CREST Centre for Research and Evidence on Security Threats

Russia and Disinformation: The Case of the Caucasus

FULL REPORT

MARCH 2019

Dr Cerwyn Moore

MARCH 2019

RUSSIA AND DISINFORMATION: THE CASE OF THE CAUCASUS

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 Ukraine', 'Maskirovka' , and 'Institutions and Actors' 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

TABLE OF CONTENTS

INTRODUCTION

How does Russian state disinformation operate in the Caucasus region? This CREST 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.

The North Caucasus, well known as the most volatile region in the Russian Federation has been the setting for violent conflicts including ethnic, religious and separatist struggles. The region is associated with human rights abuses, corruption, and the lack of economic development. Kremlin policies in the region reflect a lack of understanding of, or will to work with, the various local ethnic or clan power sources in the region, preferring to co-opt local leaders or install Kremlin-tied figures, use coercion (repression), as well as disinformation. The North Caucasus republics have little autonomy and regional officials are largely appointed by the Kremlin. Chechnya remains the exception, with leader Ramzan Kadyrov enjoying broad latitude to rule as he pleases, provided he keeps the local insurgency restrained. The South Caucasus, comprised of the sovereign states of Armenia, Azerbaijan, and Georgia is geopolitically important to Russia as a southern corridor to the Middle East, and is, in the Russian view, its 'backyard'. Georgia in particular, with its anti-Russian and pro-Western stance has been a major flashpoint of contention between Russia and NATO, with an open conflict occurring between the two states in 2008.

For the purposes of analysis, the report will analyse three case studies in order to understand the dynamics of disinformation in the North Caucasus. They are: (1) the Beslan school siege; (2) the 2008 war between Georgia and Russia; and (3) Chechen leader Ramzan Kadyrov's disinformation on social media. How are these three examples useful? The Beslan school siege tells us about the management and subsequent framing of an event of domestic terrorism that also involved the use of hard power. The 2008 war is interesting as an international military confrontation involving a significant element of disinformation. The Kadyrov case on the other hand is enlightening as an example of disinformation in the context of propaganda and technical change with the rise of social media. Moreover, these three examples tell us about how Russia variously manages disinformation in relation to: an incident/event, another sovereign state, and an individual.

Why is the Caucasus important, and what does the Russian deployment of disinformation in the region tell us? The fact that the North Caucasus and Georgia are seen by the Kremlin as areas where it can use (and has) used aggressive military force makes the disinformation deployed there important to understand how Russia sees the use of strategic influence in its own neighbourhood. This report in disinformation in the Caucasus reveals, broadly, three things: First, these cases show that the goal of disinformation circulated in the North Caucasus (domestically) is to consolidate support for Putin and support around the various power ministries and power centres of Russia, while the aim of disinformation deployed in Georgia in the South Caucasus (internationally) is to undermine the adversary's position in the eyes of the international community and its own people. Thus, despite the similarities between the way the Kremlin views Georgia and the North Caucasus, there are clear differences that reflect Georgia's sovereign status, even as Russia views it as part of its neighbourhood. Second, these cases show that despite what Western commentary often suggests, while Russian disinformation can be orchestrated in a top-down manner, it does not have to be, and disinformation can also be deployed by non-state actors as well as involve different Russian institutions in each event. Third, it shows that Russia does not use a playbook for deploying disinformation, even as it uses much of the same tactics in different disinformation campaigns. Russian disinformation is often reactionary and not as centralised as observers may believe. Furthermore, the general strategies of disinformation have not changed since the Soviet era, rather the emergence of new tools and technology through which disinformation now occurs has given the Russian authorities different, more efficient ways to exert influence.

DISINFORMATION AND PROPAGANDA AND THE RISE OF TECH

Disinformation in the Russian context is often used as an umbrella term which includes other concepts such as strategic deception (*maskirovka*), information operations, and denial. As noted in the other reports in the series, when considering disinformation and *maskirovka*, the common factor is the use of various information tools such as media distortion, social media manipulation, and cyber attacks to convey selected, incomplete and/or distorted messages in order to influence targeted audiences. The goal is to create doubt, to muddy the waters of truth, and promote false narratives. When combined together with military force, the result is known as a 'hybrid threat'. In the Soviet era, as today, Russian disinformation can be divided into two spheres: offensive disinformation, which seeks to influence decision makers abroad, and defensive disinformation which seeks to influence citizens (White, 2016). As observers have said elsewhere about Russian propaganda, offensive disinformation is also used by Russia not so much to convince, but to contaminate the information environment and create doubt among perceived adversaries and their supporters.

Propaganda on the other hand, denoting the dissemination or promotion of ideas, came from 17th century Vatican efforts to promote the Roman Catholic faith. According to the Oxford English Dictionary, propaganda is the 'systematic dissemination of information', in particular in a 'biased or misleading way, in order to promote a political cause or point of view' (Oxford English Dictionary, 2007). Propaganda can be used by state actors to achieve national goals as well as by non-state actors such as terrorists. Just as propaganda can be used by various actors in different contexts and purposes, channels of communication are also evolving. With the Internet, new ways of making the mass production of propaganda are being made possible.

While in the Soviet-era information flows could be controlled, in the new global digital media environment, Russia's disinformation and propaganda campaigns are vulnerable to challenge by alternative domestic information sources, international news, and other transnational actors (Oates, 2014). This has provided new opportunities also for coercion and control of information in Russia, from the state buy-out of mass media and censorship to the murder of critical Russian journalists. While some studies show that the Internet provides new spaces for civic discussion in Russia (Kelly et al, 2012; Etling et al, 2014), other studies cast doubt on the democratising impact of the Internet on Russian politics, showing there is no distinguishing difference between opinions of television viewers and internet users (Cottiero et al. 2015). At the same time, the Internet's rise has undeniably provided new opportunities for top-down strategic narrative work. Old strategies of covert influence and propaganda are now more rapidly and readily deployed on a mass scale at little cost.

