CREST Centre for Research and Evidence on Security Threats

Russia and Disinformation: Institutions and Actors

FULL REPORT

MARCH 2019

Dr Cerwyn Moore

MARCH 2019

RUSSIA AND DISINFORMATION: INSTITUTIONS AND ACTORS

FULL REPORT

Dr Cerwyn Moore, University of Birmingham

How does Russian state disinformation operate in the Caucasus region? This report considers three different cases of disinformation deployment in the Caucasus region to highlight the dynamics of Russian state influence, both domestically in the Russian Federation's North Caucasus region as well as in Georgia, just across the Russian border in the South Caucasus.

This report is part of a series on disinformation to come out of the Actors and Narratives programme. The other three reports in the *Russia and Disinformation* series: 'The Case of the Caucasus', 'The Case of Ukraine', and 'Maskirovka' can be found at www.crestresearch.ac.uk/tag/russia-disinformation/

About CREST

The Centre for Research and Evidence on Security Threats (CREST) is a national hub for understanding, countering and mitigating security threats. It is an independent centre, commissioned by the Economic and Social Research Council (ESRC) and funded in part by the UK security and intelligence agencies (ESRC Award: ES/N009614/1).
www.crestresearch.ac.uk

E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL

TABLE OF CONTENTS

INTRODUCTION

This CREST report investigates the institutions and actors involved in Russian disinformation. It should be read in conjunction with the CREST Report on Disinformation and Maskirovka, and the two other reports in the series, which examine case studies of Disinformation.

In this Report we outline the contemporary context in which disinformation occurs, as conceived and practised by actors in the Russian Federation. The aim of this report is to investigate in more depth Russia institutions and actors that contribute in various ways in the promotion of Russian disinformation.

In particular, we consider, *inter alia*, the following themes:

- Governmental and affiliated institutions involved in disinformation activities
- The role of state and non-state/sub-state actors and networks in disinformation
- To what extent disinformation can be traced to specific actors or agents of influence

There is a burgeoning Western literature on Russian policy and practice in disinformation but very little of it has detailed and reliable material about the government agencies and affiliated actors that promote it. Many studies refer broadly to 'the Kremlin' or the 'power agencies' as the principal actors in this field, but a wider array of actors and agents can be identified as being involved. At the softer end of the power spectrum, agents of traditional diplomacy and cultural diplomacy, the Russian Orthodox Church, representatives of higher educational institutions, youth movements and intergovernmental foundations are active in the dissemination of Russian 'strategic narratives' and creating what Russian officials refer to as a 'humanitarian product for export'. In terms of disinformation as a set of tools to promote political influence and entrench Russian power, the field is similarly wide, with political/social activists, covert intelligence networks, the traditional media (print/visual/digital) and trolls, bots and purveyors of 'fake news' contributing to it.

This report has been prepared by scholars working at the interface between international relations and area studies with many years of experience in researching Russian foreign and security policy. It draws on extensive scrutiny of open-source material, including from Russian-language primary sources, particularly on the relevant government agencies, as well as Western academic research and policy-related documents prepared by experts in the field.

GOVERNMENTAL INSTITUTIONS

The main agencies forming the core of the Russian intelligence community are as follows:

MINISTRY OF DEFENCE (MOD)

Among its main tasks is organising and carrying out 'information engagement'. According to one source, Soviet information warfare theory was first taught as a separate subject in 1942 at the Military Institute of Foreign Languages, which is now known as the Military Information and Foreign Languages Department of the Military University of the Ministry of Defence of the Russian Federation; it prepares specialists in 'organising foreign information and military communication,' 'information analysis' and the 'monitoring and development of military information.' (Darczewska, 2014: 9-10). The MoD can spread disinformation via announcements, which are then picked up by and expanded on by Kremlin-aligned media outlets. For example, on 25 August 2018, the MoD put out a press release that Syrian rebel groups were about to gas their own people in Idlib, which was going to be filmed by the Syrian Civil Defense (White Helmets) in order to blame Russia or Syria (Nahas, 2018 and Ensor, 2018). By the end of the same day, dozens of Russian embassy accounts on Twitter had tweeted this information, which continued to spread by conspiracy theorists and Syrian president Bashar al-Assad supporters (Ensor, 2018), even as there was no evidence of any actual readiness for a false flag attack.

