The Rise of the Kremlin Troll

Sarah Morrison
School of Humanities and Social Sciences,
Swinburne University of Technology, Melbourne Australia
wheelz@me.com

Received Date: 30/4/2021 Accepted Date: 8/10/2021 Published Date: 1/12/2021

Abstract

After the Cold War collapse, the Russian government demonstrated several failings regarding military strategy and information operations. The Russian government then undertook improvements through critical learnings to formulate information warfare and adapt to online communication applications. Included in this strategy was the flooding of communications with a narrative designed to confuse and cast doubt on Russian and world events. This paper examines Russia's approach to information warfare during the Chechnya Wars, the Georgia war, the 2010/2011 Arab Spring protests, and the international protests and internal unrest in Russia at the end of 2011. As demonstrated through this timeline, rather than failing at information operations, Russia has been learning and adapting these techniques and strategies using online communication applications, particularly social medial networks (SMNs), resulting in the rise of the Kremlin troll. This paper will conclude by examining the Internet Research Agency (IRA), a known Russian troll farm in St Petersburg.

Keywords*: Information operations, Russian information warfare, Internet Research Agency, Kremlin troll, Disinformation*

1.0 Introduction

Russia's reliance on disinformation and propaganda is not a new instrument in the Kremlin's toolkit; it is, however, largely forgotten by Western society, believed to be a remnant of the Cold War, only to be revitalised through Russian military reform [1]. According to Giles [2], two key initiatives have led to Russian military reform since the Cold War. The first was the inauguration of the former head of the Russian Federal Security Services (FSB), Vladimir Putin, in 1999, and the second was Russia's failure in the 2008 Georgia War. However, it was not until 2011 that Russia's modern-day military began to take shape because of a series of critical events which have been said to have revolutionised Russia's information operations [3]: the Chechnya Wars in the 1990s; the armed conflict in Georgia in 2008; the 2010/2011 Arab Spring protests; the international protests and internal unrest in Russia at the end of 2011; and the annexure of Crimea in 2014. The case studies used throughout this paper were chosen as they highlight the consistent improvement to Russian information operations over the last 30+ years. The study design draws on various disciplines, such as Politics and International Studies, Human Centred Design and Media and Communication Studies and relies on secondary sources, such as known Western and Russian commentary on Russia's strategic approach to information operations and warfare.

ISSN 1985-563X

This paper explores Russia's adaptation of information operations and the rise of the Kremlin troll. What follows is an examination of the development of the Internet Research Agency (IRA), a known troll farm in St Petersburg. As demonstrated through this timeline, rather than failing at information operations, Russia has been learning and adapting these techniques and strategies using online communication applications, particularly social medial networks (SMNs). Included in this strategy is the flooding of communications with a narrative designed to confuse and cast doubt on Russian and world events and depict the role Russia envisions the West is playing in Russian affairs.

2.0 Chechen Wars

In 1991, after the fall of the Soviet Union, Chechnya declared independence from Russia. Using former Soviet Union military equipment left behind after the end of the Cold War, Chechnya was then able to create its military force. By 1994 however, Russia began to reassert authority over Chechnya, working with Chechnyan opposition leaders to try and regain control over the government and remove former Russian Air Force General turned President of Chechnya, Dzhokar Dudayev, from power. Russia undertook 'black' operations, using proxies to attack Chechnya rather than attacking Chechnya directly. Russia's proxies may be seen as a time-honoured strategy to demonstrate strength with limited resources and achieve Russia's geopolitical objectives [1]. In 1994, Russia deployed tanks to Chechnyan opposition fighters in an attempted coup against the Chechen President. The coup failed, and soon after, Russia's involvement was made public by the independent Russian press [4]. According to Finch [4], when Russian leaders realised that the Chechen proxies would not be able to defeat and to avoid any implication in the failed coup, Russian Ministers counselled the then President of Russia, Boris Yeltsin, to deploy new forces to Chechnya in the form of an outright Russian attack using conventional military forces. The sudden haste in the deployment of Russian troops revealed noticeable disorientation in Russia's command and control capabilities [4].

Galeotti [1] describes the Chechnya wars or counterinsurgencies as invasions lacking in traditional Russian panache. Notably, traditional Russian aptitude was missing in the information and political aspects of the first campaign. Journalists, Chechen government sources and Chechen sympathisers were given unfettered access to report on the events taking place, including the scourge of Russian operations and the war casualties. Russia did not have a compelling voice or counter-narrative in the global discussion of the event [1]. Russia's information operations, or lack thereof, were not the sole reason Russia lost the first Chechnya war. They merely contributed to the result of the war, which lasted until 1996. During the conflict, the Russian government and military made little effort to generate internal and external public support [4].

Furthermore, little explanation was given to Russian citizens regarding Russia's military operation [5], with the very nature of the conflict pitting the Russian military against Russian citizens living in Chechnya, a move that Russian media widely criticised [4]. As Finch [4] describes, if the

> Russian government was intent on winning the hearts and minds of the Chechen people, and convincing them to remain a part of Russia, then carpet bombing, and massed artillery strikes on civilian targets were the wrong tools. Having failed to apply lesser means of persuasion, use of the military was premature.

The lack of commentary provided by the Russian government also meant that journalists and civilians began turning to sources outside of Russia for information about the war. Head of Russia's Federal Security Service (FSB), Sergei Stepashin, recalled after the campaign that journalists, unable to receive details of the war from Russia, turned to Chechnya for information [6]. Russia was unprepared for the propaganda and ideological campaign Chechnya delivered, with Russian military

ISSN 1985-563X

forces ill-equipped to deal with the press [5]. In 1996, Russia brokered a cease-fire after Chechen guerrilla warfare led to the demoralisation of Russian troops [7].