This Russian use of the digital world for disinformation also carries markers that suggest the scale of the attacks is growing. As Thomas Rid points out, in 2000, a shift in tactics became discernible, in particular in Moscow's military intelligence agency, the GRU. Actors who were once risk-averse and careful, became more reckless, risk-taking, and error-prone (United States Senate Select Committee on Intelligence, 2017). While the magnitude of Moonlight Maze, the first major state-on-state campaign which began in 1998, lasting for two years, and which was at the time unprecedented and alarming for US defence, the shift in 2000 increased the scale and scope of attacks while adding the use of leaking to hacking. However, during the late 1990s and throughout the 2000s, more traditional means of disinformation also remained commonplace.

BESLAN

On 1 September 2004, armed Islamic militants occupied a school in the town of Beslan in the Republic of North Ossetia for three days, taking more than 1,100 hostages, of which 777 were children. The hostage takers, guided by North Caucasus insurgency leader Shamil Basaev, demanded the recognition of Chechnya's independence and the withdrawal of Russian troops from Chechnya. On the third day of the crisis, Russian security forces stormed the school with tanks and incendiary weapons. 334 people were killed, including 318 hostages, of which 186 were children.

The disinformation campaign in Beslan involved three main activities:

- Disseminating disinformation.
- Information control.
- Propaganda.

DISSEMINATING DISINFORMATION

From the beginning of the siege, the number of hostages was deliberately underestimated by the authorities. Television channels and government representatives repeated that the number of hostages was 354, up until the storming of the school building. This happened even as higher numbers of hostages were reported by some newspapers and Internet sources, as well as Beslan residents on the ground. The false numbers reported angered both local residents who in some cases physically attacked Russian and international reporters on the ground, as well as the terrorists, who had wanted their actions to resonate with the international media (Litavrin, 2016).

Moreover, independent journalists on the ground reported that a decision was made in Putin's circle to not release information about the terrorists' demands (Kara-Murza, 2015). Thus, the terrorists' demands for an end to the Chechen war and withdrawal of Russian troops from Chechnya were kept secret while it was publicly claimed that the terrorists had no demands (Satter, 2006). What is more, the Russian authorities stated that its efforts to speak to the terrorists was ignored.

As soon as the hostage crisis began, Russian officials said they would do everything to avoid an armed assault on the school by security forces. On 3 September, *Nezavisimya Gazeta* reported that intelligence forces were preparing to storm the school, referring to the fact that on 1 September military transport planes had landed in the area and the presumption was that Alfa anti-terror special units were brought in. It is known that Alfa and Vympel, another anti-terror special unit both of which are Spetsnaz took a large role in the storming of the school. There is however no indisputable evidence that an official assault was ordered. Despite this, tactical decisions did little to minimise casualties. For example, the authorities did not secure the site or establish a secure cordon around the area, which allowed unauthorised and vigilante groups within close proximity of the school and that jeopardised operational command (Forster, 2006). Moreover, the choice to use incendiary weapons and tanks, while ensuring the destruction of the terrorists only cased more casualties.

From the outset of the hostage crisis, North Ossetia FSB chief Valeri Andreev and others projected blame for the attack on Chechen and international terrorists rather than on the Ingush fighters many locals suspected. This may have been to avoid the potential intensification of interethnic tensions between the Ingush and Ossetians. The chairman of the Central Spiritual Board of Muslims, a Kremlin controlled body, Mufti Ravil Gainutdin also laid blame at the feet of 'international terrorism leaders' (Interreligious Council of Russia, 2004).

INFORMATION CONTROL

The authorities took active measures to suppress any competing stories that would damage the credibility of the government's version of events. Journalist Andrei Babitsky was prevented from traveling to Beslan after he was detained at a Moscow airport for 5 days on charges of hooliganism after unidentified men picked a fight with him (Novaya Gazeta, 2004). The late Russian journalist Anna Polikovskaya was also prevented from flying to Beslan to cover the events, and on her second attempt, she was poisoned with tea on board a plane to Rostov and fell into a coma. Meanwhile, after the

storming of the school, international journalists from Germany, the US, and Georgia had their video footage seized by local authorities (Novaya Gazeta, 2004). The crew of Georgian television outlet Rustavi 2 was arrested, and one of the correspondents, Nana Lezhava, who had been in detention for five days was poisoned by psychotropic drugs (Walsh, 2004; Novaya Gazeta, 2004; Kishkovsky, 2005). On 6 September, Al Arabia correspondent Amr Abdul Hamid was detained at the local Mineralnye Vody airport upon leaving Russia and his bags searched. A bullet was found in his baggage and a criminal case launched against him. The reporter was released two days later and stated that he thought the bullet was planted in his belongings while staying at a Beslan hotel. Moreover, editor of well-known daily *Izvestia*, Raf Shakirov, was dismissed from his job after the newspaper criticised the government's handling of the Beslan siege (Cozens, 2004; Novaya Gazeta, 2004).

Germany, the US, and Georgia had their video footage seized by local authorities (Novaya Gazeta, 2004). The crew of Georgian television outlet Rustavi 2 was arrested, and one of the correspondents, Nana Lezhava, who had been in detention for five days was poisoned by psychotropic drugs (Walsh, 2004; Novaya Gazeta, 2004; Kishkovsky, 2005). On 6 September, Al Arabia correspondent Amr Abdul Hamid was detained at the local Mineralnye Vody airport upon leaving Russia and his bags searched. A bullet was found in his baggage and a criminal case launched against him. The reporter was released two days later and stated that he thought the bullet was planted in his belongings while staying at a Beslan hotel. Moreover, editor of well-known daily *Izvestia*, Raf Shakirov, was dismissed from his job after the newspaper criticised the government's handling of the Beslan siege (Cozens, 2004; Novaya Gazeta, 2004).