ARMED FORCES GENERAL STAFF (GENSHTAB)

Within the structure of the MO is the Glavnoe Razvedyvatel'noe Upravlenie (Main Intelligence Directorate, GRU) of General Staff of the Armed Forces (Genshtab), described as the foreign intelligence organ for the MO and the central intelligence organ for the Armed Forces (*www.mil.ru*). The GRU provides strategic, operational, and tactical intelligence for the armed forces and has been described as the 'bridge' intelligence agency between the military and civilian intelligence agencies, ensuring that both the military and intelligence communities are able to carry out their mission with maximum efficiency. The GRU appears to answer only to the Russian Defence Ministry and the presidential administration, delivering intelligence reports to senior civilian and military officials; though the chief of the General Staff does not have operational jurisdiction over the GRU, he does have day-to-day control (Bartles, 2016: 30). The Centre for Military Strategic Studies of the General Staff provides analysis which is crucial to understanding Russian perspectives on information warfare (Franke, 2015). While primarily focused on conventional warfare, the Armed Forces General Staff is becoming increasingly oriented towards fulfilling a supporting role in disinformation campaigns. As Sergey Chekinov, a head of department at the General Staff Academy and head of the General Staff's Centre for Military-Strategic Research wrote in 2013, indirect actions and methods of non-military techniques and measures are needed to countercheck the adversary's actions and exercise informational superiority (Chekinov and Bogdanov, 2013).

FOREIGN INTELLIGENCE SERVICE (SLUZHBA VNESHNEI RAZVEDKI, SVR)

The organisational structure of the SVR comprises operational, analysis and functional subunits, including a bureau for links with the public and media, a foreign counter-intelligence directorate and an economic intelligence directorate. The SVR provides the presidential and governmental structures with intelligence information to support decision-making, including in the military strategic and security spheres, using 'both overt and covert methods and means' in accordance with federal laws and legal-normative acts. The SVR appears to act with diplomatic cover from Russian embassies overseas. It cooperates closely with the security and intelligence services of countries in the Commonwealth of Independent States (*svr.gov.ru*). The SVR regularly engages in active measures and has been alleged to have operated an extensive ring of spies in the United States in the 2000s (BBC, 2010). Out of the three intelligence organisations of Russia (SVR, GRU, and the FSB), the SVR is perhaps the least influential.

THE FEDERAL SECURITY SERVICE (FEDERALNAYA SLUZHBA BEZOPASNOSTI, FSB)

The FSB is responsible for broad counterespionage operations. One source suggests that the FSB Academy has formed a network of research institutions so that not only diplomatic courses but also the curricula at social science departments of universities include subjects such situation analysis, network communication technology and information/network wars; the subject of information warfare 'has been given the status of an academic science' covering a broad range of activities (Darczewska, 2014). The FSB's 16th department is reportedly involved in recruiting hackers to combat cybercrime (Thomas, 2014: 120). The FSB's loyalty to Putin has in large part helped make it the most powerful intelligence agency in Russia, with the organisation spreading its activities to encompass areas traditionally the domain of the GRU and SVR. The FSB helps create plausible deniability in Russian disinformation campaigns by co-opting or coercing 'patriotic' Russians, whether they are cyber criminals, or oligarchs, to act on behalf of the government (Watts, 2018). Furthermore, the FSB is seen to directly control Georgia's breakaway region of South Ossetia, with Russian FSB agents sitting in the government of South Ossetia (Harding, 2010).

Official documents and military theorists state that, as well as the above mentioned agencies, information warfare draws on the resources of various government agencies. The service for the supervision of communications and information technologies Roskomnadzor, the Federal Protection Service, the Ministry of Internal Affairs (MVD) and the Ministry for Foreign Affairs also play a role. Coordination of the work of government bodies is effected through the high-level Security Council, part of the presidential administration, on which the heads of the power agencies have permanent seats (Franke, 2015: 51). Roskomnadzor, Russia's federal authority, responsible for media content, has worked not just to block sites deemed 'extremist' within Russia in an effort to censor content critical of the Kremlin. It has also threatened retaliation against Google if it gives less prominence to Russian state-funded news outlets in its search results (RFE/RL, 2017).

Theoretical and practical developments have resulted in the creation of 'research units' and 'cyber troops' which, in the words of Russian Minister of Defence Sergei Shoigu, 'will be much more efficient than the "counter-propaganda" department of the Soviet period'. A new information doctrine (2016) and strategy for the development of an information society (2017) were introduced in order to strengthen the state's control over the internal information space, identify external priorities and enhance Russia's readiness for 'information warfare'. The introduction of 'cyber squads' and the extension of the Russian National Guard's responsibilities in the area of information and cyber security form part of this strategy (Canadian Security Intelligence Service, 2018). The information troops are said to be the operational force for 'coordinating counterintelligence, electronic warfare, precision strikes on enemy command and control nodes, command posts, intelligence collection assets and radars, as well as computer network operations against enemy command and control systems and the use of deception [maskirovka]' (Franke, 2015: 24).