In May 1999, President Yeltsin faced impeachment for his 1994 decision to deploy Russian troops to Chechnya. By October 1999, however, media and public support of the second Chechnya campaign and for President Yeltsin and Prime Minister Vladimir Putin was widespread [5]. In the second Chechen War (1999-2009), Russia seemed to have learnt from previous mistakes, taking draconian measures to ensure control of the media narrative of the war in both Russia and abroad [1]. Russia also appeared to have adopted the USA's example of information control during the Gulf War and entered into the second Chechen war with a strategic information plan [5].

The Russian government created a narrative of fighting Islamic extremists in Chechnya after a terrorist attack occurred in apartments in Moscow and Volgodonsk, Russia, in September 1999, leading up to the invasion. Reporters also showed little sympathy for Chechen fighters after they kidnapped approximately 1,800 people in Dagestan, the centre of the conflict during the second campaign since 1992. Some of the abducted victims were brutally murdered by Chechen fighters. Included amongst the victims were local citizens, foreigners and journalists [5]. In December 1999, Russian Federation Resolution No. 1538 was initiated by President Yeltsin, which ensured that the Russian population would only receive select information regarding the conflict from foreign sources and also filter what information concerning the campaign would be disseminated from Chechnya. Russia studied NATO's press conferences to learn how to speak to the press and, according to Thomas [5], "placed experienced people in key positions to ensure media control".

The concern in the Russian government that the Russian information war was failing outside of Russia began to emerge in October 1999. The sentiment was reiterated by the Head of the FSB Public Relations Centre, Aleksandr Zhanovich, who, when speaking to the Russian administration, criticised the foreign press for allowing Chechen rebels airtime [5]. In October 1999, the Russian Information Centre was established on the order of the newly elected Prime Minister, Vladimir Putin and headed by former Public Relations figure Mikhail Margelov in what appears to be an attempt to control the media. The centre offered instructions to reporters via a website on how to report from the front. The website also offered information on events occurring within the war, including maps and expert opinions. Margelov continued to express his concerns, including the concern that the Chechen militants were using the foreign media to open a second front in the information war [5].

In response, Russia put in place information blockades shutting down independent reporting and taking control of television and newspapers to ensure the release of sanctioned news stories only. The Russian government explained that these measures were necessary to prevent the enemy "from objectively assessing the situation" [8]. However, these information blocks were limited in their usefulness as the Kremlin had underestimated the power of the Internet. Chechnya used the new resource as a means of communicating to the outside world what was occurring internally. Chechen supporters established several internet sites to report on the Chechen version of events in Dagestan. As the Chechen versions were the only unfettered means of information, media outlets worldwide, including some within Russia, began using these sites to report on events in Chechnya. Once more, the Chechen version of events began to be the only primary source of reporting on the campaign [5].

In January 2000, heavy fighting in Groznyy saw high causalities. This, combined with the broken promises of the Russian government that the campaign was coming to an end, led to wavering in public support for the war within Russia. At this time, Chechen internet usage expanded, providing video footage of attacks on Russia, interviews with Chechen commanders, and videos of Chechen fighters in action. At the start of the second Chechen war, the Russian media appeared to accept the Russian government's story regarding the conflict. However, as the war progressed, Chechens bypassed the

ISSN 1985-563X

information blockade imposed by Russia through the Internet and foreign news reporters [5]. An important takeaway from the second Chechen War was that even though Russia may have won the war, they did not win the information war [3].

The lessons for Russia on the Chechen war were twofold. First, the mindset of Russia's leaders had been altered concerning practical knowledge and insights to its approach to information warfare [9]. Russia had learnt the importance of controlled information flow and the psychological impacts information could have on society, both of which have since been identified by the Kremlin as cardinal. As Heickerö [9] writes, "by controlling the information-psychological aspects such as the mass media - for instance, TV, radio and newspapers – as well as the information flow, stability can be achieved" [9]. Second, the Internet was a destabilising factor in information operations, and public access to the Internet and information itself should be controlled [3].

3.0 Georgian War, 2008

Since the end of the Cold War and extending into the Chechen and Georgia wars, the North Atlantic Treaty Organisation (NATO) may be seen as an area of contention for Russia. After the fall of the Berlin wall in November 1991, the US government worked with West Germany leaders to reunite Germany. Formerly secret US government documents from the early 1990s reveal an implied agreement with Russia that NATO would not expand beyond West Germany if Germany reunified. Although there is no formal contract or agreement, Sarotte's [10] investigative article discovered a trail of letters and notes suggesting that promises were made to former President of the Soviet Union Mikhail Gorbachev by the US and West Germany that NATO would not expand east from its current position. According to the letter trail, James Baker, the US Secretary of State at the time, acting on behalf of the US Government, made assurances to Gorbachev that NATO would not expand past West Germany. On hearing this discussion, staff members from the US National Security Council wrote to Helmut Kohl, the West German chancellor, on behalf of President George W Bush, explaining that the decision not to expand into East Germany after reunification did not make sense. Further, the letter requested that Kohl, in his upcoming meeting with Gorbachev, inform the Soviet Leader that special military status would apply to what is now Eastern Germany. As Sarotte [10] explains, "although the letter did not define exactly what the special status would entail, the implication was clear: all of Germany would be in the alliance, but to make it easier for Moscow to accept this development, some kind of face-saving regulations would apply to its eastern region". Kohl decided not to relay the new message but reiterated Baŧker's assertions that NATO would not expand [10].