PROPAGANDA

Putin's declarations after the crisis conveyed a sense of national humiliation through the metaphor of Russia as a human body and its existential threats as viruses attacking it. The correct response to the threat was framed as an agenda of renewal by building internal immunity and strength (Ó Tuathail, 2009). Russian media, in particular *Rossiyskaya Gazeta*, also picked up and rearticulated this metaphorical framing. Authorities positioned the Beslan school siege within a framework of competition between states in order to give it meaning. It is widely considered that the Beslan crisis was used by Putin to clamp down on media freedoms within Russia.

Another aspect of propaganda surrounding the Beslan siege is the Torshin Report, an attempt by pro-Kremlin elements to shape public perceptions of the siege. It consisted of a Russian parliamentary commission that was meant to investigate the events of Beslan and was chaired by Alexandr Torshin, a deputy speaker of the Federation Council (Dunlop, 2009). While the report criticised the Russian authorities' handling of the crisis, the majority of the blame was directed towards local law enforcement, even as survivors, witnesses, and journalists who were present during the siege were almost all critical of the federal authorities (Torshin Commission Report, 2004).

THE 2008 GEORGIA-RUSSIA WAR

The Russo-Georgian war, between Russia, Georgia, and the Russia-supported self-proclaimed republic of South Ossetia, legally a part of Georgia but de facto independent took place in August 2008. At the time, relations between Russia and Georgia had been worsening. On 1 August, South Ossetian separatists began shelling Georgian villages, with intermittent responses from Georgian peacekeepers. The Georgian Army entered the conflict zone in South Ossetia on 7 August and took control of the capital of South Ossetia, Tskhinvali the same day. Before the Georgian military response, Russian troops mercenaries and 'volunteers' streamed into Abkhazia and South Ossetia. Russia then claimed that an initial Georgian attack had killed 1500-200 South Ossetian civilians, which warranted a 'humanitarian intervention' (Nilsson, 2018) – initiating a land, air, and sea invasion of Georgia on 8 August. South Ossetians destroyed most ethnic Georgian villages in South Ossetia as Russia recognised the independence of Abkhazia and South Ossetia, leading Georgia to sever diplomatic ties with Russia. Russia mostly withdrew its troops from Georgia but has since occupied Abkhazia and South Ossetia in violation of the August 2008 ceasefire agreement.

Russia's operations during the 2008 war with Georgia provides an excellent example of the coinciding of a disinformation campaign and military action, and it is the first known case combining cyber warfare with military action in history.

The disinformation campaign during the 2008 war involved four main activities:

- Disseminating disinformation.
- Information control.
- Propaganda.
- Cyber attacks.

DISSEMINATING DISINFORMATION

Russian media sources inflated, or at the very least, did not have any basis for the casualty figures used: Russian media reported that Georgian assailants had killed between 1500 and 2000 South Ossetians (Vesti, 2008), a figure reduced afterwards by the Russian Federation's Investigation Committee of the General Prosecutor's Office to 162 civilian casualties (Fawn & Nalbandov, 2012: 59). This information was picked up by Russian media and repeated, creating part of the justification for intervention.

Medvedev called the conflict, or at least Georgian actions against South Ossetians a 'genocide', a claim that Human Rights Watch called unfounded (Human Rights Watch, 2009). RT (formerly Russia Today) and other outlets used the headline 'GENOCIDE' for their segments about the conflict (RT, 2008a). The Russian ambassador to Georgia Vyacheslav Kovalenko claimed that 'Tskhinvali does not exist anymore. It is just gone. It has been destroyed by Georgian soldiers.' (Interfax, 2008).

Other Russian allegations stated that an American citizen had been fighting with Georgian forces. At a press briefing, Deputy Chief of the General Staff Anatoly Nogovitsyn presented photocopies of an American passport, claiming it had been found in a building which served as a Georgian fighting position. Vladimir Putin then told CNN 'We have serious reasons to believe that American citizens were right at the heart of military action.' (RT 2008b). The owner of the passport later denied the allegations, saying he had lost his passport elsewhere (Fairclough and White, 2008).

At a Valdai discussion club meeting soon after the conflict, Putin was asked why Russian troops had gone beyond the borders of South Ossetia and into Georgia. Putin's response is a strong example of obfuscation and subterfuge often deployed in a disinformation campaign, and it deserves a full quote. Putin responded first that the question did not surprise him: 'What surprises me is something else: just how powerful the propaganda machine of the West is.' Putin then congratulated the organisers of this Western propaganda. 'It is remarkable work! But the results are poor. And they always will be because this work is

dishonest and amoral.' With regards to Russia's foray into Georgia, Putin says everyone should 'remember how the Second World War began. On 1 September, fascist Germany attacked Poland. Then they attacked the Soviet Union. Were we supposed to go back only to the [pre-war] borders and stop there? Moreover, Soviet forces were not the only ones to enter Berlin – there were Americans, French, and British.' These states did not stop at their own borders, as, in Putin's view, it was necessary not only to expel the invader, but to ensure that 'aggressors are punished' (Goble, 2008: 189). Tangential arguments often combine falsehoods with obvious truths, but the implication that Russia was going after 'fascists' in Georgia is important.

INFORMATION CONTROL

By disseminating television footage and daily interviews with Russian military representatives, Russia was able to control the flow of international information by shaping the conversation and sharing the progress of Russian military actions. A review of international media during this time shows that Russian President Dmitry Medvedev was perceived as less aggressive than his Georgian counterpart, and a CNN poll conducting during this period found 92 percent of respondents believed Russia was justified for intervening (Iasello, 2017).

