks) that the Internet was a dangerous destabilising factor and a threat to national security that should be carefully controlled. Among the conflict scenarios where the Russian intelligence services identified and studied the ‘threats’ to national security represented by the Internet –and its infinite possibilities as an instrument of information warfare–, the 2011 protests marked a significant advance in the use of social networks. During the protests, the Kremlin realised that the automatic systems for disseminating information (that they had used since 2009, or before) were insufficient by themselves; rather, they also required an investment in human players with the object of anticipating debates online. Since then, Russian investment has centred on three main areas: communications media that operate both abroad and inside the country, such as RT and *Sputnik*; and the use of social networks to ensure that Russian narratives reach a broad audience in both Russian and foreign languages.

The annexation of the Crimea in 2014 –which did not require the ‘little green men’ to fire a single shot– has been the biggest success of the ‘combination’ of the various instruments of information warfare and the immediate reason why it was integrated into the Military Doctrine of 2014. The chapter devoted to ‘military dangers’ included for the first time ‘the information space and the internal sphere’. Particular emphasis was placed on ‘foreign information influence on the population... aimed at undermining the spiritual and patriotic traditions’, and on ‘the use of communications technologies against the sovereignty, political independence and territorial integrity of some States, which endangers international security and peace’. One of the prime refrains of Russian

doctrine is the importance of state policy in containing the influence of foreign actors in domestic Russian affairs and in the sphere of the so-called ‘zones of vital interest’. The Military Doctrine suggests that the Russian perception of the current information war is purely defensive (although it is obvious that it has been offensive, as much in the former Soviet republics as it has been in Western countries) and that it merely gives back to Westerners some of what is considered to be ‘their own medicine’.

The Western response

Russian interference during the Brexit campaign and in the US presidential elections is already under investigation. The US Senate Select Committee on Intelligence questioned representatives from Facebook, Google and Twitter about Russian interference in the US and Catalonia. Needless to say, the Spanish government should do the same. A substantial body of research on the Russian troll campaigns has already been accumulating in various Western countries for some time now. During its recent legislative elections, Germany took a series of precautions to prevent Russian interference; its Army now has a ‘cyber-brigade’ charged with countering cyber-threats. Various European and US institutions, think tanks, non-governmental organisations, journalists and analysts have created teams to combat fake news. Their job is to detect when Russian interference takes place, to describe its characteristics, define the false information and then take measures to counter it. Although those involved in the ‘Russian plot’ must be brought to justice and their information denounced as false, this is not enough. Westerners do not understand the full significance of the Russian concept of information warfare. Above all, they resist accepting that Russia is no longer a ‘strategic partner’ –or even an adversary with whom one might differ and then reach agreements– but rather an enemy, in the sense that it desires the West’s submission or destruction.

Although Westerners tend to conflate ‘disinformation’ with ‘information warfare’ –even as they distinguish between ‘cyber warfare’ and ‘strategic communication’–, the Kremlin uses ‘disinformation’ as one of the instruments of the ‘combination’ and shows in practice that ‘cyber warfare’ and ‘information warfare’ while seemingly synonymous are actually are interdependent phenomena.

The West has concentrated on cyber-protection and on the technical responses to cyber threats. The NATO countries are well prepared for a ‘pure cyberwar’. Nevertheless, so far their response to the Russian information war has not been adequate for three major reasons: (1) because they have believed that Russia discredits itself by spreading false news; (2) because they do not understand that the West is at war with Russia; and (3) because they suppose that telling the truth is sufficient, which it is not.

Russia has failed according to Western criteria –it does not tell the truth– but according to its own criteria it has achieved an overwhelming success, particularly in two areas. Within Russia, the mission to engage the information war commissioned by the Military Doctrine has secured the national information space: Russians have been isolated from foreign information sources and most of the domestic media are controlled by the Kremlin. Abroad, Russia is exerting its influence over the consciousness of the masses, generating an atmosphere in which it is difficult to distinguish authentic information from half-truths and fake news.

Conclusion

The consciousness of the Western population is the key terrain of the confrontation with Russia. It is therefore insufficient to simply counter false information. Ignorance of the fact that Russian disinformation campaigns are paving the way for future action against the interests of the West is the principal danger of the ‘combination’ strategy.

It is impossible for the West to respond with total success to the ‘combination’ of instruments and tactics now employed by Moscow. While the intelligence agencies can engage in intelligence work, Western governments cannot effectively restrict information flows. They cannot restrict the use of the Internet as do the governments of authoritarian or totalitarian countries.

Russian Military Doctrine defines as one of its principal objects not to the destroy the enemy, but rather to exert influence, that is, not the extinction of opponents, but rather their internal decline. Therefore, warfare moves from conventional battlefields to the realm of information, psychological warfare and the distortion of perceptions. War with Russia is not fundamentally a physical conflict but rather one between consciousnesses. This is because, in the final analysis, the objective is always the same: win the war in the enemy’s hearts and minds.