When it became apparent in 1994 that NATO was planning an expansion, President Yeltsin, according to Goldgeier and McFaul [11], became enraged. From the Russian President's position, previous agreements had been broken with regards to NATOs expansion. Further, NATO had been established as a response to the Soviet threat. Therefore, the continued expansion and even the very existence of NATO after the collapse of the Soviet Union suggested that the West still considered Russia as a threat. During the Summit of the Council on Security and Cooperation in Europe in December 1994, President Yeltsin responded to the news of NATO's expansion plans in his address:

> Europe, even before it has managed to shrug off the legacy of the Cold War, is risking encumbering itself with a cold peace. NATO was created in Cold War times. Today, it is trying to find a place in Europe, not without difficulty. It is important that this search not create new divisions but promote European unity. We believe that the plans of expanding NATO are contrary to this logic. Why sow the seeds of distrust? After all, we are no longer adversaries, we are partners. Some explanations that we hear imply that this is 'expansion of stability,' just in case developments in Russia go the undesirable way. If this is the reason why some

ISSN 1985-563X

> want to move the NATO area of responsibility closer to the Russian borders, let me say this: it is too early to give up on democracy in Russia! [12].

When President Vladimir Putin came to power in 1999, the relationship between Russia and NATO was unresolved. In November 2001, in what appears to be an attempt to resolve relations, Russia established the NATO-Russia Council. However, the alliance did nothing to stop NATO's intentions of expansion. From 2003 the West continued to extend influence in Eastern Europe by funding anti-Russian revolutions in Georgia and Ukraine [13]. According to the Australian Institute of International Affairs, over one billion dollars in aid from the US and Eastern Europe was directed into Georgia. Western NGOs played "a key role in financing opposition parties and organising demonstrations" [13]. In March of 2004, NATO accepted seven new member States, three of which were Baltic: NATO was now the closest it had ever been to the Russian heartland. Later that same year, Georgia and Ukraine would also sign Individual Partnership Action Plans with NATO. NATO continued to be a threat to Russia, with the Bush administration in 2007 releasing plans for a missile defence system in Eastern Europe under the pretext of protecting Europe from an Iranian nuclear attack. Russia responded with a counter plan to construct a joint Russia-US warning system in Azerbaijan, but the US rejected the proposal. In response, President Putin declared that NATO was a real threat to Russia. In 2008 NATO released a statement asserting the intention of extending an invitation to Georgia and Ukraine to join NATO, a move that would position military forces on Russia's doorstep [13]. The 2008 Russo-Georgia war would prevent this from occurring [14].

Russia's campaign in Georgia in 2008 is viewed as a success, as Russia met its goal of taking control of Abkhazia and South Ossetia. The military operation was planned carefully, demonstrating a coordinated approach between military, cyber warfare and diplomatic offensives [15]. As Donovan [14] explains, "in the brief war, the Russian military in a quick and decisive campaign overwhelmed Georgian forces to gain control of two breakaway republics, destroyed much of Georgia's armed forces on land and sea, and caused NATO to reconsider its offer of membership to Georgia". In agreement is Galeotti [1], who states that Russia saw a convincing victory in the Georgia war, demonstrating coordination at the highest level between State and non-State actors and military and political actors.

The "Ossetian problem", as it has been referred to (see for example Donovan [14]), is the result of ethnic enclaves between Georgian and Ossetian created deliberately during the Soviet Union to manage the territory and prevent centralisation of authority in the region. On the collapse of the Soviet Union, both South Ossetia and Abkhazia declared their independence from Georgia. Georgia, however, had sought to regain control of the South Ossetian republic. In response, Russia volunteered to aid in peacekeeping exercises, and in doing so, gained a permanent position on the peacekeeping forces in the Ossetian regions. In the months leading up to the war, several activities allowed Russia to increase its troops and military presence in the region. An increase of 1,000 Russian peacekeeping forces, were introduced in approximately April of 2008. The troops were reported as paratroopers, which Donovan [14] describes as "some of the best trained and prepared forces within Russia". Russia also sent battalion troops into Abkhazia to repair a disused railroad in anticipation of the Sochi Olympics. The troops finished their work one week before the commencement of the war. Lastly, Russian military training was held in the North Caucasus, opposite South Ossetia [14].

When the war began, Russia presented itself as a peacemaker after proxy South Ossetian militias carried out attacks provoking Tbilisi to make the first move. Separatist forces were also engaged in South Ossetia and Abkhazia. Russia's information campaign against Georgia began strong. Russia portrayed President Mikheil Saakashvili as the aggressor. At the same time, Russia was the victim, who was obliged to defend its citizens as attempts by South Ossetia and Abkhazia to become recognised by the Russian parliament were being thwarted by Georgia. Russia entered South Ossetia in anticipation of Georgia's troops responding to separatist troops breaking a cease-fire that had been in place since 1992. Russia was accusing Georgia of aggression towards South Ossetia [16]. The back-story presented

ISSN 1985-563X

by Russia was so compelling that 92 per cent of people polled by CNN at the time found in favour of Russia's intervention [17]. According to Thomas [5], the ostensibly humanitarian position Russia had undertaken in joining the conflict was believed to fit in with what Russia referred to as the "Western doctrine's" need to legitimise military intervention on the national stage. Vladimir Putin, then Prime Minister of Russia, would also blame the US for what was occurring in Georgia, claiming that America should have done more to prevent the conflict. Putin accused the US of orchestrating the campaign as part of an election stunt [18]. In response to Putin and Russia's information campaign, Georgia launched a counter-disinformation campaign led by a private consultancy and public relations firms. The Georgia campaign included images of the Russian military targeting civilians, portraying Moscow as the villains [19].