Suggesting some level of war planning, Russian state media was 'extremely well prepared to cover the outbreak of armed conflict in Georgia' with the main TV channels quickly displaying 'elaborate graphics' and 'news anchors and commentators [keeping] to disciplined talking points accusing Saakashvili of aggression and the Georgian armed forces of genocide and ethnic cleansing' (Whitmore, 2008). The Russian government positioned Russian journalists in Tskhinvali, the capital of the unrecognised Republic of South Ossetia before the start of hostilities. The day before Georgia introduced its troops into South Ossetia, there were already at least forty-eight Russian journalists there, and only two accredited foreign journalists. This suggests that Moscow knew that Tbilisi was going to bring in its troops and had planned its own military response, and that it wanted to make certain that both events were thoroughly covered (Goble, 2015). This enabled Russia to further control the dynamics of the way the conflict was discussed, airing details that seemed to impart a more open readiness to discuss details.

Furthermore, independent Russian media were absent from the ground, and the initial international reports filed from outside the conflict were riddled with factual errors. For example, the BBC initially used a map of North Ossetia rather than that of South Ossetia (Fawn & Nalbandov, 2012: 59), highlighting the problem of international journalistic knowledge and coverage of events in little known regions of the world during a disinformation campaign.

PROPAGANDA

Russia concentrated on disseminating three key themes to the international community: First, that Georgian President Saakashvili and Georgia was the aggressor; second, that Moscow had no choice but to intervene in protection of its citizens; and third, that the United States in particular and the West more generally had no right to criticise Russian actions because of NATO's previous intervention in Kosovo and elsewhere (Goble, 2015). While the argument may, at first glance, seem as an attempt at deflection, it is representative of 'whataboutism', a tactic Soviet propagandists were trained in, and which has made a resurgence in Russia over the last fifteen years. Thus, when, in the past, any criticism of the Soviet Union was responded to with 'what about…' the treatment of black Americans or Contras in Nicaragua, for example, now any criticism of Russia can be met with reminders about Guantanamo Bay (Economist, 2008).

While Georgia sought to counter these narratives with its own information and disinformation campaign, Russia's greatest success in the information war was the claim that it was acting defensively in response to Georgian aggression. This is despite the fact that Tbilisi did not move troops across an international border while Russia did exactly that. Furthermore, there were indications that Russia had been planning the campaign in Georgia in advance of years. For example, some years before the war, significant numbers of Abkhaz and South Ossetians had been given Russian passports, giving Russia the ability to justify its intervention in Georgia with needing to 'protect' Russian citizens.

Moscow however clearly went into serious preparations in the spring of 2008.

Interestingly, both Russia and Georgia consider their information war to have been overall unsuccessful. It is of general knowledge that Russia applied the lessons learned in this conflict in its annexation of Crimea and conflict with Ukraine (Iasiello, 2017: 54).

CYBER ATTACKS

Cyber attacks included webpage defacements, denial of service, and distributed denial of service on Georgian government, media, and financial institutions. Overall, citizens were denied access to 54 websites related to communications, finance, and government leading to some speculation about Russian complicity (Iasiello, 2017: 52).

While the Russian government denied the allegations that it was responsible for the attacks, some sources claimed that a Saint Petersburg criminal group known as the Russian Business Network, known as one of the worst spammer, child pornography and malware hosting networks, was behind many of the cyber attacks during the conflict (Swaine, 2008; Markoff, 2008).

Security researcher Greylogic however published a report which concluded that Russia's Foreign Military Intelligence Agency (GRU) and the Federal Security Service (the FSB), not civil hackers, were likely to have played a key role in coordinating and organising the attacks. In particular, it was found that an online forum, called *StopGeorgia.ru*, which was the centre for attacks on key Georgian websites, used an ISP situated a few doors down from GRU headquarters. According to Greylogic, the site was created as a front for state-backed cyber attacks under the pretence of cyber crime (Leyden, 2009). As Greylogic states, the *StopGeorgia.ru* forum 'was part of a bulletproofed network that relied on shell companies and false WHOIS data to (a) prevent its closure through Terms of Service violations, and (b) to mask the involvement of the Russian FSB/GRU. By mimicking the structure of the Russian Business Network, a cyber criminal enterprise, it creates plausible deniability that it is a Kremlin-funded Information Operation' (Leyden, 2009).

The Greylogic report concludes that the evidence available strongly suggests GRU/FSB planning and direction at a high level at the same time as it relied on Nashi (a Kremlin-allied youth group) agents as well as crowdsourcing to obfuscate their involvement.

Furthermore, a report from the United States Cyber Consequences Unit concluded that the organisers of the cyber attacks were aware of Russian military plans while the attackers themselves were thought to be civilians (Lemos, 2008; Prince, 2009). While there is no conclusive evidence that the attacks were tied to the Russian government or military, the hackers seem to have had advance notice of Russia's incursion into South Ossetia.

RAMZAN KADYROV AND DIGITAL MEDIA

This section deals with Chechen leader Ramzan Kadyrov's use of Internet Communication Technologies (ICTs), and in particular social media platforms highlighting the way he uses a mix of disinformation and propaganda to present his regime as successful and to inspire fear of existential threats to Chechnya in a way that asserts he is the most qualified person for the job.

Historically, political leaders have used all types of media for influence and propaganda and have taken advantage of new forms of communication as they have arisen; cyberspace is now also an arena for states to pursue strategic competition and exert sovereignty. In Russia, however, where all major media outlets and most smaller outlets are under state control, the Internet is the last place where information can be acquired freely by citizens. This has brought on consequences from crackdowns on Internet freedom within Russia, to the use of bots, trolls, and cyber operations to disrupt and muddy narratives opposed to the Kremlin outside it.