Recent military exercises involving Russian forces witnessed the explicit use of 'psychological warfare and information confrontation subunits', which are distinct from units responsible for cyber intelligence operations. Russian officers have emphasised that formations tested in these exercises (and already deployed in Syria) are using some techniques 'unchanged since the Great Patriotic War', including loudspeaker broadcasts in foreign languages and leaflet drops, while also making use of new capabilities such as UAVs designed to intercept or broadcast data on cell-phone networks. Strategic cyber information campaigns appear to be conducted by other organisations to target critical infrastructure systems and conduct espionage. Nevertheless, the use of information subunits may reflect a shift in Russian thinking about the role information warfare in war fighting (Giles, 2017).

STATE, NON-STATE AND SUB-STATE ACTORS

State agencies responsible for the control of information form the apex of a complex structure which also includes independent actors, whose views reinforce disinformation narratives. One report suggests that the key actors are members of the presidential administration and its associated networks of business leaders, veteran officers and former agents of the Soviet intelligence services who have links to the presidential circle. These actors constitute a 'state within a state' which interacts with but is distinct from formal elements of the government of the Russian Federation. However, 'the extent to which activities within this complex system are orchestrated, and by whom, remains unclear' (Canadian Security Intelligence Service), in terms of the loci of decision-making and organisational framework.

Authoritative scholars have offered two important observations. First, they cast doubt on the notion that Russian information campaigns are 'attributable to a Kremlin strategy implemented with an iron hand and from the top down', as are given the freedom to interpret and develop official thinking; and second, official thinking at the top level is developed partly in response to and under the influence of thinking circulating below the level of official discourse employing state-aligned media to 'mainstream' those currents. Their conclusion is that 'the development of the post-Ukraine Russian world view is not an entirely top-down process and betrays the influence of powerful sub-official and popular discourses, which must be alternatively appropriated, moderated, and reconciled with one another, and with the official line' (Hutchings and Szostek).

One of the most difficult questions to answer is thus to what extent there is a centralised network within Russia's 'power vertical' with formal control over the content and promotion of disinformation and to what extent activities which may appear to be coordinated are in fact the product of multiple, fragmented and decentralised networks. The most recent version of Russia's Foreign Policy Concept, promulgated on 30 November 2016, states that 'soft power' includes 'the tools offered by civil society, as well as various methods and technologies – from information and communication, to humanitarian and other types'; one of Russia's main objectives is 'to bolster the standing of Russian mass media and communication tools in the global information space and convey Russia's perspective on international process to a wider international community'. Russia 'takes necessary steps to counter threats to its information security', including through the use of 'new information and communication technology' (Ministry of Foreign Affairs web site).

Numerous organisations and networks contribute to activities related to the promotion of information and opinion-forming. These include research institutes such as the Russian Institute for Strategic Research, founded by the Russian president and playing a consultative role to the presidential administration, government agencies and the State Duma. One reliable source (see Darczewska, 2014: 28-30) describes the activities of patriotic networks inspired by prominent public intellectuals such as Aleksandr Dugin. The portal of the 'Dugin network' (*http://rossia3.ru*) is linked to those of other groups such as the International Eurasian Movement, the National Bolshevik Party and their 'network clones', and its content, inspired by their 'patriotic mission', is disseminated via various social media platforms and discussion groups and thereby achieves widespread coverage. Another portal focuses on the topic of information warfare (*http://ruexpert.ru*) and is linked to numerous other pro-Kremlin internet forums including Russian diaspora portals.

These networks are primarily active among Russians. The information campaign addressed to overseas audiences, particularly Western audiences, is modified into a more sophisticated set of narratives on current affairs and disseminated through specialist media, particularly television, radio and internet media, including the Ministry of Foreign Affairs web site, which interprets political developments in a more sophisticated manner. In this case disinformation is usually more subtle and difficult to decipher (Darczewska, 2014: 35; see the CREST report: *Russia and Disinformation: Maskirovka*).

Numerous organisations promote Russian narratives in countries susceptible to them through the promotion of education and culture, the Russian language and the 'Russian world', chief among them the Russkii Mir Foundation, the Gorchakov Foundation and the Federal Agency for the Commonwealth of Independent States, Compatriots Living Abroad and International Humanitarian Cooperation (Rosstrudnichestvo), as well as other government-organised NGOs, non-profit civil society organisations, proxy groups and networks.

The Russian Orthodox Church, especially the Moscow Patriarchate, and Russian compatriot organisations and other groups which identify with official narratives, also play an important role. These include the World Congress of Russian Compatriots, the International Union of Russian Compatriots and the Institute of Russian Compatriots, Cossack organizations, Afghan veterans, paramilitary or ultra-radical groups, and youth groups. Educational and cultural links are promoted through Russian educational institutions. A range of business and economic networks link individuals and companies in Russia and overseas countries, especially in its neighbourhood.