Cyberspace played an essential role in the Russo-Georgian War, as military and civilians leveraged its power on both sides of the conflict [14]. Media and communications were redistributed via the Internet employing blogs, news channels and rumours, proving so useful that Russian internet and television sites were filtered by Georgian authorities [20]. Command-and-control servers originating from Russia were responsible for malicious hacks, DoS and DDoS attacks against Georgian systems and websites, including web page defacements, and attacks against critical Georgian websites including government, financial services and media [19]. It was unclear, however, who was responsible for these cyberattacks. As Donovan [14] explains, the Russian government has never claimed responsibility for these activities, and it remains unclear whether these operations were coordinated, encouraged, or officially tolerated by Russian authorities.

Several lessons learnt from the Chechnya conflict may be seen in the five-day war in Georgia. A communication plan coordinated responses between the government and military with a pro-Russian message seen across traditional and new media sites. Influential political figures were engaged to undertake political communications on the conflict, such as Prime Minister Vladimir Putin, former President Mikhail Gorbachev and the then-current President Medvedev. Russia strikes were also taken against "key communication facilities severely restrict[ing] communication with the national command authority. National fibre-optic trench lines were severed, and DDoS activities disrupted Internet-based " [14].

The five-day war in Georgia demonstrated the need for heterogeneity of Russian military proficiency; one example may be seen in Russian command and control capabilities [15]. Russia fell short with poor communication strategies on numerous fronts, with criticism occurring within the Russian government of the information warfare strategy that occurred throughout the campaign. As previously noted, pro-Russian media coverage was undertaken, and cyberattacks by alleged Russian patriot hackers throughout the war. Russian analysts, however, suggest that the campaigns were amateur and that the personnel attached to the information warfare division were not trained efficiently [15]. In terms of the cyberattacks undertaken in Russia against Georgia, although seen as successful in interrupting websites and Georgian government information systems, they appear to have had no apparent impact on Georgia's fighting ability [14]. Further, Russian command and control capabilities fell short with regards to a Russian spokesperson. While Georgian nationals presented themselves to a global audience speaking clearly and precisely in English, no one had the same skillset to speak for Russia [3].

In response to Russia's command and control deficiencies during the Georgia war, an idea was formed to create information troops. The information troops would include specialists in a range of hacking, journalism, psychological operations, strategic communications and linguistics. Although there is no proof that the information troops came to fruition, a push for change towards information capabilities was orchestrated [3] [21], leading to, for example, the development of the Russian troll.

ISSN 1985-563X

The war was also used to emphasise Russia's need for military reform and establish the need to improve Russian military equipment and capabilities [15].

4.0 Arab Springs, 2010-2011 and Russian Demonstrations, 2011

A critical event that demonstrated the power of social media to Russia and the world was the Arab Springs uprisings. The Arab Springs uprisings saw citizens in various Middle East and North Africa countries, such as Egypt, Libya, Tunisia, Bahrain and Syria, unite in anti-government protests [22]. Several factors may be seen to have contributed to the uprisings. In June 2010, Khaled Said was brutally murdered by two police officers after the Alexandrian man posted a video online of the same police officers carrying out a drug deal and exchanging money. Said's parents were told that he had choked on a packet of drugs. However, the Internet was soon flooded with images of Said's bloodied and disfigured face, causing public outrage in Egypt and worldwide [23]. Later that year, Mohammed Bouazizi, a vegetable merchant in Tunisia, set himself alight in front of a municipal building protesting the government [24]. Not long after the death of Bouazizi, the world witnessed the fall of President Zine El Abidine on the back of the Tunisian revolution, which was said to have further inspired Egyptian protestors. As Eltantawy and Wiest [23] write, even though Egypt had committed to protests on Egypt's Army Day, "the success in Tunisia appears to have influenced Egyptians and strengthened a sense of collective identity and purpose, primarily because of the similarities in the oppressive conditions under which both groups lived and the goals of the citizen-activists".

During the protests, the Internet and SMNs represented a critical new capability in citizen solidarity and a unified movement [23]. In a study by Eltantawy and Wiest [23] on the use of SMNs during the Egyptian revolutions, it was demonstrated that:

> Egyptian protesters were able to disseminate a continuous stream of text, videos, and images from the streets of the revolution directly to millions via social media technologies, and indirectly through the republication of these messages on news networks such as Al Jazeera and CNN.

SMNs had created a new form of a social movement, known as cyberactivism, which would change the landscape of collective action [23]. According to Eltantawy and Wiest [23], the revolution may be traced to the early 2000s when Egyptian bloggers began to tackle political issues online, attracting a global audience. Then in 2008, Egypt saw its first cyberactivism attempt, when textile workers used social media to organise a strike. The strike, however, was not successful and was defeated by Egyptian State security forces [23]. By the end of 2010, Western news sites were being used by Egyptian individuals and political organisations "to spread credible information to their supporters through the revolutionary period" [24].