A look at Chechnya's leader Ramzan Kadyrov and his use of the internet provides a clear example of a Russian political figure using the digital space for a unique combination of disinformation and propaganda. Kadyrov's online practices can be contextualised as the use of new digital spaces by an authoritarian leader for projecting power, representing a dominant hegemonic power responding to changing social relations globally, brought on by increased ICT interconnectivity (Avedissian, 2015). Evgeny Morozov presents a useful summary of the process of authoritarian regimes' response to the Internet in *The Net Delusion*, explaining that it begins with resistance, which is then "followed by a wide embrace" (Morozov, 2011: 115).

Ramzan Kadyrov is an avid user of social media, and was previously best known for his Instagram account, which had more than 3 million followers before it was blocked in late 2017 as a result of US sanctions. He is now on the Telegram messenger application, which was recently blocked in Russia, but which Kadyrov defiantly continues to use to disseminate his messages.

Kadyrov's online disinformation involves two main activities:

- Digital disinformation and propaganda.
- Information control.

KADYROV'S DIGITAL DISINFORMATION AND PROPAGANDA

Kadyrov's digital strategy constitutes an intersection between a personality cult and a nation-building project and represents the process of how technology has influenced the capacity of Russian leaders to roll out disinformation strategies. This type of disinformation campaign is less about preventing messages from getting out than it is about delivering a leader's favoured messages, symbols, and myths. Along the lines of Polese & Horak's work (Polese and Horák, 2015), in this specific context, Kadyrov's personality cult serves as an instrument of nation-building which Chechen identity becomes one comprising a set of attributes defined by Kadyrov. In line with Hobsbawm and Ranger's (1992) work, being a 'real Chechen' in Kadyrov's official narratives depends in large part on the willingness to accept the absolute power of Kadyrov, his quasi holiness, and the specific version of history that heroicises his family.

Digital technologies generate fresh challenges and opportunities for states and leaders to engage in propaganda. The Chechen case in particular is interesting as some of the official narratives constructed by Kadyrov about Chechens may seem natural or are taken for granted, and yet they are not at all inevitable. For example, Kadyrov's efforts to Islamicise Chechnya have led to the ban of alcohol sales and the covering of women's heads in schools and government buildings. While this may seem natural to observers now, this was not the case even ten years ago.

Kadyrov's account of reality as expressed in his social media communications fuses selective aspects of pre-Soviet and Soviet conceptions of power and order in pre-Islamic/traditional, Islamic (both Sufi and Salafi),

and Soviet practice. For example, Kadyrov's framing of the Chechen wars in the 1990s and early 2000s transform them into a conflict of the Chechen people against 'terrorists' instead of against Russian rule. Such a conception of history erases Chechnya's aspirations for independence, the root of the conflict(s), casting them in a way that flatters Russia and Putin in particular.

Kadyrov also makes frequent references to existential threats to Chechnya, in particular the West, 'enemies' of Islam (presumably Salafi Muslim opponents of Kadyrov's regime), who are all presented in a way that their continued threat becomes necessary to understand the regime's actions today (Avedissian, 2015). Kadyrov writes about events such as Chechnya's defence preparedness and planned infrastructure works. As Avedissian (2015) has noted, these posts do not provide new insights into governance or increase transparency; rather, they offer a chance for opportunistic celebration of the regime. Kadyrov's use of the Internet to portray himself as the only man for the job are communicated through posts that frame himself as the natural predecessor to his father's short rule over Chechnya, as well as the frequent posts showing him working out, which suggest his prowess and readiness as leader.

INFORMATION CONTROL

Kadyrov heavy-handedly controls information about the Chechen Republic. All information given by Chechnya's television, radio, and online news outlets is censored or self-censored to avoid retribution for criticising the authorities. Numerous sources about local Chechen journalists note that they work under the principle of not making Kadyrov angry (Anonymous, 2016). The last groups left to report truthfully from the republic – independent journalists from other parts of Russia (usually Moscow), and human rights organisations, have been threatened and their work impeded by the Chechen security services. While the physical repression of journalists and human rights workers occurs in the real world, the digital space is an essential factor that facilitates it and it is only when accounting for the real-life coercion and violence can we fully understand Kadyrov's digital disinformation and propaganda.

Human rights defenders who were previously numerous in Chechnya have been repressed to the point of all but stopping their work in the republic. After Memorial's Natalia Estemirova was murdered in 2009, the Chechen government continued to intimidate and discredit the organisation, and the Committee Against Torture's Mobile Group took over in Chechnya. By 2014, however, the Mobile Group's offices had been attacked three times and set on fire and its staff was the target of a smear campaign in the Chechen media. In June 2015, a mob destroyed the office and seized documents related to ongoing cases the Committee was in the process of investigating. The Mobile Group ceased its permanent residence in the republic in 2016.

For example, in March 2016, a bus with journalists who had travelled to Chechnya including a journalist from Sweden and Norway, was stopped on the border of Chechnya and Ingushetia by masked men. The men pulled the passengers out, beat up some of them, told them there was nothing for them to do in Chechnya, and set the bus on fire (Walker, 2016).

Part of Kadyrov's information control strategies involve the crushing of dissent expressed online. Research on cases similar to Chechnya's where autocratic governments actively censor online content and levy high penalties for online expression of dissent (e.g., Egypt, Gambia) (Hellmeyer, 2016), have led researchers to understand that the Internet's impact on democratisation is at best limited (Hellmeyer, 2016).

