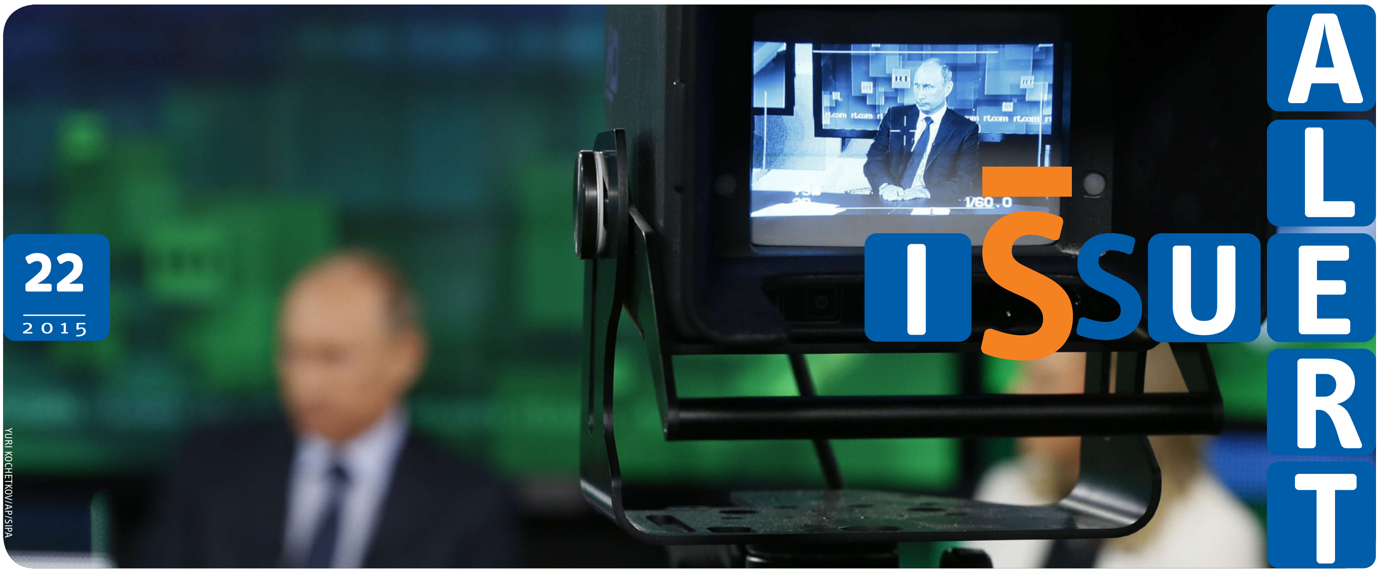
YURI KOCHETKOV/AP/SIPA

22
2015
ISSUE ALERT

Russia’s info-war: theory and practice

by Cameron Johnston

The fabrications and distortions propagated by the Kremlin during the Ukraine crisis have made the concept of ‘information warfare’ common currency. Less widely appreciated is the Russian leadership’s understanding of the term and the vision of the world upon which it rests.

Putin and Hobbes

Russian military theorists often argue that the international arena, like Thomas Hobbes’ state of nature, is defined by ‘a war of all against all’. Without an all-powerful sovereign capable of imposing order, they believe, states have licence to subvert one another’s information spaces. The aim? To stymie their opponents’ decision-making processes and stir unrest in their societies. The means states employ range from disinformation and info-blockades, to leaks and ‘information deterrence’. Since these military theorists perceive Russia to be the target of such aggression, it follows that it must act first lest the country fall further and further behind.

Extreme as this theory might sound, it goes a long way towards explaining Russia’s tactics during the Ukraine crisis. For whereas dystopian thinking is characteristic of military theorists the world over, in Russia it drives foreign policy. ‘Information warfare needs to be continuously conducted in peacetime [as well as] in wartime…’, advises retired Major General Charis Saifetdinov of the Russian Academy of Military Science. If that is so, the EU and its allies must be prepared to resist aggression long after the guns fall silent in the Donbas.

Whereas liberals see globalisation as a good thing, because it promotes the free exchange of people, goods and information, Russian military theorists view it as a threat. The flow of information across national borders and the growth of the digital world make people ever more susceptible, they fear, to outside influence and manipulation. Information warfare, according to the Chief of the General Staff Valery Gerasimov, can help to turn ‘a relatively flourishing state, in just months or even days, [into] an arena for vicious armed conflict’, bringing ‘chaos, humanitarian catastrophe and civil war’ in its wake. Gerasimov was describing alleged US involvement in the Arab Spring, but his words may also serve as a guide to Russia’s aims in Ukraine.