These instruments have been characterised by one extensive academic study as 'vertically integrated propaganda networks'; however, the links described 'do not necessarily promote authoritarianism as a system of rule, but often represent values and ideas that stand in opposition to the values and ideas supported by the EU... we do not find evidence of authoritarian diffusion, but rather of the promotion of Russia's role as a centre of gravity aiming to appeal to Russians, Slavs and Orthodox Christians' (Dimitrova et al, 2017).

REFERENCES

Bartles, C. K. (2016). Getting Gerasimov Right. *Military Review*, 96:1.

BBC (2010) Profile: Russia's SVR intelligence agency. *BBC News*. 29 June, at *https://www.bbc.com/news/10447308* (accessed 26 September).

Canadian Security Intelligence Service (2018). Who said what? The security challenges of modern disinformation, *World Watch: Expert Notes publication no*. 2018-02-01, February, at *https://www.canada.ca/content/dam/csis-scrs/documents/publications/disinformation_post-report_eng.pdf* (accessed 4 May 2008).

Chekinov, S. and Bogdanov, S. (2013) O kharaktere i soderzhanii voiny novogo pokoleniia. Voennaia mysl'. No. 10. Pp. 13-24.

Darczewska, J. (2014). The anatomy of Russian information warfare. The Crimean operation, a case study. Ośrodek Studiów Wschodnich Warsaw, Point of View no 42, May.

Dimitrova, A., Frear, M., Mazepus, H., Toshkov, D., Boroda, M., Chulitskaya, T., Grytsenko, O., Munteanu, I., Parvan, T. and Ramasheuskaya , I. (2017). The Elements of Russia's Soft Power: Channels, Tools, and Actors Promoting Russian Influence in the Eastern Partnership Countries, EU-STRAT *Working Paper* no. 04, August.

Ensor, J. (2018) Russian misinformation about 'imminent' White Helmets chemical attack could spell start of Idlib siege. *The Telegraph*. 2 September, at *https://www.telegraph.co.uk/news/2018/09/02/russian-disinformation-campaign-syria-threatened-spark-new-war/* (accessed 26 September 2018).

Franke, U. (2015). War by non-military means: understanding Russian information warfare, FOI research report FOI-R--4065--SE, March, at *http://johnhelmer.net/wp-content/uploads/2015/09/Sweden-FOI-Mar-2015-War-by-non-military-means.pdf* (accessed 3 September 2018).

Giles, K. (2017). Assessing Russia's Reorganized and Rearmed Military. Carnegie Endowment for International Peace, Task Force White Paper, May, at *https://carnegieendowment.org/2017/05/03/assessing-russia-s-reorganized-and-rearmed-military-pub-69853* (accessed 4 May 2018).

Harding, L. (2010) Wikileaks cables claim Russia armed Georgian separatists. *The Guardian*. 1 December, at *https://www.theguardian.com/world/2010/dec/01/wikileaks-cables-russia-georgian-separatists* (accessed 26 September 2018).

http://svr.gov.ru web site of the Foreign Intelligence Service (accessed 3 September 2018).

Hutchings, S. and Szostek, J. (2015). Dominant narratives in Russian political and media discourse during the Ukraine crisis. *Ukraine and Russia: people, politics, propaganda and perspectives*, at *http://www.e-ir.info/wp-content/uploads/2016/06/Ukraine-and-Russia-E-IR-2016.pdf#page=184* (accessed 17 February 2018).

Nahas, N. (2018) Russia Ramps Up Chemical Weapon Disinformation Leading up to Idlib Offensive. Bellingcat. 30 August, at *https://www.bellingcat.com/news/mena/2018/08/30/russian-chem-disinfo-idlib/* (accessed 26 September 2018).

RFE/RL (2017) Russia Threatens Retaliation if Google Downgrades RT, Sputnik News Sites. RFE/RL. 22 November, at *https://www.rferl.org/a/russia-roskomnadzor-zharov-threatens-retaliation-google-downgrades-rt-spunik-news-sites/28868922.html* (accessed 26 September 2018).

Thomas. T. (2014). Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts, *Journal of Slavic Military Studies*, 27:1.

Watts, C. (2018) Russia's Active Measures Architecture: Task and Purpose. Alliance for Securing Democracy. 22 May, at *https://securingdemocracy.gmfus.org/russias-active-measures-architecture-task-and-purpose/* (accessed 26 September 2018).

www.mil.ru web site of the Russian Ministry of Defence (accessed 3 September 2018).

For more information on CREST
and other CREST resources, visit
www.crestresearch.ac.uk

CREST

CENTRE FOR RESEARCH AND
EVIDENCE ON SECURITY THREATS

19-026-01