In Chechnya, online dissenters are often unlawfully detained, sometimes kidnapped, humiliated, threatened with physical harm and public humiliation. Often the families of these individuals are also threatened. In one case, a social worker named Aishat Inaeva, urged Kadyrov on the WhatsApp application, popular in Chechnya, to investigate ordinary people's problems (Translation Service from Caucasian Languages, 2015), and was publicly shamed and humiliated on television. A week later, Inaeva found herself sitting in front of Kadyrov, in a 20-minute segment of public shaming that was aired by Grozny TV (Shamanska, 2015). Another woman who used an audio message addressed to Kadyrov, also posted on the WhatsApp messaging application to complain that her husband had been taken away by Chechen security services for allegedly trying to join militants in Syria. The woman was forced to publicly apologise to Kadyrov in a video recording posted again to WhatsApp in which she recants her previous statement and asks for Kadyrov's forgiveness

(Caucasian Knot, 2017). In a society in which collective responsibility is the norm, the gravity of publicly losing face like this cannot be underestimated.

Kadyrov is attempting to halt the diversification of public debate in the republic, brought on by both human rights workers and lawyers, but also by citizens on social media. Kadyrov sees the digital space as a place people can sidestep traditional media as a state-controlled controlled entity that reports only the official viewpoint of the state. While Kadyrov does not engage in Internet shutdowns of networks as other authoritarian leaders have done and are doing with increased frequency around the world (Hellmeyer, 2016), his actions still represent those of a rational autocratic actor whose primary goal is to stay in power and extract as many resources as possible (see Olson, 1993). The Internet is a communication tool that lowers costs of transactions and facilitates collective action. Its repression is not different from that of civil rights such as freedom of association, speech, or press.

CONCLUSION

What do these cases tell us? Firstly, the tell us that there is no playbook by which the Russian authorities use for disinformation campaigns. During the Beslan siege, the disinformation was mostly reactive, highlighting the unpreparedness of the Russian authorities and constituting a series of responses to control the framing of extremely fluid and unpredictable events as they developed. In the aftermath of the school storming, confronted with emerging discourses about the incompetence of the Russian government's handling of the events, Putin blamed an international conspiracy, and characterised Russia as a 'besieged fortress', which served as justification for paring down on civil liberties and strengthening censorship of media across Russia.

It is possible that Russia has learned from the Beslan events and has invested in the widespread framing of traditional adversaries of Russia, such as international terrorism, fascism, and/or the West, frames Russia has since readily and repeatedly drawn from in different contexts. For example, during the 2008 war, Georgian actions were framed as 'terrorist' (RT, 2008c) and Saakashvili as 'Hitler' suggesting that the similarities in the framing of adversaries is not a coincidence. There is however no discernible sequence of steps that Russia uses in its disinformation campaigns.

Secondly, these cases show that Russian disinformation campaigns are not managed in a strictly top-down manner. Rather, lower-ranking government officials can voluntarily pick up and repeat the specific government talking points, as do various actors in society such as the media and bloggers. For example, in the Beslan siege, while local residents whose family members and children were held hostage stuck to their experiences of and conclusions about the events before during and after, it is clear that the local authorities changed the way they spoke about the events over the course of the siege and its aftermath. While it is impossible to know whether there was any directive from above about how to speak about the events, it is clear there was no coordinated disinformation campaign, at least from the beginning. For example, North Ossetian President Dzasokhov shifted the blame for the events from the Ingush fighters he had previously pointed to 'international terrorists', following Putin's narrative (O'Tuathail, 2009: 12). A week later, the North Ossetian Parliament also followed the same line with an appeal to President Putin on 10 September, saying, 'The terrorist acts that have occurred recently in different Russian cities show that international terrorism has declared war on us.' (O'Tuathail, 2009: 12).

Lastly, these cases tell us that different Russian institutions are involved in each case of disinformation. In Kadyrov's case, you have a disinformation and propaganda project that is completely separate from the Kremlin, even as it is used to support the Kremlin and Putin in particular. Kadyrov enjoys broad carte blanche for his actions within the republic and is very independent on the one hand, while on the other, his power derives in large part from Putin in the form of federal subsidies. Thus, Kadyrov's disinformation project is one that can be said to be to primarily influence Putin, to convince him of Kadyrov's loyalty and suitability for his post, and to show how the republic is developing. Disinformation in the form of cyber attacks is also almost always attributable to the GRU, which, for example, had little role in the Beslan siege.

In regard to cyber attacks and their content and dynamics, as Dr Thomas Rid stated during a hearing before the Select Committee on Intelligence of the United States Senate in March 2017, attributing and countering Russian disinformation is impossible without first grasping how the US and its allies attributed and countered active measures throughout the Cold War. Active measures used 'an adversary's existing weaknesses against himself, to drive wedges into pre-existing cracks. The more polarised a society, the more vulnerable it is' (United States Senate Select Committee on Intelligence, 2017). Thus, with increasing polarisation of societies in the West and in Europe in particular, there are numerous opportunities for more active measures in the form of disinformation to be used to further disrupt and divide society. With the rise of tech however, the speed and scale of Kremlin attacks on its targets has exponentially increased, with Russia's use of aggressive digital espionage campaigns becoming the norm.

Front organisations have appeared that spread stolen information to the public in a targeted way (United States Senate Select Committee on Intelligence, 2017).

With the addition of the exploitation of 'unwitting agents', brings into focus the political and ethical challenge of disinformation. As Thomas Rid illustrates, three types of unwitting agents have emerged in the contemporary global political arena: WikiLeaks, Twitter, and journalists who eagerly cover political leaks without discretion (United States Senate Select Committee on Intelligence, 2017).

In some cases, online attacks are labelled as advanced persistent threats (APT). An APT is a set of covert and continuous hacking processes often carried out by an individual or group targeting a specific entity. Bodmer et al. (2015: 20) state that the actors behind APTs create increasing and shifting risk to organisations' and institutions' financial assets, intellectual property and reputation by following a continuous process or 'kill chain':

1. Target specific organisations for one objective
2. Attempt to gain a foothold in the environment, for example using spear phishing emails
3. Use the compromised systems as access into the target network.
4. Deploy additional tools that help fulfil the attack objective.
5. Cover tracks to maintain access for future initiatives.

