Security Policy Working Paper, No. 1/2015

Russia's Hybrid Warfare: A Success in Propaganda

by Keir Giles

Moscow's media campaign on the war in Ukraine has been surprisingly effective – not only in Russia itself but also in the Western public. This propaganda success is the result of a long term effort which included significant investments and a skilful use of TV and social media. Hardly noticed, Russia has built up a highly developed information warfare arsenal NATO and EU are currently unable to compete with.

The current Russian practice of information warfare combines a number of tried and tested tools of influence with a new embrace of modern technology and capabilities. Some underlying objectives, and some guiding principles, are broadly recognisable as reinvigorated aspects of subversion campaigns from the Cold War era. But their recognition as such, not only by Western societies but also by their leaderships, has been slow.

This is due to two main factors. First, there is a collective lack of institutional memory among target audiences – a significant proportion of which was not even born when Soviet subversion was last a present concern. Second, Russia has invested hugely in enabling factors to adapt the principles of subversion to the internet age. These new Russian investments cover three main areas:

- both internally and externally focused media with a substantial online presence, of which "Russia Today" is the best known but only one example;
- use of social media and online fora as a force multiplier to ensure Russian narratives achieve broad reach and penetration;
- language skills, in order to engage with target audiences on a broad front in their own language.

Examining Russian assessments of current events makes it clear that Russia considers itself to be engaged in full-scale information warfare, involving not only offensive but also defensive operations – whether or not its notional adversaries have actually noticed this is happening. Understanding how this came about, and how Russian capability developed to a stage which has taken its targets entirely by surprise, is more easily understood by looking at three distinct stages of how the current Russian approach evolved.

Each of these stages involved Russia taking action which was unpopular either at home or abroad, and subsequently realising that it could no longer influence the global narrative about that action in the same way as the USSR could – that the old levers and tools for manipulating global opinion were either unavailable or inoperative, and something new needed to be done. In each case, the resulting shock to the Russian system led to a distinctive response which has shaped today's impressive information warfare capability.

1999

In the Second Chechen War, Russia realised with dismay that in information terms, it was outmanoeuvred by a notionally weaker and less capable enemy – since that enemy was more adept at use of the internet to bring its message to a global audience. Despite the fact that the war began with an unprovoked invasion of a Russian republic from Chechnya, in global media Russia found itself incapable of overcoming the adversary narrative of Russian aggression against heroic Chechen freedom fighters.

The Russian response was twofold. On the one hand, the experience served to reinforce the consistent message from Russian security services, led by the FSB, that the internet as a whole was a dangerous destabilising factor and a threat to national security, public access to which should be carefully controlled. At the same time, the security services themselves continued to develop their own means and methods of exploiting the new medium to target adversaries abroad.

2008

The armed conflict in Georgia resulted in a convincing military victory for Russia, but at the same time exposed serious deficiencies in Russian military performance. Dismay at conventional military failings was accompanied by a failure to agree on who had won the information war – but strong consensus that major reform was needed to improve military capability in this field as well as many others. A stark contrast was noted between Mikheil Saakashvili speaking to Western audiences directly in their own languages (while sitting in front of an entirely misplaced EU flag), and Russia's own belated and stilted attempts at organising press conferences led by the monolingual and uninspiring Deputy Chief of the General Staff Anatoliy Nogovitsyn.

The result, among other recommendations for overhauling the Russian Armed Forces, was calls for the creation of Information Troops, a dedicated branch which could manage the information war from within the military. Reflecting the holistic and full-spectrum nature of the Russian information war concept, these would include hackers, journalists, specialists in strategic communications and psychological operations, and crucially, linguists to overcome Russia's now perceived language capability deficit.

In the event, no formed unit known as Information Troops materialised in the Russian order of battle. The notion of the Russian military handling large-scale offensive cyber operations appeared to be publicly squashed by the FSB, and the other capabilities referred to began to develop elsewhere.

2011

Three years later, protest movements both at home and abroad caused a further refining of the approach to information warfare. The Arab Spring demonstrated the power of social media to both mobilise and organise, to the extent of facilitating regime change – a prospect which caused deep alarm at the prospect of this being applied to Russia. Meanwhile at home, the election protests of 2011/12 saw Russian attempts to use automated systems to dominate or suppress online debate, or divert or disrupt social media as a facilitator for organisation. A large array of pre-positioned Twitterbots, and sporadic but highly targeted DDoS attacks, were combined with old-fashioned dirty tricks against opposition leadership figures to attempt to defuse and discredit the protest movement.