SMNs were also used to organise and mobilise demonstrators to facilitate regime change [2]. When the Egyptian and Libyan governments realised that SMNs were being used to coordinate protests and provide footage to the outside world of internal unrest and violence, cellular communications and the Internet were turned off. In response, the sharing of how-to documents instructing people to use dial-up modems were distributed. Additionally, engineers from Twitter, Google and SayNow initiated 'SpeaktoTweet", which provided a means for activists to call and leave messages that would be tweeted [23]. Bloggers whose servers resided outside of Egypt were also relied on to spread the news of the protests, knowing that their voices would not be taken offline [24]. In a study on the Tunisia and Egypt protests, Howard, Duffy [24] found that democracy advocates used social media to connect with supporters outside of their relevant countries. The connections provided a means to get information on what was happening during the protests and throughout the various regions to inform the Western world. Additionally, in many cases, the researchers found that "democracy advocates in Egypt and Tunisia

ISSN 1985-563X

picked up followers in other countries, where similar democratic protests would later erupt. Ultimately social media brought a cascade of messages about freedom and democracy across North America and the Middle East and helped raise expectations for the success of political uprisings" [24].

It is easy to imagine that Russian authorities would have been watching the various uprisings occurring on its doorstep and monitoring for potential replications inside the State [25]. Russia's last revolution led to the collapse of the Soviet Union and what Putin referred to as "the greatest geopolitical disaster of the 20th century". Russian media responded by suggesting that the colour revolutions and the Arab Springs uprisings were orchestrations of the West in a direct attack against Russia and the Russian way of life [26]. In 2015 Vladimir Putin reiterated this allegation in his state-of-the-nation address, where he accused the US of creating "a zone of chaos" in Libya, Iraq and Syria [27]. Russia portrayed the Arab Springs Uprisings as a product of 'social control technology' set in motion from the US as a form of aggression towards Russia. A year later, during the protest movement in Russia surrounding the parliamentary and presidential elections, Moscow would again claim that the manifestation of aggression resulted from information encroachment formulated by the US and codenamed 'Anti-Putin' [28].

According to Lonkila [29], the Putin regime was surprised by the internal protests and degree of civil unrest witnessed during the lead up to the Russian Duma elections in 2011. United Russia was "dubbed a party of swindlers and thieves" [29] as Russia witnessed online activism and public demonstrations denouncing Vladimir Putin. Where in the past there was public fear of participation in political opposition, a result of previous public beatings and the deaths of human rights activists and journalists, such as the murder of Anna Politkovskaya, by December 2011 videos ridiculing Putin and his political party had begun to appear [29].

Putin also blamed the then US Secretary of State Hillary Clinton for interfering in Russia by setting the "tone for some opposition activists" [27]. During her speech at the meeting of the 56-nation Organization for Security and Co-operation in Europe (OSCE), Clinton stated that the US had "serious concerns" regarding Russia's Duma elections. Further, Clinton told the room that "when authorities fail to prosecute those who attack people for exercising their rights or exposing abuses, they subvert justice and undermine the people's confidence in their governments" [30].

Like other cries for democracy around the world, Russia's protests were a direct result of the growth of the Internet and mobile communications [29]. Whereas previously, Russian households received their news from Kremlin-controlled news sources such as Sputnik and RT, the growth of the Internet and mobile communications provided a new source of information for the Russian population. Stories of political corruption and maladministration began to appear on YouTube, questioning Putin's government and authority, while gatherings and protests were organised via SMNs. SMNs brought together like-minded people and provided a platform where participants trusted what was said, which had previously been lost through corrupt Kremlin-controlled media sources. SMNs also provided a way for participants to stay anonymous [29].

In 2016, Russian General Valery Vasilyevich Gerasimov, speaking on the events of the Arab Spring, suggested that the rules of war had changed. "The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness" [31]. Gerasimov [31] suggested that information operations open vast asymmetrical possibilities to reduce an enemy’s fighting potential and that a coordinated effort of research organisations, ministries and agencies could achieve this.

ISSN 1985-563X

5.0 The Kremlin's Response

During the Chechen and Georgia Wars, Russia had learnt that the Internet was a powerful tool in controlling perceptions of the events taking place. The Kremlin's response, at first wary, had changed. The Kremlin's aim was no longer to maintain internet communications. As Galeotti [32] writes:

> The Internet was identified as a potential threat emerged at a time when the security apparatus was relatively weak and in no position to control it. While attempts have been made […] to try and control online activity, instead the security structures had to accept that they operated in an information age and instead looked to means to exploit this.

Russia had invested heavily after 2008 in Twitterbots and targeted DDoS attacks, combining modern technology with "old-fashioned dirty tricks" [3]. However, the results were unsettling as it became evident to the Kremlin that something was missing from Russia's disinformation strategy. Automated systems were not enough, and actual human engagement was needed to penetrate the mass consciousness online [3]. The solution: troll farms.

Exactly when the Kremlin began to use troll farms to spread disinformation and propaganda is debatable. A 2011 report suggests that Russian troll farms began using Twitter to spread propaganda and misinformation to Russian citizens and their neighbours in 2009 [24]. Then in 2012, Russia began targeting misinformation at US voters utilising the techniques deployed on Russian citizens and neighbouring Eastern European countries [24]. According to Planton Mamatov, director of the Russian company, Magic Inc PR, Mamatov ran a troll farm in partnership with the founder of Ra Digital, Arseny Kamyshev, of approximately 20-30 people, from 2008-2013, to "carry out online tasks for Kremlin contacts and regional authorities from Putin's United Russia Party" [33].