Such attacks require a high degree of covertness and are deployed over a long period of time. These attacks are often undertaken by groups or states that can draw on military and business interests, as a way to engage with targets. Importantly, these attacks involve relatively sophisticated methods to extract information or monitor activity, they are ongoing or occur over long periods of time – hence the label persistent – and they are orchestrated and controlled by external human factors. But such forms of attack, threat and disinformation largely mirror the use of similar tactics in physical space.

Russian disinformation often involves numerous competing power ministries, institutions, and actors including organisations involved in finance, energy companies, media organisations and business entrepreneurs, many of which are part of a wider coterie of officials linked to the Russian Government. The emergence of social media technologies – and an online security ecology - has presented a plethora of new opportunities for influence and disinformation. Nonetheless, the examples herein illustrate that contemporary online and digital influence is somewhat piecemeal. ATPs emanating from the Kremlin exist, but they are part of a range of 'hybrid threats' which involve different institutions that seek to exploit weaknesses, exert influence and coerce. These threats blend forms of manipulation to leverage support.

The Russian authorities often base their disinformation on the masking of real identities (plausible deniability), meaning that perpetrators can remain unidentified. A similar process has been enabled by the emergence of computer technologies – as proxy servers, infected computers, spyware and viruses are used to compromise the online information space. Very similar principles underpin aspects of disinformation as deployed physically, in the North Caucasus, as this report demonstrated.

GLOSSARY

Advanced Persistent Threats (APT) – An attack in which an unauthorised individual gains access to a network in order to steal data, rather than cause damage, and remains there undetected for a period of time. APT attacks usually target organisations with sought-after information, such as national defence and financial sectors.

Spear phishing – An attack involving email fakes which target an organisation or person, seeking unauthorised access to information. Attempts are usually initiated by perpetrators for financial gain, trade secrets or military information.

Moonlight Maze – The set of FBI inquiries of intrusions into key military and political computer systems in the United States that began in 1998.

Instagram – A social networking application designed for sharing photos and videos. As with Facebook or Twitter, an account on Instagram comes with a profile and newsfeed which display the author's posts.

BIBLIOGRAPHY

Anonymous (2016). Chechen journalists, international journalists – Ramzan Kadyrov has silenced us all. *The Guardian*. 10 October. Available at: *https://www.theguardian.com/world/2016/oct/10/chechnya-no-longer-help-foreign-journalists-ramzan-kadyrov*

Avedissian, Karena (2016) Clerics, Weightlifters and Politicians: Ramzan Kadyrov's Instagram as an official project of Chechen memory and identity production. *Caucasus Survey*. 4:1. 20-43.

Bodmer et al (2015) *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. McGraw Hill.

Caucasian Knot (2017). Zhitel'nitsa Chechni izvinilas' za slova o nezakonnom areste muzha. 2 May. Available at: *http://www.kavkaz-uzel.eu/articles/302025/?utm_source=feedburner&utm_medium=twitter&utm_campaign=Feed%3A+kavkaz-uzel%2FuqrI+%28Кавказский+Узел++-+все+материалы%29*

The Economist (2008) Whataboutism. 31 January. Available at: *https://www.economist.com/node/10598774*

Cottiero, et al. (2015) War of words: the impact of Russian state television on the Russian Internet. *Nationalities Papers*. 43:4. 533-555.

Cozens, Claire (2004) Russian editor faces sack over Beslan coverage. *The Guardian*. 28 September. Available at: *https://www.theguardian.com/media/2004/sep/28/pressandpublishing.russia*

Dunlop, John (2009) *The September 2004 Beslan Terrorist Incident: New Findings*. Center on Democracy, Development, and Rule of Law, Stanford. July Number 115. Available at: *https://cddrl.fsi.stanford.edu/sites/default/files/No_115_Dunlop_Beslan_2004.pdf*

Etling, Bruce; Roberts, Hal; Faris, Robert (2014) Blogs as an Alternative Public Sphere: The Role of Blogs, Mainstream Media, and TV in Russia's Media Ecology. Berkman Center Research Publication. No. 2014-8. Available at: *https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2427932*

Fairclough, Gordon and White, Gregory (2008) From Russia Without Love: Kremlin Calls Mr. White a US Agent. *Wall Street Journal*. 3 September. Available at: *https://www.wsj.com/articles/SB122040803393693743*

Fawn, Rick and Nalbandov, Robert (2012) The difficulties of knowing the start of war in the information age: Russia, Georgia, and the War over South Ossetia, August 2008. *European Security*. 21:1. 57-89.

Forster, Peter (2006) Beslan: Counter-terrorism Incident Command: Lessons Learned. *Homeland Security Affairs*. October. Available at: *https://www.hsaj.org/articles/162*

Goble, Paul (2015) Defining Victory and Defeat: The Information War Between Russia and Georgia. In: Cornell, Svante E., and S. Frederick Starr. *The Guns of August 2008: Russia's War in Georgia*. Routledge.

Hellmeyer, Sebastian (2016) The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes. *Politics & Policy*. 44:6. 18 December.

Human Rights Watch (2009). Up in Flames: Humanitarian Law Violations and Civilian Victims in the Conflict over South Ossetia. 23 January. Available at: *https://www.hrw.org/report/2009/01/23/flames/humanitarian-law-violations-and-civilian-victims-conflict-over-south*

Iasello, Emilio J. (2017) Russia's Improved Information Operations: From Georgia to Crimea. *Innovations in Warfare and Strategy*. 47:2. 51-63.