Examination of the results appears to have led to the conclusion that automated systems are simply not sufficient, and dominating mass consciousness online requires the engagement of actual humans. This led to intense investment in human capabilities to direct or prevent online debate and comment. This capability, which had previously had only limited targeting and mostly within Russia, was bolstered by the recruitment or training of foreign language speakers (at varying degrees of capability) to exploit the hyper-connected nature of online space. Meanwhile, the recruitment of talent for online media saw journalists tempted from their work with traditional media by offers of doubled or tripled salaries. Thus parts of the original Information Troops concept morphed into the Kremlin Troll Army, in cooperation with state-backed media with a strong internet presence.

Western media organisations were entirely unprepared for a targeted and consistent hostile information campaign organised and resourced at state level. The result was an initial startling success for the Russian approach – exemplified in Crimea, where reports from journalists on the ground identifying Russian troops did not reach mainstream audiences because editors in their newsrooms were baffled by the inexplicable Russian denials.

Months later, Western media outlets were still faithfully reporting Russian disinformation as fact, but the realisation that they had been subjected to a concerted campaign of subversion was beginning to filter through into reporting. One assessment of this change is that Russian information campaigns are failing. By Western criteria, this may be true; to an informed observer, Russian disinformation often appears clumsy, counter-productive, obvious, and easily debunked. But assessing the campaigns by these standards presents a significant risk of misinterpreting their objectives as a result of mirroring – projecting our own assumptions and criteria onto decision-makers in Moscow.

Measured by some Russian objectives, the information campaign has made substantial achievements. This is particularly the case in two key areas – controlling the domestic media environment, and undermining the objectivity of Western media reporting (and hence influencing the information available to policymakers).

1. Russian Domestic Media

To use Russian doctrinal jargon, Russia has succeeded in “securing its national information space”, and “preventing breaches” in it. In other words, the population has been effectively isolated from sources of information other than those which follow the Kremlin line. This isolation is not total and hermetic – it is still possible for interested Russians to access foreign media if they wish. But recent clampdowns on foreign media operations in Russia, combined with the withdrawal of rebroadcasting licences and tighter controls on internet usage within the country, combine to make that process far harder than it was just a year ago. In other words, if you are living in Russia, finding alternative sources of news now takes effort. The result is broad acceptance of the alternative reality provided by Russian state media, and a resultant state of collective delusion among ordinary Russians.

The exception that proves the rule is the internet, including social media. As has been demonstrated repeatedly throughout the seizure of Crimea and operations in eastern Ukraine, the ability of journalists and ordinary citizens - as well as Russian servicemen themselves – to reach directly a wide audience with information which undermines or contradicts the official Russian line poses the single greatest challenge to Russian information campaigns. The result is a range of recent suppressive measures targeting social media within Russia itself, and attempting to control this last unregulated subset of Russia’s “national information space”.

2. Russian External Media

Alternative realities have also been presented to audiences outside Russia, where liberal societies and free media provide weaknesses ready for exploitation by a coordinated information warfare onslaught. Western societies put faith in their own independent media to arrive at and report the truth thanks to their relative freedom of action. But Western liberal media training proved initially to be no match for the unity of message emanating from Russia. In fact, the opposite was true: the emphasis on balance in many Western media ensured that Russian narratives, no matter how patently fraudulent, were repeated to European and American audiences by their own media. When presented with a consistent version of events being repeated by all levels of the Russian media machine from the President to the lowliest foot soldier in the Kremlin troll army, Western news editors had little choice but to report it – hence lending that version weight and authority.

Here, too, the internet and social media played their own distinctive role. The Kremlin troll army interacting directly with readerships in a range of fora including online discussion boards, Twitter and more, acted as a force multiplier for driving home the Russian message – especially by diverting or suppressing any debate which pointed out the inconsistencies or implausibilities of the Russian version of events.

The resulting scale, intensity, volume and consistency of the Russian arguments online exacerbates the Western media problem of favouring balance over objectivity, and can result in reporting being further skewed by taking into account the entirely false, but ubiquitous, Russian alternate narrative.

Both of these aspects of the Russian disinformation campaign illustrate a key reason why its success or failure should not be judged by criteria set other than in Moscow. The assessment that Russia is failing in its objectives often rests on the implausibility of Russian narratives, and the consequent assumption that they will be rejected by their audience. But while truth is a fundamental requirement of Western communications strategies, Russian campaigns need not even remotely resemble the truth to be successful.