Olga Kryshtanovskaya, Russian sociologist, activist, State Duma deputy from the United Russia party and Director of Kryshtanovskaya Labs, suggests Russia's use of troll farms began in approximately 2011 in response to Alexei Navalny's successful social media campaign. Navalny, the Russian Opposition Leader, used social media to support the Russian people leading up to the 2012 Russian parliamentary election. As the Russian media is mostly under the control of the Russian government, opposition activists in Russia are often ignored intentionally by the media leading up to the elections. In response, Navalny turned to an alternative communication space built on SMNs: "This space influences traditional media and the political agenda of the country, giving Navalny a far-ranging voice" [34]. Navalny's campaign gained significant momentum very quickly as he built a rapport with younger voters. Herasimenka [34] attributes Navalny's success to five points:

1. Navalny politicised VKontakte (VK), Russia's largest social media network;
2. Navalny's campaign used an encrypted platform called Telegram to communicate, protecting members;
3. Navalny's team created their own TV network utilising YouTube;
4. Navalny targeted his campaign to Russian provinces, which had until this point, kept out of politics as they were seen by many in these areas as Moscow's domain; and
5. The use of SMNs identified supporters of Navalny as an opposition activist from all over Russia, who would mobilise and spillover from the online and into the streets.

According to Weir [35], the Kremlin would soon mimic this behaviour to spread propaganda and disinformation online. In approximately 2012, the Kremlin tasked Vyacheslav Volodin, known as 'Putin's Cardinal', with designing a strategy to deal with the challenges presented by Facebook, Twitter and other social networks used during the 2011 Russian demonstrations. In response, Volodin installed

ISSN 1985-563X

Prism Corporation, a computer program that monitors 60 million online sources at once, enabling online access to public opinion. Prism provided Volodin with a way to closely monitor social media sites and social tensions, ensuring the government's immediate reaction when necessary (Chen, 2015). Volodin also introduced the mandatory registration of Russian bloggers and began blacklisting internet sites without legal authority, just based on what the Kremlin believed to be unsuitable to the Russian people. Alexei Navalny's blog was among those internet sites that have since been blacklisted [35].

6.0 The Rise of the Troll Farm

The first identifiable troll farm activity that this research was able to identify was Platon Mamatov's troll farm in the Ural Mountains. According to Platon Mamatov, in an interview with the New York Times, Mamatov coordinated a group of Internet trolls to assist in boosting the image of Alexander Misharin, Governor of the Sverdlovsk Region [36]. The farm aimed to "carry out online tasks for Kremlin contacts and regional authorities from Putin's United Russia Party" [33]. The farm's existence was confirmed in late 2011 when Russian News outlet URA.RU reported that paid commentators were operating in the Russian Ural segment of the Internet in a bid to form a positive image of Urals regional authorities. The story came to light after hackers posted correspondence from the Kremlin and Kremlin officials outlining the campaign [37]. Members of Mamatov's staff confirmed this story in response to not having been paid for the work they had carried out throughout the campaign [37]. The project entitled, Improving the Information Background in the Sverdlovsk Runet Segment had been operational since mid-December 2011 in response to online criticism leading up to the Russian Duma elections [37]. According to URA [37], approval for the project was granted by Andrei Vorobyov, the head of the Central Election Commission of the European Union, "when it became clear that opposition activity on the Internet posed a real political threat".

Deputy Prime Minister Alexei Bagaryakov coordinated the project and was in charge of ensuring online discussions 'did not get heated' and to direct conversations in what has been described as a more constructive direction [37]. However, reports indicate that the trolls were utilised instead as a political tool in the upcoming elections to paint a favourable picture of Vladimir Putin and Alexander Misharin. It was not long after that the trolls became known as 'Misharin bots' after online users noticed an influx of positive feedback concerning the regional authorities, particularly Misharin, in forums and blogs [36]. The comments were tied back to the PR Consultant Platon Mamatov. At the time of discovery, Mamatov did not hide his involvement in the campaign, and as highlighted previously, he has been willing to talk about his work with reporters. Mamatov described the process of his operation as follows:

> The group of influence will include a curator from the administration of the governor (Yevgeny Zorin), a coordinator, a monitoring specialist, and commentators. At the first stage, it is supposed to use ten commentators provided with a special program complex and geographically located outside Yekaterinburg.
>
> Subsequently, volunteers from various social movements, members of United Russia, members of the regional government and other people loyal to the regional administration can be connected to the comment. The coordinator of the influence group will also be coordinating and monitoring their work.
>
> Each commentator will have at his disposal several (from three to five) network characters. Each of them will not be a faceless "bot", but a unique personality with a separate IP address, its own character, life history, activity on the Internet, relationships with other users and other properties. Every character will be completely indistinguishable from a real person [37].

ISSN 1985-563X

From news reports and interviews with Platon Mamatov, the troll farms Mamatov created were based on human interactions and not bot activity. Mamatov's operation also appears to be a private company hired to run information campaigns for Russian political figures [33] [38].

7.0 The Internet Research Agency (IRA)

One of the most notorious troll farms which came to public attention in 2014 is the Internet Research Agency (IRA), said to have been established in 2013. According to Ludmila Savchuk, a reporter who went undercover to work for the IRA to uncover the trolling activities of the farm, the IRA operated out of a basement [33] until 2014. Then, with an increase in online activity concerning the Ukraine crisis and Russia's annexure of Crimea, the IRA offices expanded to cover the extra workload expected of employees. The IRA then moved to a different location and occupied over four floors, employing more than 600 workers. The workers were split into two central departments [33]. At the beginning of each shift, employees were assigned a technical task sheet that contained a message that the employee was instructed to support and spread online. As the technical task sheet of former employee Marat Mindiyarov reads;

> The majority of experts agree that the US is deliberately trying to weaken Russia, and Ukraine is being used only as a way to achieve this goal. If the Ukrainian people had not panicked and backed a coup, the west would have found another way to pressure Russia. However, our country is not going to go ahead with the US plans, and we will fight for our sovereignty on the international stage [37].