Interfax (2008) Posol RF v Gruzii: V Tkhinvale pogibli kak minimum dve tysachi chelovek. 9 August. Available at: *http://www.interfax.ru/russia/26124*

Interreligious Council of Russia (2004) Obrashchenie v sviazi s tragediei v Beslane. 22 September. Available at: *http://interreligious.ru/documents/documents_41.html*

BIBLIOGRAPHY

Markoff, John (2008). Before the Gunfire, Cyberattacks. *The New York Times*. 12 August. Available at: *https://www.nytimes.com/2008/08/13/technology/13cyber.html*

Lemos, Robert (2009) Georgian Cyberattacks Traced to Russian Civilians. *MIT Technology Review*. 18 August. Available at: *https://www.technologyreview.com/s/414930/georgian-cyber attacks-traced-to-russian-civilians/*

Leyden, John (2009) Russian spy agencies linked to Georgian cyber attacks. *The Register*. 23 March. Available at: *https://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis*

Litavrin, Maksim (2016) Chto strashnogo v slovah "Putin – palach Beslana". *Open Russia*. 3 September. Available at: *https://openrussia.org/post/view/17316/*

Kara-Murza, Vladimir (2015) Beslan: Voprosy bez otveta. Radio Svoboda. 1 September. Available at: *https://www.svoboda.org/a/27220792.html*

Kelly et al. (2012) Mapping Russian Twitter. *Berkman Research Publication*. No. 2012-3. Available at: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2028158*

Kishkovsky, Sophia (2005) Cold War Tactics. Committee to Protect Journalists. Spring/Summer 2005. Available at: *https://cpj.org/regions_06/europe_06/cold_war_tactics.pdf*

Nilsson, Niklas (2018) Russian Hybrid Tactics in Georgia. Silk Road Paper. January. Available at: *https://silkroadstudies.org/resources/pdf/SilkRoadPapers/2018_01_Nilsson_Hybrid.pdf*

Novaya Gazeta (2004) Spetsoperatsiia v Beslane proshla uspeshno. Protiv zhurnalistov. 20 September. Available at: *https://www.novayagazeta.ru/articles/2004/09/20/20900-spetsoperatsiya-v-beslane-proshla-uspeshno-protiv-zhurnalistov*

O'Tuathail (2009) Placing Blame: Making Sense of Beslan. *Political Geography*. 29:1 (January).

Oates, Sarah (2014) Russian State Narrative in the Digital Age: Rewired Propaganda in Russian Television News Framing of Malaysia Airlines Flight 17. Paper prepared for the American Political Science Association Annual Meeting, Washington, DC. Available at: *http://www.media-politics.com/presentationspublications.htm*

Oxford English Dictionary (2007) Propaganda. Available at: *http://www.oed.com/view/*

Polese, Abel and Horák, Slavomir (2015) A tale of two presidents: personality cult and symbolic nation-building in Turkmenistan. *Nationalities Papers*, 43:3. 457-478

Prince, Brian (2009) Cyber-attacks on Georgia Show Need for International Cooperation, Report States. EWeek. 18 August. Available at: *http://www.eweek.com/security/cyber attacks-on-georgia-show-need-for-international-cooperation-report-states*

RT (2008a) Did mercenaries help Georgia? 10 August. Available at: *https://www.youtube.com/watch?v=Bcv-ynUDYHc*

RT (2008b) U.S. may have staged Georgian conflict – Putin. 28 August. Available at: *https://www.rt.com/news/us-may-have-staged-georgian-conflict-putin/*

RT (2008c) Abkhazia calls on the world to stop 'Georgian terror'. 8 July. Available at: *https://web.archive.org/web/20080712182053/http://www.russiatoday.ru/news/news/27084*

Satter, David (2006) The Truth About Beslan. Hudson Institute. 16 November. Available at: *https://www.hudson.org/research/4307-the-truth-about-beslan*

Shamanska, Anna (2015). Chechen leader shames social worker on live TV after complaint. *The Guardian*. 24 December. Available at: *https://www.theguardian.com/world/2015/dec/24/chechen-leader-ramzan-kadyrov-shames-social-worker-live-on-tv*

Swaine, John (2008) Georgia: 'Russia conducting cyber war'. *The Telegraph*. 11 August. Available at: *https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html*

Translation Service from Caucasian Languages (2015). Aishat Inaeva obviniaet Ramzana Kadyrova v neposil'nyh poborah v Chechnie. 18 December. Available at: *https://www.youtube.com/watch?v=fLhwQpQynxo*

United States Senate Select Committee on Intelligence 2017 Available at: *https://www.intelligence.senate.gov/hearings/open-hearing-intelligence-matters-1*

Vesti (2008) Lavrov: Nikakomu doveriiuk gruzinskomu rukovodstvu ne ostalos'. 12 August. Available at: *https://www.vesti.ru/doc.html?id=200375*

Walker, Shaun (2016) Journalists and activists beaten and bus torched on Chechnya tour. *The Guardian*. 10 March. Available at: *https://www.theguardian.com/world/2016/mar/10/journalists-beaten-and-bus-torched-on-chechnya-tour-say-activists*

Walsh, Nick (2004) Second Beslan reporter drugged. *The Guardian*. 11 September. Available at: *https://www.theguardian.com/media/2004/sep/11/russia.pressandpublishing*

White, Jon (2016) Dismiss, Distort, Distract, and Dismay: Continuity and Change in Russian Disinformation. *Institute for European Studies Policy Brief*. Issue 13. Available at: *http://aei.pitt.edu/77604/1/Policy_Brief_Jon_White.pdf*

Whitmore, Brian (2008) Scene at Russia-Georgia Border Hinted at Scripted Affair. Radio Free Europe/Radio Liberty. 23 August. Available at: *https://www.rferl.org/a/Russia_Georgian_Scripted_Affair/1193319.html*

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

CREST

CENTRE FOR RESEARCH AND
EVIDENCE ON SECURITY THREATS

19-020-01