Domestically, there is no challenge to the Kremlin narrative now that independent media have been effectively removed from the marketplace; and so, Russians who do not deliberately seek out alternative sources of information are tending to accept what they are being told about their own country and the outside world. Abroad, the Russian alternative reality need not be plausible in order to provide alternatives to the truth, since saturation coverage by Russian external media, the strictures of balance, and the efforts of the Kremlin troll army will ensure that it achieves penetration among its target audience regardless of credibility. Simply by causing confusion and doubt, these alternatives to the truth serve the purpose of undermining trust in objective reporting, and especially in official statements by Russia's adversaries and victims.

A key example of this approach followed the shooting down of the Malaysia Airlines Flight MH17. Four days after the crash, by which time it was already clear that Russia held ultimate responsibility for the tragedy, the Russian Ministry of Defence held a press conference to present explanations absolving Russia. The scenarios presented were diverse and mutually contradictory, and did not stand up to the briefest examination by experts with even basic knowledge of the aircraft and missile systems claimed to be involved.

But this was not a Russian concern: their instant rejection by both foreign and Russian experts did not prevent them being reported in the West as well as receiving broad coverage within Russia. In the same fashion, almost four months later when Russia issued crudely doctored satellite images suggesting the Malaysian airliner had been downed by a missile attack from a Ukrainian aircraft, these were instantly detected as fake – but this did not prevent the claims being reported, initially without qualification, by a range of Western media. Russian disinformation thus continues to reach its targets, sowing confusion and doubt abroad and obscuring the truth with a thicket of falsehoods.

To dismiss the importance of Russian denials because they are implausible is also to underestimate the concept and power of the direct lie. Given the habit of liberal leaders in democratic nations to attempt always to say something which at least resembles the truth, implausible denials are a ploy which Western media are particularly ill-equipped to respond to and report appropriately. Thus when Vladimir Putin denies that Russian troops are in Crimea or in eastern Ukraine, it is not important that what he is saying is plainly untrue - the approach is effective not only in press conferences, especially when unchallenged by a compliant media; but as Canadian Premier Stephen Harper found at the G20 summit in Brisbane, it also makes it impossible to confront or engage with President Putin even when face to face.

It has also been suggested that Russian disinformation campaigns are self-defeating because they lead their creators into a "discourse trap" – constraining their options by forcing them to subscribe to their own narratives and act in line with their own propaganda. But this too risks disregarding the particular features that pertain in Russia, in particular the complete unconcern for truth, reality or even consistency. Within Russia, there is no discourse trap, since the picture of the world provided by Russian media is entirely under Kremlin control and can be adjusted at will to justify any leadership action to the domestic audience. Abroad, foreign audiences are already baffled by the multiplicity of conflicting narratives already available, and which few outside a narrow expert community will be tracking and attempting to expose as false. In this way, while the discourse trap would be a severe constraint for leaderships which were obliged to be even partially truthful or consistent, it fails entirely to close in Moscow.

Danger arises when successful pollution by Russia of the opinion-forming process in the West spills over into influence on the policy-making process itself. Many narratives absolving Russia or placing the blame for the current crisis elsewhere will find willing audiences in those policy circles which would wish to appease Russia and return to business as usual as swiftly as possible, as was the case following the armed conflict in Georgia in 2008. Even more dangerously, in circumstances which would require complete Western consensus – such as a decision on collective action to be taken by NATO-Russian information warfare could play a key role by fatally undermining the essential unity among Western allies.

The threat of Russian information campaigns is thus that they prepare the ground for future Russian action which would be directly counter to the interests of Europe and the West. By either undermining the will or support for deterrent measures, or sowing an entirely false impression that Russia is justified in its actions, Russia adjusts key variables in the security calculus determining the risk inherent in future assertive action against its neighbours. In the case of Ukraine, Russia felt the balance was tipped sufficiently in its favour to act; but Ukraine, and Georgia before it, are unlikely to be the last neighbours of Russia to fall victim to this calculation. Current Russian ambitions, if followed to their conclusion, must necessarily lead to a more direct confrontation with the West. Russia now benefits from a highly developed information warfare arsenal which will be a key facilitator in preparing for further actions which the West will find unthinkable in advance, and unacceptable after the fact.

Keir Giles is Director of the Conflict Studies Research Centre, Oxford. The views expressed in this article are the author's alone.