The job description of the first group of employees, according to Walker [37], was to troll social media sites, both legitimate sites and sites set up by other employees and spread the message on their daily task sheet. The employees were told to create original and new content for each new message they posted; they were not to be repetitive in their postings [37]. Often employees would work in groups of three, with one making a comment or responding to an online post, and then the other two employees would respond to the post to start a discussion and get the thread trending [37]. The second group of employees created mundane blogs or accounts that looked at everyday living, such as gardening or craft. Then between the mundane posts, the employees would include political commentary in an attempt to influence followers. Both groups of employees used Virtual Private Networks (VPNs) to route their operations through computers outside of Russia, presumably to hide the operative's location.

As per Savchuk's original reporting on the IRA activities, employees would create content for popular SMNs such as LiveJournal, Vkontakte, Facebook, Twitter and Instagram. Comments were also left in the comment section of news outlets. For example, when opposition leader Boris Nemtsov was murdered, Savchuk was moved into a specific team to leave comments on various news sites, to suggest that Nemtsov's murder was initiated by his party and not by the Kremlin as per speculation of various sources [38] [33]. Savchuk would work two days on and two days off on twelve-hour shifts. Over those two shifts, Savchuk would be expected to submit five political posts, ten non-political posts and 150-200 comments on other workers posts. Grammar and what Savchuk describes as politology lessons, that is, the study of how the Kremlin manipulated and reported on politics, was also provided to new employees to ensure employees were aware of the "proper Russian point of view on current events"(Chen, 2015).

In a recount of his two months working for the IRA, Mindiyarov explains how he was assigned to post comments on Russian political sites, the work he describes as his rendition of George Orwell's book 1984. Mindiyariov also discusses how he had applied for a position within the English comment department of the IRA, a specific area where employees left comments in English on Western sites, a position held in high regard with a higher salary. However, he did not pass the assessment criteria,

ISSN 1985-563X

which was to write an essay in English on his views on 'if Hillary Clinton were to become president'. Mindiyarov, in his interview with Washington's Top News, recalled writing favourably of Hillary Clinton becoming president, the basis he believes, to his unsuccessful application [38].

At the time of writing, the IRA continues to be referenced as the only known and researched troll farm in Russia. However, Giles [3] suggests that rather than be the only troll farm in existence, the IRA exists as an "effective distraction from the wider network of troll farms, or the organisation behind them".

8.0 Conclusion

After the fall of the Soviet Union, Russia appeared to have lost the sophistication and flair of information warfare seen during the Cold War era. The Russian government demonstrated several failings after the collapse of the Cold War in terms of military strategy and information operations. However, the Russian government also undertook improvements through critical learnings in their formulation of information warfare and their adaptation to online communication applications. During the first Chechen war, Russia's government was not prepared for an information war against Chechnya in their haste to deploy troops. In the second Chechen war, Russia's information operations started strong. However, Russia was unable to maintain control of the information war, as the Internet had emerged as a new and formidable force, the likes of which had never been seen before. In 2008, Russia's military entered the Georgia war prepared for an information and a kinetic war. Unknown persons unleashed an array of cyber-attacks against Georgian websites. The Russian government established a communication plan to ensure the Russian government controlled the information flow. However, once again, Russia fell short concerning information operations. The cyber-attacks did not impact Georgia's ability to respond to Russia's attacks, and unqualified personnel appeared to have led the information operation side of Russia's campaign. Unlike the first Chechen war, Russia demonstrated a successful kinetic military strategy in both the second Chechen war and the Georgia war, but not with information. Tanks and soldiers were not enough for Russia to win on all sides of the war; more was needed.

In response, Russia learnt from the failings of the three wars and began to create an information army to respond to the type of harmful rhetoric seen during both the Chechen wars and the Georgia war. A new imposing strength was in the making, the Internet troll. With the internal unrest occurring in countries bordering Russia and eventually entering Russia, the Russian government needed a way to control the discourse: The Internet appears to be the Kremlin’s answer. In 2008/2009, Russian government officials may be seen using online communication forums to spread favourable messages towards the United Party of Russia and Vladimir Putin. Russian authorities also took back control of the Internet by implementing Prism and patrolling internet sites for anti-Russia discourse. From a Russian government perspective, Russia’s development of kinetic and information warfare techniques responded to the growing threat posed by NATO and the US. At the end of the Cold War, NATO implied that it would not expand. However, by 1994 NATO was the closest it had ever been to Russia and was threatening to advance even closer to Russia's borders with an invitation extended to Georgia and Ukraine; if not for the 2008 Georgia war, this expansion would almost certainly have occurred.

9.0 References

[1] Galeotti, M., Hybrid, ambiguous, and non-linear? How new is Russia’s ‘new way of war’? Small Wars & Insurgencies, 2016. 27(2): p. 282-301.
[2] Giles, K., Russia’s Toolkit, in The Russian Challenge. 2015, Chatham House: London.
[3] Giles, K., The Next Phase of Russian Information Warfare. Vol. 20. 2016: NATO Strategic Communications Centre of Excellence.