In a report written in 2003, Andrei Manoilo, now a professor at Moscow State University and a member of the Russian National Security Council, outlined the defining features of information warfare. First, it blurs the line between war and peace by allowing an aggressor to launch an attack without ever declaring war. In the case of Ukraine, Russia had slandered the Maidan protesters and predicted that the country would break apart long before its special forces appeared in Crimea.

Second, an aggressor can destabilise a foreign state by setting off ‘lots of local information-psychological conflicts’, which spread chaos in the information space of the adversary and 'divert society's main forces towards a disadvantageous object, [creating] good conditions for the imposition of external… control'. During the Ukraine crisis, Russian state media tried to divert international attention towards the supposed fascism of the Maidan protesters, thereby masking the Kremlin's own intentions. This calumny resonated in many quarters and often resurfaces in Western debates about Ukraine. As late as February 2015, for instance, *The Huffington Post* deemed it necessary to run a story entitled 'Is Ukraine Fascist?'.

Third, the aggressor can impose an 'information blockade' on its target by isolating it from international media. In Crimea, armed men seized television transmission stations, cut off the peninsula's access to most Ukrainian channels and started broadcasting Russian TV. In eastern Ukraine, the rebels were equally decisive. They seized control of the Donetsk TV tower on 28 April 2014, and stopped the transmission of all Ukrainian channels. Once it has a captive audience, the Kremlin can sell its own narrative more easily: a separatist from the Donetsk People's Republic (DNR), interviewed by the BBC on 3 April 2015, was adamant, for example, that American tanks had been deployed in Ukraine. It has to be acknowledged that Ukraine has itself resorted to similar tactics in denying accreditation to some 200 Russian media outlets.

Lastly, one of the tell-tale signs that a country has been subject to an information attack, Manoilo says, is the emergence of 'quasi-independent subjects of geopolitical competition capable of independently [launching] their own initiatives in the international arena'. Although the Donetsk and Lugansk People's Republics are far from being autonomous actors internationally, they are *de facto* no longer under the control of the government in Kiev and are most certainly objects of geopolitical competition.

A comprehensive approach

Information warfare, however, is not simply an umbrella term for a wide array of disparate techniques, used at various times for different ends. On the contrary, it works best when different tools are used in concert over a short period of time to achieve a limited number of goals. This unified approach was most evident in early February 2014, when the outcome of the Maidan protests was still uncertain, and in March, when the position of many countries was still ambiguous.

It was at this critical time that leaks of secretly recorded conversations appeared to cast doubt on the West's interpretation of events. Whether it was the phone call between Assistant Secretary of State Victoria Nuland and the US ambassador to Ukraine, Geoffrey Pyatt, released on 7 February 2015, or the conversation between the Estonian foreign minister and then HR/VP Catherine Ashton, released on 5 March 2014, these leaks were designed to convey the impression that the US was secretly orchestrating events and that the transatlantic allies were divided. Although Russia has always denied any involvement in the leaks, it clearly had the most to gain from them.

Likewise, in March 2014, a video appeared on YouTube purporting to show mercenaries from the US security firm Academi (previously known as Blackwater) operating in eastern Ukraine. The controversy grew quickly. Stories appeared in the Russian and Western press, the Russian and US governments issued claims and counter-claims, and political commentators waded into the debate. Social media, conventional media, government statements and political punditry were all employed to convey the message that the US, not Russia, was a party to the conflict.

At the same time, Russia was issuing threats that amounted to an 'information deterrent'. In the documentary film 'Return to the Motherland', which aired on 15 March 2015, Putin hinted that he had deterred Western countries from intervening over Crimea by threatening a nuclear strike. In combination with the massing of troops, military exercises and provocative aerial manoeuvres, these threats allegedly gave Putin a free hand in the peninsula.

If the EU and its allies are to defend themselves effectively in future, it is vital to understand the importance that the Russian government ascribes to information war and the pessimistic vision of the world in which it is rooted. For Russia at least, information warfare is about employing a wide range of techniques in a concerted attempt to destabilise, and ultimately control, a foreign state.

The US and various EU member states are now launching initiatives to increase Russian speakers' access to reliable information. But if they are to prove equal to their task, they will have to remain in force long after an accommodation with Russia is reached. For in the Hobbesian world of Russia's military theorists, the war never truly ends.

Cameron Johnston is a Junior Analyst at the EUISS.

© EU Institute for Security Studies, 2015. | QN-AL-15-022-2A-N | ISBN 978-92-9198-317-9 | ISSN 2315-1129 | DOI 10.2815/75791