ISSN 1985-563X

[4] Finch, R.C.I., Why the Russian military failed in Chechnya. 1998, Foreign Military Studies Office (Army) for Leavenworth KS.
[5] Thomas, T., Manipulating the Mass Consciousness: Russian & Chechen "Information War" Tactics in the Second Chechen-Russian Conflict. The Second Chechen War, 2003: p. 112-129.
[6] Falichev, O., FCS will Certainly Publish Information on Who Helped Dudayev and How. Krasnaya Zvezda, 1995. 21.
[7] Global Security, First Chechnya War - 1994-1996. 2019, Globalsecurity.org.
[8] Polkovnikov, P., A Painful Spot. Nezavismoye Voyennoye Obozreniye, 1999.
[9] Heickerö, R., Emerging cyber threats and Russian views on Information warfare and Information operations. 2010: Defence Analysis, Swedish Defence Research Agency (FOI).
[10] Sarotte, M.E., A Broken promise: What the West really told Moscow about NATO expansion. Foreign Aff., 2014. 93: p. 90.
[11] Goldgeier, J.M. and M. McFaul, Power and purpose: US policy toward Russia after the Cold War. 2003: Brookings Institution Press.
[12] Asmus, R.D., Opening NATO's door: how the alliance remade itself for a new era. 2004: Columbia University Press.
[13] Thalis, A., Threat or Threatened? Russia in the Era of NATO Expansion. Austraian Institute of International Affairs, 2018(Australian Outlook).
[14] Donovan, G.T.J., Russian Operational Art in the Russo-Georgian War of 2008. 2009, Army War Coll Carlisle Barracks PA.
[15] Vendil Pallin, C. and F. Westerlund, Russia's war in Georgia: lessons and consequences. Small wars & insurgencies, 2009. 20(2): p. 400-424.
[16] Roudik, P., Russian Federation: Legal Aspects of War in Georgia, in Library of Congress. 2019.
[17] Cohen, A. and R.E. Hamilton, The Russian military and the Georgia war: lessons and implications. 2011: Strategic Studies Institute.
[18] Chance, M., Putin accuses U.S. of orchestrating Georgian war, in CNN. 2008.
[19] Iasiello, E., Russia's Improved Information Operations: From Georgia to Crimea. Parameters, 2017. 47(2).
[20] Deibert, R.J., R. Rohozinski, and M. Crete-Nishihata, Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. Security Dialogue, 2012. 43(1): p. 3-24.
[21] Giles, K., Russia and its Neighbours: old attitudes, new capabilities. Cyber War in Perspective: Russian Aggression against Ukraine, 2015: p. 19-28.
[22] Bruns, A., T. Highfield, and J. Burgess, The Arab Spring and its social media audiences: English and Arabic Twitter users and their networks, in Cyberactivism on the participatory web. 2014, Routledge. p. 96-128.
[23] Eltantawy, N. and J.B. Wiest, The Arab spring| Social Media in the Egyptian revolution: reconsidering resource mobilization theory. International journal of communication, 2011. 5: p. 18.
[24] Howard, P.N., et al., Opening closed regimes: what was the role of social media during the Arab Spring? Available at SSRN 2595096, 2011.
[25] Bechev, D., Russia in the Middle East: From the Arab Uprisings to the Syrian Conundrum, in Alsharq Forum. 2016: Turkey.
[26] Katz, M.N., No Reason to Fear Arab Spring in Russia, in The Moscow Times. 2011: Moscow.
[27] CBSNews, Putin makes accusation against U.S. over Syria policy, in CBS News. 2015.
[28] Darczewska, J., The anatomy of Russian information warfare. The Crimean operation, a case study. 2014: Ośrodek Studiów Wschodnich im. Marka Karpia.
[29] Lonkila, M., Russian Protest On-and Offline: The role of social media in the Moscow opposition demonstrations in December 2011. UPI FIIA Briefing Papers, 2012. 98.
[30] Mohammed, A. and N. Adomaitis, Clinton criticizes Russia vote, Germany urges improvement, in Reuters. 2011.
[31] Gerasimov, V., Po opytu Sirii. Voenno-promyshlennyi kur'er 2016.

ISSN 1985-563X

[32] Galeotti, M., Russian Political War: Moving Beyond the Hybrid. 2019: Routledge.
[33] Chen, A., The Agency, in The New York Times Magazine 2015. 2015.
[34] Herasimenka, A., What's behind Alexei Navalny's digital challenge to Vladimir Putin's regime? Five things to know., in The Washington Post. 2018: Washington DC.
[35] Weir, F., Before Russia's 'troll farm' turned to US, it had a more domestic focus, in The Christian Science Monitor. 2018.
[36] Business Quarter, The author of the Urals "Botgate" runs a business with the founder of "Ra Digital", in Business Quarter. 2013.
[37] URA, Hackers have made public the work of Sverdlovsk PR people who are helping the Misharin administration on the Internet. In the open access - hundreds of letters with "temniki", instructions, instructions, in URA.RU. 2012: Russia.
[38] URA, For the last month and a half a secret squad of bloggers has been working. They were asked, for example, to call Tagil workers "cattle" ... in URA.RU. 2012: Russia.
[39] Walker, S., The Russian troll factory at the heart of the meddling allegations, in The Guardian. 2015.
[40] Satter, D., Russia Questions for Rex Tillerson. Wall Street Journal, 2017.
[41] Green, J.J., Tale of a Troll: The Russian operation to target Hillary Clinton, in Washington's Top News. 2018.

ISSN 1985-563X

